[I216e] Computational Complexity and Discrete Mathematics

Ryuhei Uehara, and Eiichiro Fujisaki

Japan Advanced Institute of Science and Technology

November 20th, 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. Normal Subgroup (正規部分群) and Residue Class Group (剰余類群)
2. Group Homomorphism (群準同型) and Group Isomorphism (群同型)
3. Fundamental Homomorphism Theorem (群の準同型定理)
4. Ideal (イデアル) and Residue Class Ring (剰余類環)
5. Fundamental Ring Homomorphism Theorem (環準同型定理)
6. Chinese Remainder Theorem (中国人の剰余定理)
7. Extended Euclidean Algorithm (拡張ユークリッドの互除法)
8. Appendix (Reminder)

How to Define Binary Operation on Quotient Set?

Let H be a subgroup of $(G, \circ)$. Define a new operation $\star$ on G/H as follows:

$$aH \star bH \triangleq \{(a \circ h_i) \circ (b \circ h_j) | h_i, h_j \in H\}.$$

We want $\star$ to be a binary operation. So, we want to hold

$$cH = aH \star bH$$

for some $c \in G$. *However, it is not the case (for arbitrary group G and subgroup H)*.

Normal Subgroup (正規部分群)

Definition 1 (Normal Subgroup)

Let H be a subgroup of G. We say that H is *a normal subgroup* of G if for all $a \in G$, it holds that

$$aH = Ha.$$

We often write $H \lhd G$ to denote that H is a normal subgroup of G.

By definition, left coset (左剰余類) aH and right coset (右剰余類) Ha are the same subset of G if H is a normal subgroup. Hence, G/H and $G \backslash H$ are the same partition of G.

More importantly, it holds that (proven later)

$$aH \star bH = (a \circ b)H,$$

and hence, $\star$ is a binary operation!

[Note] We often write a normal subgroup as N (instead of H) and often abusely use $\circ$ as $\star$ on G/H.

Property of Normal Subgroup (1)

Theorem 1

Let N be a subgroup of G. Then, all the following conditions are equivalent:

1. N is a normal subgroup of G.
2. For all $a \in G$, $aN = Na$.
3. For all $a \in G$, $aN \subset Na$.
4. For all $a \in G$, $Na \subset aN$.
5. For all $a \in G$, $N = aNa^{-1}$.
6. For all $a \in G$, $N \subset aNa^{-1}$.
7. For $a \in G$, $aNa^{-1} \subset N$.

Property of Normal Subgroup (2)

Show that if $aN = Na$ for all $a \in G$, then $N = aNa^{-1}$.

Proof.

- $\forall n \in N, \exists n' \in N,$

  $$n = (a \circ a^{-1}) \circ n \circ (a \circ a^{-1}) = a \circ n' \circ a^{-1} \circ a \circ a^{-1} = a \circ n' \circ a^{-1} \in aNa^{-1}.$$

  Hence, $N \subset aNa^{-1}$
- $\forall n \in N, \exists n' \in N,$

  $$a \circ n \circ a^{-1} = n' \circ a \circ a^{-1} = n \in N.$$

  Hence, $aNa^{-1} \subset N$.

Therefore, it holds $N = aNa^{-1}$. □

Try to prove all the remaining directions by yourself.

Residue Class Group (剰余類群)

Let N be a normal subgroup of G. Then $G/N = G\backslash N$, because $aN = Na$ for all $a \in G$. We say that $aN(= Na)$ is *a coset or residue class of* G.

Theorem 2

$G/N(= G\backslash N)$ is a group, which is called *a residue class group.*

See $\star$ is a binary operation on G/H. Indeed, $aN \star bN$ turns out $(a \circ b)N$ as follows:

- $\forall h, h' \in N, \exists \hat{h} \in N,$

  $$(a \circ h) \circ (b \circ h') = a \circ (h \circ b) \circ h' = a \circ (b \circ \hat{h}) \circ h' \in (a \circ b)N.$$

  Hence, $aN \star bN \subset (a \circ b)N$.

- $$(a \circ b)N = a \circ (bN) = a \circ e \circ bN \subset aN \star bN$$

  Hence, $(a \circ b)N \subset aN \star bN$.

