[I216e] Computational Complexity and Discrete Mathematics

Ryuhei Uehara, and Eiichiro Fujisaki

Japan Advanced Institute of Science and Technology

November 8th, 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

1. Remindar:Groups, Ring, and Fields
2. Group Theory: Monoid and Its Properties
3. Group Theory: Subgroup (部分群) and Residue Class (剰余類)
4. Examples of Groups

Group (群)

Definition 1 (Axiom of Group)

Let G be a set and $\circ$ be a binary operation on G. $(G, \circ)$ is called a *group* if the it satisfies the following axioms:

- G_0 （二項演算） $\circ : G \times G \to G$ is a binary operation on G.
- G_1 （結合法則） $\forall a, b, c \in G \quad [(a \circ b) \circ c = a \circ (b \circ c)]$.
- G_2 （単位元の存在） $\exists e \in G, \forall a \in G \quad [a \circ e = e \circ a = a]$.
- G_3 （全て可逆元） $\forall a \in G, \exists a^{-1} \in G \quad [a \circ a^{-1} = a^{-1} \circ a = e]$.

- G_0: Magma (マグマ)
- G_0, G_1: Semi-group (半群)
- G_0, G_1, G_2: Monoid (単位的半群)

用語: 単位元 (Identiy); 可逆元 (invertible element, or unit (単元)); 逆元 (inverse).

Abelian Group (or Commutative Group)

Definition 2

Group $(G, \circ)$ is called *abelian* or *commutative* if the following holds:

- G_4 （可換律） $\forall a, b \in G \quad [a \circ b = b \circ a]$.

An Abelian group (or a commutative group (可換群)) is also known as the name of an *additive* group (加法群) with binary operation $+$, instead of $\circ$.

Definition 3 (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, i.e., $\forall a, b \in R \quad [(a \cdot b) \cdot c = a \cdot (b \cdot c)]$.
- R_3 [分配法則]: 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 $(R, +)$.
- Denote by 1 the identity of $(R, \cdot)$ (if it exists).

Definition 4

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

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

Field (体)

Definition 5

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.

Today's Contents

1. Remindar:Groups, Ring, and Fields
2. Group Theory: Monoid and Its Properties
3. Group Theory: Subgroup (部分群) and Residue Class (剰余類)
4. Examples of Groups

Monoid (単位的半群), Just reminder

Definition 6 (Semi-group (半群))

$(G, \circ)$ is called a semi-group if G is a set accociated with binary operation $\circ : G \times G \to G$ and the following holds.

- G_1（結合法則）: $\forall a, b, c \in G \quad [(a \circ b) \circ c = a \circ (b \circ c)]$.

Definition 7 (Monoid (単位的半群))

A semi-group $(G, \circ)$ is called a monoid (単位的半群) if:

- G_2（単位元）: it has an identiy $e \in G$.

Let's see what properties can be induced by a monoid.

From Monoid (1)

Let $(G, \circ)$ be a monoid.

Proposition 1 (Uniquness of Identity)

An idenity e is *unique*,
i.e., If there are two identies, e, e', then $e = e'$.

Proposition 2 (Uniqueness of Inverse)

An inverse of a, a^{-1}, is *unique* if a is an invertible element.

The above does not always hold for a magma $(G, \circ)$, which does not hold the associative law (結合法則).

Proposition 3

For an invertible element $a \in G$, the solution of $a \circ x = b$ is unique, in addition $x = a^{-1} \circ b$.

From Monoid (2)

Let $(G, \circ)$ be a monoid.

Proposition 4

The inverse of identity e is e.

Proposition 5

If $a, b \in G$ are both invertible, $a \circ b$ is also invertible, and

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

Proposition 6

If $a \in G$ is invertible, then a^{-1} is also invertible, and $(a^{-1})^{-1} = a$.

From Monoid (3)

Let $(G, \circ)$ be a monoid.
Let $G^\times$ be the set of the invertible elements in G.

Proposition 7

$(G^\times, \circ)$ turns out a group.

Definition 8

$(G^\times, \circ)$ is called the *unit group* (単元群).

NOTE: Propositions, 1 – 7, hold in any group because a group is a monoid. (The only difference is that $G^\times = G$ when $(G, \cdot)$ is a group.)

Today's Contents

1. Remindar:Groups, Ring, and Fields
2. Group Theory: Monoid and Its Properties
3. Group Theory: Subgroup (部分群) and Residue Class (剰余類)
4. Examples of Groups

Subgroup (部分群)

Definition 9

$(H, \circ)$ is called a *subgroup* of group $(G, \circ)$ if:

- $H \subseteq G$ (i.e., H is a subset of G).
- $\forall a, b \in H \quad [a \circ b \in H]$ (i.e., $\circ$ is a binary operation on H).
- $\forall a \in H \quad [a^{-1} \in H]$.

From now on, I often omit to write a binary operation if not confused.

Theorem 10

H is a subgroup of G if and only if

$$\forall a, b \in H \quad [a \circ b^{-1} \in H]$$

Residue class (剰余類) or Coset (傍系)

Definition 11

Let H be a subgroup of G. For $a \in G$, define

$$aH := \{a \circ h | h \in H\}$$
$$Ha := \{h \circ a | h \in H\}.$$

Then aH is called a *left coset* of H (in G), and Ha is called a *right coset* of H (in G).

- In Japanese, a left (resp. right) coset is called 左剰余類 (resp. 右剰余類).

Partitioning (分割)

Let H be a subgroup of G. Later (not today!), prove that

- (Left coset) $aH = bH \iff (a \in bH \text{ or } b \in aH)$
  $\iff (a \in bH \text{ and } b \in aH)$.
- (Right coset) $Ha = Hb \iff (a \in Hb \text{ or } b \in Ha)$
  $\iff (a \in Hb \text{ and } b \in Ha)$.

That is to say, there is a subset A of G such that $\{aH\}_{a\in A}$ is a *partition* of G, i.e., for all $a, b \in A$ $(a \neq b)$,

$$aH \bigcap bH = \emptyset \quad \text{and} \quad G = \bigcup_{a\in A} aH.$$

Similarly, there is a subset B of G such that $\{Hb\}_{b\in B}$ is a partition of G.

(Informal) Lagrange's Theorem

Theorem 12

Let H be a subgroup of G. By $|G|$ (resp. $|H|$), denote the order of G (resp. H). Then, it holds that $|G|$ is divided by $|H|$, i.e., $|H| \mid |G|$.

This is led by the statement that when $\{aH\}_{a \in A}$ is a partition of G, it holds that $|aH| = |H|$ for all $a \in A$.

Similarly, $|Hb| = |H|$ for any partition $\{Hb\}_{b \in B}$ and any $b \in B$.

Today's Contents

1. Remindar:Groups, Ring, and Fields
2. Group Theory: Monoid and Its Properties
3. Group Theory: Subgroup (部分群) and Residue Class (剰余類)
4. Examples of Groups

Examples of Groups

- $(\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$,..
- $(\mathbb{Z}, \times)$, $((\mathbb{Z}/n\mathbb{Z})^{\times}, \times)$, $(Q^{\times}, \times)$,..
- Triangle rotation group, symmetric group..