# Lecture 11

# Integral Domains (整域)

**11.1** Euclidean Domains (ユークリッド整域)

**11.2** Factorization (分解) in Integral Domains

# 11.1 Euclidean Domains

# (ユークリッド整域)

# 11.1 Euclidean Domains (ユークリッド整域)

We have seen that both rings $\mathbb{Z}$ and $F[x]$, where $F$ is a field, have a **division algorithm**. In this lecture, we discuss the properties for **integral domains (整域)**.

Recall in Lecture 1, we defined Complement of Set as

**Definition 1.4**

Given two sets $A$ and $B$, the **relative complement** of $B$ in $A$, denoted by *the set difference* $A \backslash B$, is the set

$$A \backslash B = A \cap B' = \{x \mid x \in A, \ \text{but } x \notin B\}.$$

## Definition 11.1

A **Euclidean domain** is an **integral domain** $(E, +, \cdot)$ together with a function $v: \ E\backslash\{0\} \to \mathbb{Z}^{\#}$ (Here $\mathbb{Z}^{\#}$ denotes **the set of nonnegative (非負の) integers**) such that

(i) for all $a, b \in E$ with $b \neq 0$, there exist $q, r \in E$ such that $a = qb + r$, where either $r = 0$ or $v(r) < v(b)$

and

(ii) for all $a, b \in E\backslash\{0\}, v(a) \leq v(ab)$.

The function $v$ is called a **Euclidean valuation (ユークリッド賦値) (or Euclidean norm)**.

# 11.1 Euclidean Domains (ユークリッド整域)

**Example 11.1**
Let $(E,+,\cdot)$ be a **Euclidean domain** with **Gaussian valuation** $v$.
(a) Show that $v(a) = v(-a)$ for all $a \in E\backslash\{0\}$.
(b) Show that for all $a \in E\backslash\{0\}, v(a) \geq v(1)$, where equality holds if and only if $a$ is a **unit** in $E$.
(c) Let $n$ be an integer such that $v(1) + n \geq 0$. Show that the function

$$v_n\colon E\backslash\{0\} \to \mathbb{Z}^\#$$

defined by $v_n(a) = v(a) + n$ for all $a \in E\backslash\{0\}$ is a **Euclidean valuation**.

**Solution**
(a) For all $a \in E\backslash\{0\}, v(a) = v((-1)(-a)) \geq v(-a) = v((-1)a) \geq v(a)$ according to definition 11.1. Hence, $v(a) = v(-a)$ for all $a \in E\backslash\{0\}$.
(b) Let $a \in E\backslash\{0\}$. Now $v(a) = v(1a) \geq v(1)$. Suppose $a$ is a **unit**. Then there exists an element $c \in E$ such that $ac = 1$. Thus, $v(1) = v(ac) \geq v(a)$. This implies that $v(a) = v(1)$. Conversely, suppose that $v(a) = v(1)$. Since $a \neq 0$, there exist $q, r \in E$ such that $1 = qa + r$, where $r = 0$ or $v(r) < v(1)$. Now $v(r) < v(1)$ is impossible. Hence, $r = 0$, showing that $1 = qa$. Thus, $a$ is a unit.
(c) Let $a \in E\backslash\{0\}$. Then $v_n(a) = v(a) + n \geq v(1) + n \geq 0$. Hence, $v_n(a) \in \mathbb{Z}^\#$. Suppose $a, b \in E$ with $b \neq 0$. There exist $q, r \in E$ such that $a = qb + r$, where either $r = 0$ or $v(r) < v(b)$. Now $v(r) < v(b)$ implies that $v(r) + n < v(b) + n$. Thus, $v_n(r) < v_n(b)$. Also, for $a, b \in E\backslash\{0\}, v_n(ab) = v(ab) + n \geq v(a) + n = v_n(a)$. Therefore, $v_n$ is a **Euclidean valuation** on $E$.

# 11.1 Euclidean Domains (ユークリッド整域)

**Example 11.2**

The ring $\mathbb{Z}$ of integers can be considered a **Euclidean domain** with $v(a) = |a|, a \neq 0$.

# 11.1 Euclidean Domains (ユークリッド整域)

## Theorem 11.1

If $F$ is a **field**, then the **polynomial ring** $F[x]$ is a **Euclidean domain**.

