[I216e] Computational Complexity and Discrete Mathematics

Ryuhei Uehara, and Eiichiro Fujisaki

Japan Advanced Institute of Science and Technology

November 22nd, 2017.

I216e (Computational Complexity and Discrete Math): Discrete Math

- URL: `http://www.jaist.ac.jp/~fujisaki/index-e.html`
- Date: 11/6, 11/8, 11/13, 11/15, 11/20 (twice), 11/22, 11/27 (test)
- Room: Room I-2
- Office Hour: Monday 13:30 – 15:10
- Reference (参考図書)
  - 「代数概論」森田康夫著，裳華房.
  - “Abstract Algebra,” David Dummit and Richard Foote, Prentice Hall.
  - 「代数学入門」松本眞,
    Free eBook URL:
    `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/`
  - “A Computational Introduction to Number Theory and Algebra,”
    Victor Shoup, Cambridge University Press.
    Free eBook URL: `http://www.shoup.net/ntb/`

What will you study in the part of Discrete Math.?

From Algebra (抽象代数)

- Axioms of Groups (群), Rings (環), Fields (体)
- Equvalent class (同値類)
  - Equivalent relation (同値関係), Congruence (合同)
- Lagrange's Theorem (ラグランジェの定理)
  - Lagrange's Theorem $\rightarrow$ Fermat's little Theorem, and Euler's Theorem
- Fundamental Homomorphism Theorem(s) (準同型定理)
  - Normal subgroup (正規部分群), Residue class group (剰余類群) (= Quotient group (商群))
  - Fundamental Homomorphism Theorem $\rightarrow$ Chinese Reminder Theorem (CRT).
- Ring Fundamental Homomorphism Theorem (環準同型定理)
  - Ideal; Ideal (for ring) $\Longleftrightarrow$ Normal subgroup (for group).
  - Residue class ring (剰余類環) (= Quotient ring (商環))

What will you study (cont.)

Number Theory (初等整数論)

- Generalization of Integers (Informal)
  - Integral Domain (整域): Euclidean domain (ユークリッド整域), Principal ideal domain (PID) (単項イデアル整域), Unique factorization domain (UFD) (一意分解整域).
  - Euclidean domain $\subset$ PID $\subset$ UFD.
- Extended Euclidean Algorithm (拡張ユークリッドの互除法)
  - Solution for:
    - linear Diophantine equation (一次ディオファントス方程式), and
    - computing the inverse of an (invertible) element in (residue class) ring $\mathbb{Z}/n\mathbb{Z}$.

Application: RSA public-key cryptosystem. Related to:

- Euler's totient function $\phi(n)$, Euler's Theorem
- Structure of $\mathbb{Z}/n\mathbb{Z}$
- Chinese Remainder Theorem

Today's Contents

Today's Summary

Generalization of Integers: Integral Domain (整域).

$$\mathbb{Z} \subset \text{ED} \subset \text{PID} \subset \text{UFD} \subset \text{ID} \subset \text{Commutative Ring},$$

where ED: Euclidean Domain and ID: Integral Domain.

Generalization of Prime Numbers: Prime Ideal (素イデアル)

$$\text{Maximal Ideal (極大イデアル)} \subset \text{Prime Ideal}$$

Theorem

Let R be a ring and I be a maximal ideal. Then R/I is a field.

Theorem

In PID R, a prime ideal = a maximal ideal.

Today's Summary (Cont.)

Theorem

Denote by $\mathbb{F}_q$ a finite field of order q. Then, $q = p^r$ for some prime p and integer $r (\geq 1)$. In addition,

- $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ if $q = p$.
- $\mathbb{F}_q \cong \mathbb{F}_p[X]/f(X)$ if $q = p^r$ $(r \geq 2)$ where $f(X)$ is a monic polynomial of degree r.