Therefore, $aN \star bN = (a \circ b)N$.

Proof of Theorem 2.

$G/H(= G\backslash H)$ is a group, because:

- G_0: $\star$ is a binary operation on G/N. (Already shown!)
- G_1: The associative law (結合法則) holds. (Omit)
- G_2: eN is the identity of G/N, because

$$aN \star eN = (a \circ e)N = aN$$

- G_3: The inverse of aN is $a^{-1}N$, because

$$aN \star a^{-1}N = (a \circ a^{-1})N = eN$$

Prove by yourself that the associative law holds.

The Integers Modulo n: $\mathbb{Z}/n\mathbb{Z}$, again

As a residue class group: $(\mathbb{Z}/n\mathbb{Z}, +)$.

- Binary operation, addition "+", on $\mathbb{Z}/n\mathbb{Z}$:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \triangleq \{a + \alpha + b + \beta \mid \alpha, \beta \in n\mathbb{Z}\},$$

- $(\mathbb{Z}/n\mathbb{Z}, +)$ is an additive group. So, $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.
- Hence, $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$.
- Note: $(a + b) + n\mathbb{Z} = (a + b \bmod n) + n\mathbb{Z}$.

As a partition of $\mathbb{Z}$: $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z}\}_{a \in Zn}$ where $Zn = \{0, 1, \ldots, n-1\}$ is called *a complete system of representatives (for the coset of $n\mathbb{Z}$ in $\mathbb{Z}$)* (完全代表系).

Today's Contents

Group Homomorphism (群準同型)

Let $(G, \circ)$ and $(G', \cdot)$ be groups. Let $f : G \to G'$ be a map from G to G'. Let e, e' be the identities of G, G', respectively.

Definition 2 (Homomorphism (準同型写像))

We say that $f : G \to G'$ is *homomorphic* if for all $x, y \in G$, it holds that $f(x \circ y) = f(x) \cdot f(y)$.

Property of Group Homomorphism

Proposition 1

Let e and e' be the identities of G and G', respectively. If $f : G \to G'$ is homomorphic, then $f(e) = e'$.

Proposition 2

If $f : G \to G'$ is homomorphic, then for all $x \in G$, it holds that $f(x^{-1}) = f(x)^{-1}$.

Proposition 3

If $f : G \to G'$ is homomorphic, then $\mathrm{Im}(f)$ is a subgroup of G'.

Proofs

Proof of Propostion 1.

Since $e \circ e = e$ and f is homomorphic, $f(e) = f(e \circ e) = f(e) \cdot f(e)$. Act $f(e)^{-1}$ on the both sides, then $e' = f(e)$. □

Proof of Proposition 2.

By definition, $x \circ x^{-1} = e$ for all $x \in G$. Hence, $f(x \circ x^{-1}) = f(x) \cdot f(x^{-1}) = f(e) = e'$. Then act $f(x)^{-1}$ from the left on the both sides of $f(x) \cdot f(x^{-1}) = e'$. Then, we have $f(x^{-1}) = f(x)^{-1}$. □

Proof of Proposition 3.

Omit. Prove by yourself. □

Group Isomorphism (群の同型)

Let $(G, \circ)$ and $(G', \cdot)$ be groups.

Definition 3 (Isomorphism Map (同型写像))

$f : G \to G'$ is *isomorphic* if $f : G \to G'$ is bijective and homomorphic. Then, we say that G and G' are isomorphic, denote by $G \cong G'$.

Definition 4 (Kernel (核))

Let $\mathrm{Ker}(f) \triangleq \{x \in G \mid f(x) = e' \in G'\}$, which is called *the kernel* of f.

Proposition 4

A homomorphism map $f : G \to G'$ is isomorphic if $\mathrm{Im}(f) = G'$ and $\mathrm{Ker}(f) = \{e\}$.