**Proof** (See page 185 of Ref. Textbook, *Introduction of Abstract Algebra*)

# 11.1 Euclidean Domains (ユークリッド整域)

**Example 11.3**

**Any field** can be considered as a **Euclidean domain** with $v(a) = 1$ for all $a \neq 0$.

$(a \ = \ (ab^{-1})b + 0.)$

# 11.1 Euclidean Domains (ユークリッド整域)

## Definition 11.2

The **subset** $\mathbb{Z}[i] = \{a + bi \mid a, b \in Z\}$ **of the complex numbers** is called **the set of Gaussian integers (ガウス整数)**.

Carl Gauss (German mathematician, 1777-1885) was the first to study $\mathbb{Z}[i]$ and hence in his honor $\mathbb{Z}[i]$ is called **the ring of Gaussian integers.**

## Theorem 11.2

The set $\mathbb{Z}[i]$ of **Gaussian integers** is a **subring** of $\mathbb{C}$. The units of $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$.

**Proof** (See page 186 of Ref. Textbook, *Introduction of Abstract Algebra*)

# 11.1 Euclidean Domains (ユークリッド整域)

**Notice**: The (field) **norm** $N$ is a particular mapping defined in field theory, which maps elements of a larger field into a subfield.

## Theorem 11.3

The **ring** $\mathbb{Z}[i]$ of **Gaussian integers** becomes a **Euclidean domain** when we let the function,

$$N: \mathbb{Z}[i] \backslash \{0\} \to \mathbb{Z}^{\#}$$

defined by $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$ for all $a, b \in \mathbb{Z}$, serve as a **Euclidean valuation** function $v$.

**Proof** (See page 186 of Ref. Textbook, Malik, *Introduction to Abstract Algebra*)

# 11.1 Euclidean Domains (ユークリッド整域)

We now consider the **ideals of a Euclidean domain**.

Recall that an **ideal** $I$ of a **ring** $R$ is called a **principal ideal** if $I = \langle a \rangle = \{ar : r \in R\}$ for some $a \in I$.

## Definition 11.3

Let $R$ be a **commutative ring with identity**. If **every ideal** of $R$ is a **principal ideal**, then $R$ is called a **principal ideal ring**. An **integral domain** which is also a **principal ideal ring** is called a **principal ideal domain** (**PID**) (**単項イデアル整域**).

## Theorem 11.4

**Every Euclidean domain** is a **principal ideal domain (PID)**.

Proof (See page 186 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

# 11.1 Euclidean Domains (ユークリッド整域)

## Theorem 11.5

Let $R$ be a commutative ring with identity. **The following conditions are equivalent.**
(i) $R$ is a **field**.
(ii) $R[x]$ is a **Euclidean domain**.
(iii) $R[x]$ is a **PID**.

**Proof** (See page 187 of Ref. Textbook, Malik, Introduction of Abstract Algebra)

## Corollary 11.1

$\mathbb{Z}[x]$ is not a PID.

**Proof**

Now $\mathbb{Z}$ is a commutative ring with identity. Since $\mathbb{Z}$ is not a field, $\mathbb{Z}[x]$ is not a **PID** by Theorem 11.5.

# 11.2 Factorization (分解) in Integral Domains

# 11.2 Factorization (分解) in Integral Domains

## Definition 11.4

Let $R$ be a commutative ring and $a, b \in R$ be such that $a \neq 0$. If there exists $c \in R$ such that $b = ac$, then $a$ **is said to divide** $b$ or $a$ is said to be a **divisor** of $b$ and we write $a \mid b$.

## Definition 11.5

Let $R$ be a commutative ring with identity. **A nonzero element $a \in R$ is said to be an associate (同伴) of a nonzero element $b \in R$ if $a = ub$ for some unit $u \in R$.**

# 11.2 Factorization (分解) in Integral Domains

**Example 11.4**

(i) In $\mathbb{Z}$, $1$ and $-1$ are the only **units**. For every $a \in \mathbb{Z}$ and $a \neq 0$, we know $a$ and $-a$ are **associates**.

(ii) In $\mathbb{Z}[i]$, $1, -1, i, -i$ are the **only units**. Thus, $1 + i$, $-1 - i$, $-1 + i$, $1 - i$ are all **associates** of $1 + i$.

**Example 11.5**

In the **polynomial ring** $F[x]$ over a field $F$, the units form the set $F\backslash\{0\}$. A **nonconstant polynomial** $f(x)$ has $uf(x)$ for an **associate**, where $u$ is a **unit** in $F$.