- $\mathbb{F}_p[X]$: Polynomial ring over $\mathbb{F}_p$.
- $\mathbb{F}_p[x]$ is an Euclidean domain.
- A polynomial $f(X) = a_0 + a_1 X + \cdots + a_r X^r$ is called monic if $a_r = 1$.

Today's Contents

Integral Domain (整域)

Definition 1 (Zero-Divisor (零因子))

Let R be a ring. A non-zero element $a \in R$ $(a \neq 0)$ is called *a zero-divisor* (零因子) if there is non-zero $b \in R$ $(b \neq 0)$ such that $a \cdot b = b \cdot a = 0$.

Definition 2 (Integral Domain (整域))

A commutative ring (with 1) R is called *an integral domain* if it has no zero-divisor.

- A field is an integral domain.
- $\mathbb{Z}$ is an integral domain.
- $\mathbb{Z}/15\mathbb{Z}$ is not an integral domain, because $3, 5$ are zero-divisors of $\mathbb{Z}/15\mathbb{Z}$.

Divisor (約元) and Multiple (倍元)

Integral Domain: A generalization of $\mathbb{Z}$.

Definition 3

Let R be an integral domain. For $a, b \in R$, we write $a|b$ if there is $x \in R$ such that $a \cdot x = b$. The element a is called *a divisor* of b and the element b *a multiple* of a.

- $\mathbb{Z}$: divisor (約数), multiple (倍数)
  vs Integral domain R: divisor (約元), multiple (倍元)
- $x \in R^{\times} \iff x|1$.

Prime Element (素元) and Irreducible Element (既約元)

Definition 4

Let R be an integral domain.

- An element p in R is called *a prime element* if the following holds:

$$\forall p, a, b \in R \quad \left(p \notin R^{\times} \wedge p|ab \quad \Longrightarrow \quad p|a \text{ or } p|b\right).$$

- An element q in R is called *an irreducible element* if the following holds:

$$\forall q, x, y \in R \quad \left(q \notin R^{\times} \wedge q = xy \quad \Longrightarrow \quad x \in R^{\times} \text{ or } y \in R^{\times}\right).$$

- Any prime element is irreducible, but not vice versa, i.e., Prime $\subsetneq$ Irreducible.
- The set of the prime elements (Prime) in $\mathbb{Z}$ is $\{\pm p \mid p : \text{ prime }\}$.
- In $\mathbb{Z}$ (or UFD), Prime $=$ Irreducible (NOTE: $\mathbb{Z}^{\times} = \{\pm 1\}$).

Euclidean Domain (ユークリッド整域)

Definition 5 (Euclidean Domain)

An integral domain R is called an Euclidean domain if there is a map $\lambda : R \to \mathbb{Z}^{\geq 0}$ such that

- For all non-zero $x \in R$, $\lambda(0) < \lambda(x)$.
- For all non-zero $x \neq R$ and all $d \in R$, there exist $q, r \in R$ such that $x = q \cdot d + r$ and $\lambda(r) < \lambda(d)$.

- $\mathbb{Z}$ is Euclidean with $\lambda(x) = |x|$.
- A polynomial ring $K[X]$ over field K is Euclidean. For $f \in K[X]$, define $\lambda(f) = \deg(f)$.

Principal Ideal (単項イデアル) and Prime Ideal (素イデアル)

Let R be an integral domain ($=$ a commputative ring with no zero-divisor).

Definition 6 (Principal Ideal)

For $a \in R$, define $(a) = \{r \cdot a \mid r \in R\}$. (a) is called *a principal ideal* in R.

Definition 7 (Prime Ideal)

An ideal I such that $I \subsetneq R$ is called *a prime ideal* in R if

$$\forall a, b \in R \left(a \cdot b \in I \implies a \in I \text{ or } b \in I \right).$$

Proposition 1

Let R be an integral domain.
$a \in R$ is a prime element $\iff$ (a) is a prime ideal in R.

Principal Ideal Domain (単項イデアル整域)

Definition 8 (Principal Ideal Domain (PID))

Let R be an integral domain. If every ideal in R is a principal ideal, then R is called *a principal ideal domain*.