Proof of Proposition 4

It surfices to show that homomorphic f is bijective. f is surjective because of $\mathrm{Im}(f) = G'$. f is injective if

$$\forall x_1, x_2 \in G \quad \Big(f(x_1) = f(x_2) \quad \Longrightarrow \quad x_1 = x_2 \Big)$$

which can be shown as follows: By f being homomorphic and the fact that $f(x^{-1}) = f(x)^{-1}$, the above condition is equivalent to

$$\forall x_1, x_2 \in G \quad \Big(f(x_1 \circ {x_2}^{-1}) = e' \quad \Longrightarrow \quad x_1 \circ {x_2}^{-1} = e \Big).$$

This implies that (let $x_1 = x$ and $x_2 = e$)

$$\forall x \in G \quad \Big(f(x) = e' \quad \Longrightarrow \quad x = e \Big)$$

This condition is equivalent to $\mathrm{Ker}(f) = \{e\}$.

Today's Contents

Fundamental Homomorphism Theorem (群の準同型定理)

Theorem 3 (Fundamental Homomorphism Theorem)

Let $f : G \to G'$ be a homomorphism map from group G to group G'. Then, all the followings hold.

1. $\mathrm{Im}(f)$ is a subgroup of G'.
2. $\mathrm{Ker}(f)$ is a normal subgroup of G.
3. $\bar{f} : x \circ \mathrm{Ker}(f) \in G/\mathrm{ker}(f) \mapsto f(x) \in G'$ is homomorphic, and it holds that
$$G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$
In particular, when $\mathrm{Im}(f) = G'$ (surjective), $G/\mathrm{Ker}(f) \cong G'$.

Proof.

1. $\mathrm{Im}(f)$ is a subgroup of G'. Omit.
2. $\mathrm{Ker}(f)$ is a normal subgroup of G, because: For all $a \in G$, all $x \in \mathrm{Ker}(f)$,

$$f(a \circ x \circ a^{-1}) = f(a) \cdot f(x) \cdot f(a^{-1}) = f(a) \cdot e' \cdot f(a)^{-1} = e'.$$

   Hence, for all $a \in G$, it holds that $a \circ \mathrm{Ker}(f) \circ a^{-1} \subset \mathrm{Ker}(f)$. This implies that $\mathrm{Ker}(f)$ is a normal subgroup of G.
3. Go to next page.

Proof (Cont.)

Since $N := \text{Ker}(f)$ is a normal subgroup,

$$\bar{f} : xN \in G/N \mapsto f(x) \in G'$$

is homomorphic, because

$$\bar{f}((xN) \circ (yN)) = \bar{f}((x \circ y)N) = f(x \circ y) = f(x) \cdot f(y).$$

Think of $\bar{f}(xN) = \bar{f}(yN) \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x \circ y^{-1}) = e' \Leftrightarrow$ $x \circ y^{-1} \in N(:= \text{Ker}(f)) \Leftrightarrow x \in yN \Leftrightarrow xN = yN$. Hence,

$$\bar{f}(xN) = \bar{f}(yN) \Longrightarrow xN = yN,$$

which means $\bar{f}$ is injective and hence, $G/\text{Ker}(f) \cong \text{Im}(f)$. In particular if $\text{Im}(f) = G'$, then $G/\text{Ker}(f) \cong G'$. *Quod erat demonstrandum* (Q.E.D.)

Direct Product of Groups (群の直積)

Let $(G_1, \cdot_1), \ldots, (G_n, \cdot_n)$ be groups. Define the direct product of $G_1, \ldots, G_2$ as

$$G_1 \times \cdots \times G_n \triangleq \{(x_1, \ldots, x_n) \mid x_1 \in G_1, \ldots, x_n \in G_n\}.$$

Define a binary operation $\circ$ on $G_1 \times \cdots \times G_n$ as

$$(x_1, \ldots, x_n) \circ (x_1', \ldots, x_n') \triangleq (x_1 \cdot_1 x_1', \ldots, x_n \cdot_n x_n').$$

Then, $G_1 \times \cdots \times G_n$ turns out a group (under binary operation $\circ$).

Applications (1)

In general, it is not easy to show two groups are isomorphic. The Fundamental Homomorphism Theorem is a very useful tool for investigating such problems.