# 11.2 Factorization (分解) in Integral Domains

## Definition 11.6

Let $R$ be a commutative ring with identity.
(i) An element $p$ of $R$ is called **irreducible (既約な)** if $p$ is nonzero and a nonunit and $p = ab$ with $a, b \in R$ implies that either $a$ or $b$ is a **unit**. An element $p$ of $R$ is called **reducible** if $p$ is **not irreducible**.
(ii) An element $p$ of $R$ is called **prime** if $p$ is **nonzero** and a **nonunit**, and if whenever $p \mid ab$, $a, b \in R$, then either $p$ divides $a$ or $p$ divides $b$.
(iii) Two elements $a$ and $b$ of $R$ are called **relatively prime** if their only **common divisors** are **units**.

From the definition of an irreducible element, it follows that the **only divisors of an irreducible element $p$ are the associates of $p$ and the unit elements of $R$.**
The converse of this result does not always hold in a commutative ring with identity.

# 11.2 Factorization (分解) in Integral Domains

## Theorem 11.6

Let $R$ be an **integral domain** and $p \in R$ be such that $p$ is **nonzero** and a **nonunit**. Then $p$ is **irreducible if and only if** the **only divisors** of $p$ are the **associates** of $p$ and **the unit elements of** $R$.

**Proof** (See page 194 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

**Example 11.6**
In $\mathbb{Z}$, $1$ and $-1$ are the only units, and therefore 2 is divisible by $\pm 1$ and $\pm 2$. It follows that 2 is not divisible by any other integer. Therefore, 2 is an irreducible element.
Suppose now 2 | $ab$ and 2 does not divide $a$ for some $a, b \in \mathbb{Z}$. Since 2 does not divide $a$, $a$ is an odd integer and so $\gcd(2, a) = 1$.
Therefore, there exist $c, d \in \mathbb{Z}$ such that $1 = 2c + ad$. Thus, $b = 2bc + abd$. Since 2 | $ab$ and 2 | $2bc$, it follows that 2 | $b$. Hence, 2 is prime.

# 11.2 Factorization (分解) in Integral Domains

**Example 11.7**

Consider the integral domain

$$\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in Z\}$$

Let us show that $3 = 3 + 0i\sqrt{5} \in Z[i\sqrt{5}]$ is **irreducible**, **but not prime**. Suppose $3 = (a + bi\sqrt{5})(c + di\sqrt{5})$ in $\mathbb{Z}[i\sqrt{5}]$. Then $3 = \overline{3} = \overline{(a + bi\sqrt{5})(c + di\sqrt{5})} = (a - bi\sqrt{5})(c - di\sqrt{5})$. Hence, $9 = (a^2 + 5b^2)(c^2 + 5d^2)$. Since $a, b, c, d$ are integers, the previous equality implies that

$$a^2 + 5b^2 = 3 \text{ and } c^2 + 5d^2 = 3 \qquad (11.1)$$

or

$$a^2 + 5b^2 = 1 \text{ and } c^2 + 5d^2 = 9 \qquad (11.2)$$

or

$$a^2 + 5b^2 = 9 \text{ and } c^2 + 5d^2 = 1 \qquad (11.3)$$

Clearly there do not exist integers $a, b, c, d$ satisfying Eqs. (11.1). The first equation of Eqs. (11.2) implies that $b = 0$ and $a = \pm 1$. Thus, it follows that $a + bi\sqrt{5}$ is a unit. Similarly, the second equation of Eqs. (11.3) implies that $c + di\sqrt{5}$ is a unit. Hence, $3$ is irreducible. Now $3 \mid 6$ and $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Suppose $3 \mid (1 + i\sqrt{5})$. Then $1 + i\sqrt{5} = 3(a + bi\sqrt{5})$ for some $a, b \in \mathbb{Z}$. This implies that $3a = 1$, a contradiction, since the equation $3a = 1$ has no solution in $\mathbb{Z}$.

Hence, $3$ does not divide $(1 + i\sqrt{5})$. Similarly, $3$ does not divide $(1 - i\sqrt{5})$. Thus, $3$ is not prime.

# 11.2 Factorization (分解) in Integral Domains

Every field is also an integral domain; however, there are many integral domains that are not fields. For example, the integers $\mathbb{Z}$ form an integral domain but not a field. A question that naturally arises is how we might associate an integral domain with a field.