- Euclidean Domain (ユークリッド整域) $\subset$ Principal Ideal Domain (単項イデアル整域).
- In a PID, a prime element (素元) $=$ an irreducible element (既約元).
  - In a PID R,
    $a \in R$: an irreducible element $\Leftrightarrow$ $a \in R$: a prime element $\Leftrightarrow$ $(a) \subset R$: a prime ideal.
- In $\mathbb{Z}$, any ideal is of the form $(n) = n\mathbb{Z}$; $p\mathbb{Z}$ is a prime ideal for any prime p; if I is a prime ideal, there is a prime p such that $I = p\mathbb{Z}$.

NOTE: Unique Factorization Domain (UFD, 一意分解整域). Euclidean Domain $\subset$ PID $\subset$ UFD.

In a UFD, a prime element $=$ an irreducible element, and a factorization is unique and hence, so is in a PFD.

NOTE: Principal Ideal

- For commutative ring R,

$$(a_1, \ldots, a_n) \triangleq \{r_1 \cdot a_1 + \cdots + r_n \cdot a_n \mid r_1, \ldots, r_n \in R\}$$

  is an ideal. When R is a PID, by definition, there exists $a \in R$ such that

$$(a_1, \ldots, a_n) = (a).$$

  Here, a is called *the greatist common divisor* (GCD) of $a_1, \ldots, a_n$.
- NOTE: $(1) = R$.
- In the case of $(a_1, \ldots, a_n) = (1)$, by definition, there are $r_1, \ldots, r_n \in R$ such that

$$r_1 \cdot a_1 + \cdots + r_n \cdot a_n = 1.$$

  [Corollary] For $a_1, \ldots, a_n \in \mathbb{Z}$, if $(a_1, \ldots, a_n) = 1$, there are $r_1, \ldots, r_n \in \mathbb{Z}$ such that

$$r_1 \cdot a_1 + \cdots + r_n \cdot a_n = 1.$$

Reminder: Field (体)

Definition 9

A commutative ring $(K, +, \cdot)$ is called a *field* if

- $(K - \{0\}, \cdot)$ is a commutative group (可換群),

where 0 denotes the identy of $(K, +)$.

- We write $K^{\times}$ to denote the set of the invertible elements in monoid $(K, \cdot)$.
- $(K, +, \cdot)$ is a field if and only if $K^{\times} = K - \{0\}$.
- $(K^{\times}, \cdot)$ is called the multicative group (乗法群) (of field $(K, +, \cdot)$).
- Let 1 be the identiy of $(K^{\times}, \cdot)$. Then, $1 \neq 0$ by definition.

Definition 10 (Characteristic)

The *characteristic* of field K, denoted $\mathrm{chr}(K)$, is defined to be the smallest positive integer p such that

$$\overbrace{1 + \cdots + 1}^{p} = 0.$$

If there is no such positive integer, then define $\mathrm{chr}(K) = 0$.

- The characteristics of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are 0.

Maximal Ideal (極大イデアル)

Let R be a ring (with 1).

Definition 11 (Maximal Ideal)

An ideal I in R is called *a maximal ideal* if $I \neq R$ and the only ideals containing I are I and R, i.e., there is no ideal $\tilde{I}$ such that $I \subsetneq \tilde{I} \subsetneq R$.

Theorem 1

For an ideal I in R, it holds that

$$I \text{ is a maximal ideal.} \quad \Longleftrightarrow \quad R/I \text{ is a field.}$$

Theorem 2

When R is a PID, I is a prime ideal $\Leftrightarrow$ I is a maximal ideal.

Hence, in a PID R,

p: irreducible $\Leftrightarrow$ p: a prime element $\Leftrightarrow$ (p): a prime ideal $\Leftrightarrow$ (p): a maximal ideal

Today's Contents

Polynomial Ring (多項式環)

Proposition 2

Let K be a field. Then the polynomial ring in X over K, denoted $K[X]$, is an Euclidean domain with $\lambda(f) = \deg(f)$.