There is a natural way to construct the rationals $\mathbb{Q}$ from the integers: the rationals can be represented as formal quotients of two integers. The rational numbers are certainly a field. In fact, it can be shown that the rationals are the smallest field that contains the integers.

Given an integral domain $D$, our question now becomes how to construct a smallest field $F$ containing $D$. We will do this in the same way as we constructed the rationals from the integers.

# 11.2 Factorization (分解) in Integral Domains

Let's introduce the **Fundamental Theorem of Arithmetic (算術の基本定理)**.

**Theorem 11.7 (Fundamental Theorem of Arithmetic)**

Let $n$ be an **integer** such that $n > 1$. Then

$$n = p_1 p_2 \cdots p_k$$

where $p_1, p_2, \ldots, p_k$ are primes (not necessarily distinct).

Furthermore, this **factorization** is **unique**; that is, if

$$n = q_1 q_2 \cdots q_l$$

then $k = l$ and the $q_i$'s are just the $p_i$'s rearranged.

**Proof** (See page 13 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

# 11.2 Factorization (分解) in Integral Domains

We study those integral domains in which an analogue of the **Fundamental Theorem of Arithmetic** holds.

## Definition 11.7

A **nonzero nonunit element** $a$ of an **integral domain** $D$ is said to **have a factorization (分解)** if $a$ can be expressed as

$$a = p_1 p_2 \cdots p_k$$

where $p_1, p_2, \dots, p_k$ are **irreducible elements of** $D$. The expression $p_1 p_2 \cdots p_k$ is called **a factorization of** $a$.

## Definition 11.8

**An integral domain** $D$ is called a **factorization domain (FD)** if **every nonzero nonunit element has a factorization.**

# 11.2 Factorization (分解) in Integral Domains

In an integral domain $D$ every nonzero element $a \in D$ is always divisible by the associates of $a$ and the units of $D$. These are called the **trivial factors** of $a$. **All other factors (if any) of** a are called **nontrivial**. For example, $\pm 2$ and $\pm 3$ are **nontrivial factors** of $6$ in $\mathbb{Z}$.

In the following lemma, we show that a nonzero nonunit element that has no factorization as a product of irreducible elements can be expressed as a product of any number of nontrivial factors.

**Lemma 11.1**

Let $D$ be an **integral domain**. Let $a$ be a **nonzero nonunit element** of $D$ such that a **does not have a factorization**. Then for **every positive integer** $n$, there exist **nontrivial factors** $a_1, a_2, \ldots, a_n \in D$ of a such that $a = a_1 a_2 \cdots a_n$.

**Proof** (See page 199 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

## Theorem 11.8

Let $D$ be an **integral domain** with a function $N\colon D\backslash\{0\} \to \mathbb{Z}^{\#}$ such that for all $a, b \in D\backslash\{0\}$, $N(ab) \geq N(b)$, **where equality holds if and only if $a$ is a unit**. Then $D$ is a **FD**.

**Proof** (See page 199~200 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

**Example 11.8**

Consider the integral domain $\mathbb{Z}[i]$. Define

$$N: \mathbb{Z}[i] \backslash \{0\} \to \mathbb{Z}^{\#}$$

By $N(a+bi) = a^2 + b^2$ for all $a + bi \in \mathbb{Z}[i]$.

It is easy to verify that $a + bi$ is a **unit** if and only if $N(a+bi) = 1$.

Let $a + bi$, $c + di$ be two nonzero elements of $\mathbb{Z}[i]$.

Then $N\big((a+bi)(c+di)\big) = N\big((ac-bd) + (ad+bc)i\big)$

$$\begin{aligned} &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\ &= a^2(c^2+d^2) + b^2(c^2+d^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &\geq (c^2+d^2) \\ &= N(c+di) \end{aligned}$$

where the equality holds if and only if $N(a+bi)$ is a **unit**.

Hence, $\mathbb{Z}[i]$ is a **FD**.

# 11.2 Factorization (分解) in Integral Domains

## Definition 11.9

An **integral domain** $D$ is called a unique factorization domain (UFD) (一意分解整域) if the following two conditions hold in $D$:

(i) every nonzero nonunit element of $D$ can be expressed as

$$a = p_1 p_2 \cdots p_k$$

where $p_1, p_2, \ldots, p_k$ are irreducible elements of $D$

and

(ii) if $a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ are two factorizations of $a$ as a finite product of irreducible elements of $D$,

then $k = l$ and there is a permutation $\sigma$ of $\{1, 2, \ldots, k\}$ such that $p_i$ and $q_{\sigma(i)}$ are associates for all $i = 1, 2, \ldots, k$.