Since an Euclidean domain is a PID, the following conditions are all equivalent:

- $f(X)$ is an irreducible polynomial in $K[X]$.
- $f(X)$ is a prime element in $K[X]$.
- $(f(X))$ is a prime ideal.
- $(f(X))$ is a maximal ideal.
- $K[X]/(f(X))$ is a field.

Finite Field (有限体) $\mathbb{F}_q$

- The order of $\mathbb{F}_q$, q, satisfies $q = p^r$ where p is prime and r is a positive integer.
- The characteristic of $\mathbb{F}_q$ is p, i.e., $\mathrm{chr}(\mathbb{F}_q) = p$.
- $\mathbb{F}_q$ is often written as $GF(q)$ in the area of the coding theory.
- $\mathbb{F}_p$ is called *a prime field* and $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.
- When $q = p^r$, for any monic irreducible $f(X) \in \mathbb{F}_p[X]$ of $\deg(f) = r$,

$$\mathbb{F}_q \cong \mathbb{F}_p[X]/f(X).$$

- (which implies that) any element in $\mathbb{F}_q$ can be represented as a polynomial of $r-1$ degree in $\mathbb{F}_p[X]$. The addition and multiplication operations can be defined as

$$a(X) + b(X) \triangleq a(X) + b(X) \bmod f(X), \quad \text{and}$$
$$a(X) \cdot b(X) \triangleq a(X) \cdot b(X) \bmod f(X),$$

respectively.

Today's Contents

Reminder: Ring (環)

Definition 12 (Axiom of Ring)

A *ring* $(R, +, \cdot)$ is called a *ring* if R is a set with two binary operations, $+$ and $\cdot$, on R, and satisfies the following axioms:

- R_1: $(R, +)$ is an Abelian group (or an additive group).
- R_2: $(R, \cdot)$ is a sem-group with the multiplicative identity 1 (i.e., a monoid).
- R_3 [Distributive]: For all $a, b, c \in R$, the following holds:

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \text{ and } a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Conventions:

- $(+, \cdot)$ are often called *addition* (加法) and *multiplication* (乗法), respectively.
- Denote by 0 the identiy of $(R, +)$, *the additive identity.*
- Denote by 1 the identity of $(R, \cdot)$, *the multiplicative identity.*

Reminder: Commutative Ring (可換環)

Definition 13

A ring $(R, +, \cdot)$ is called *commutative* if $(R, \cdot)$ is commutative, i.e.,

$$\forall a, b \in G \quad [a \cdot b = b \cdot a].$$

For commutative ring $(R, +, \cdot)$, the distibuted law R_3 (分配法則) is simplified as

$$\forall a, b, c \in R \quad [(a + b) \cdot c = (a \cdot c) + (b \cdot c)].$$

Reminder: Ideal (イデアル)

Definition 14 (イデアル)

A subset I of ring $(R, +, \cdot)$ is called *a left ideal* (左イデアル) if it satisfies (1) and (2), *a right ideal* (右イデアル) if it does (1) and (3), or *a (two-sided) ideal* ((両側) イデアル) if it does (1), (2), and (3).

1. $(I, +)$ is a subgroup of $(R, +)$.
2. $r \in R,\ x \in I \implies r \cdot x \in I$.
3. $r \in R,\ x \in I \implies x \cdot r \in I$.

- If R is a commutative ring, then any left or right ideal of R is trivially a two-sided ideal.
- $n\mathbb{Z}$ is an ideal of ring $\mathbb{Z}$, because
    - $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$ and for any $a \in \mathbb{Z}$ and $x \in n\mathbb{Z}$, it holds that $a \cdot x = x \cdot a \in n\mathbb{Z}$.
- $\{0\}$ and R are always two-sided ideals of any ring R.