From the above definition, it follows that an **integral domain** $D$ is a **UFD if and only if** $D$ is a **FD** and **every nonzero nonunit element of** $D$ **is uniquely expressible** (apart from unit factors and order of the factors) **as a finite product of irreducible elements**.

# 11.2 Factorization (分解) in Integral Domains

## Theorem 11.9

In a **unique factorization domain** (UFD), **every irreducible element** is **prime**.

**Proof** (See page 201 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

## Theorem 11.10

A **factorization domain** (FD) $D$ is a **UFD if and only if every irreducible element of** $D$ is a **prime element**.

**Proof** (See page 201 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

## Theorem 11.11

A **Euclidean domain** is a **unique factorization domain (UFD)**.

**Proof** (See page 202 of Ref. Textbook, Malik, *Introduction of Abstract Algebra*)

# 11.2 Factorization (分解) in Integral Domains

**Example 11.9**

Consider the integral domain $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} | \ a, b \in Z\}$. Define

$$N\colon Z[i\sqrt{5}]\backslash\{0\} \to \mathbb{Z}^{\#}$$

by

$$N(a + bi\sqrt{5}) \ = \ a^2 + 5b^2$$

We can show that $a + bi\sqrt{5}$ is a unit if and only if $N\left(a + bi\sqrt{5}\right) = 1$. Let $a + bi\sqrt{5}$, $c + di\sqrt{5}$ be two nonzero elements of $\mathbb{Z}[i\sqrt{5}]$.

Then $N\left(\left(a + bi\sqrt{5}\right)\left(c + di\sqrt{5}\right)\right) = N\left((ac \ - \ 5bd) + i(ad + bc)\sqrt{5}\right) = \ (ac - 5bd)^2 + 5(ad + bc)^2 = (a^2 + 5b^2)(c^2 + 5d^2) \geq (c^2 + 5d^2) = N\left(\left(c + di\sqrt{5}\right)\right)$, where equality holds if and only if $N\left(a + i\sqrt{5}\right) = 1$, i.e., if and only if $a + bi\sqrt{5}$ is a unit. Hence, $\mathbb{Z}[i\sqrt{5}]$ is a **FD** by Theorem 11.8. In Example 11.7, we showed that 3 is an irreducible element. Now 3 | $(2 + i\sqrt{5})(2 - i\sqrt{5})$. Suppose 3 | $(2 \ + \ i\sqrt{5})$. Then $2 \ + i\sqrt{5} = \ 3(m \ + \ ni\sqrt{5})$ for some $m + ni\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$. This implies $2 \ = \ 3m$ and $1 \ = \ 3n$, which is impossible for integers $m$ and $n$. Therefore, 3 does not divide $(2 + i\sqrt{5})$. Similarly, 3 does not divide $(2 - i\sqrt{5})$. Thus, 3 is not prime in $\mathbb{Z}[i\sqrt{5}]$. Hence, $\mathbb{Z}[i\sqrt{5}]$ is not a **UFD** by Theorem 11.9.

## Review for Lecture 11

- Euclidean Domain (ユークリッド整域)
- Gaussian Integers (ガウス整数)
- Associate (同伴)
- Fundamental Theorem of Arithmetic (算術の基本定理)
- Unique Factorization Domain (UFD) (一意分解整域)

## Assignment

Please Check https://github.com/uoaworks/Applied-Algebra

## References

[1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018
[2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007
[3] **(おすすめ)** 松本 眞, 代数系への入門, http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf
[4] Wikipedia
[5] Materials from internet.

# Appendix

## *Definition

Let $R$ be a commutative ring and $a_1, a_2, \ldots, a_n$ be elements in $R$, not all zero. A nonzero element $d \in R$ is called a **common divisor** of $a_1, a_2, \ldots, a_n$ if $d \mid a_i$ for all $i = 1, 2, \ldots, n$. A nonzero element $d \in R$ is called a **greatest common divisor** (**gcd**) of $a_1, a_2, \ldots, a_n$ if

(i) $d$ is a **common divisor** of $a_1, a_2, \ldots, a_n$ and

(ii) if $c \in R$ is a **common divisor** of $a_1, a_2, \ldots, a_n$, then $c \mid d$.