- From a map $x \in \mathbb{Z} \mapsto i^x \in \mathbb{C}^\times (= \mathbb{C} - \{0\})$, it is shown that

  $$\mathbb{Z}/4\mathbb{Z} \cong \langle i \rangle,$$

  where $\mathbb{Z}/4\mathbb{Z}$ is an additive group under $+$. Generally speaking, if the order of a is n where a is an element in some group,

  $$\mathbb{Z}/n\mathbb{Z} \cong \langle a \rangle.$$

- By $x \mapsto e^{2\pi \imath x}$, define a map from $(\mathbb{R}, +)$ to $(\mathbb{C}^\times, \cdot)$.

  $$\mathbb{R}/\mathbb{Z} \cong T := \{z \in \mathbb{C}^\times \mid |z| = 1\}.$$

Applications (2)

- Let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices whose entries are real numbers. Let $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$, and $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) = 1\}$.
  By $\det : M_n(\mathbb{R}) \to \mathbb{R}^\times$, it holds that
  $$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times.$$
- Define a map from $(\mathbb{Z}, +)$ to $(\mathbb{Z}/p_i\mathbb{Z}, +)$ as
  $$x \mapsto (x \bmod p_i) + p_i\mathbb{Z}.$$
  Let $n = n_1 \cdot n_2 \cdots n_\ell$, where $n_1, \ldots, n_\ell$ are relatively prime to the others. Then, it holds that
  $$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_\ell\mathbb{Z},$$
  where $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n_1\mathbb{Z}, \ldots, \mathbb{Z}/n_\ell\mathbb{Z}$ are additive groups under $+$.

Today's Content

Reminder: Ring (環)

Definition 5 (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 6

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

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

Property of Ring

Let $(R, +, \cdot)$ be a ring and 0 denotes the identity of $(R, +)$.

Proposition 5

Fro all $r \in R$, it holds that

$$r \cdot 0 = 0 \cdot r = 0.$$

For all $a \in R$, $a + 0 = a$. Hence, $r \cdot (a + 0) = r \cdot a + r \cdot 0$ and $r \cdot (a + 0) = r \cdot a$, which implies $r \cdot a + r \cdot 0 = r \cdot a$. By adding $-(r \cdot a)$ in both sides, we have $r \cdot 0 = 0$. Similarly, by $0 + a = a$, we have $0 \cdot r = 0$.

Ideal (イデアル)

Definition 7 (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.

Subring (部分環)

Definition 8 (Subring (部分環))

Let S be a subset of ring $(R, +, \cdot)$. S is called *a subring* of R if the follwing conditions hold:

- $(S, +)$ is a subgroup of $(R, +)$,
- $\cdot$ is a binary operation on S, i.e., $a, b \in S \implies a \cdot b \in S$, and
- $1 \in S$.

- If (two-sided) ideal I is a subring of R, then $I = R$, because $1 \in I$.
  - For instance, ideal $n\mathbb{Z}$.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ ($\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$) are all subrings of $\mathbb{C}$.

Define Multiplication on R/I

Let I be a left (or right) ideal of R. Then $(I, +)$ is a normal subgroup of $(R, +)$, because $(R, +)$ is an additive group. So, R/I is a residue class group, where $r + I \triangleq \{r + i \,|\, i \in I\}$ $(r \in R)$ is a coset (or a residue class). Define a multiplication operation $\cdot$ on R/I as

$$(r + I) \cdot (s + I) \triangleq \{(r + i) \cdot (s + i') \,|\, i, i' \in I\}.$$

We want to hold for all $r, s \in R$, there is $t \in R$ such that

$$(r + I) \cdot (s + I) = t + I,$$

which implies $\circ$ is a binary operation on R/I.
If I is a two-sided ideal of R, then we indeed have

$$(r + I) \cdot (s + I) = (r \cdot s) + I.$$

Residue Class Ring (剰余類環)

Theorem 4 (Residue Class Ring (剰余類環))

Let I be an ideal of ring $(R, +, \cdot)$. Since $(R, +)$ is a normal subgroup of $(I, +)$, R/I is a residue class group. Define the multiplication on R/I as

$$(r + I) \cdot (s + I) \triangleq \{(r + i) \cdot (s + i') \mid i, i' \in I\}.$$

Then, it holds $(r + I) \cdot (s + I) = r \cdot s + I$, and R/I is a ring, called *a residue class ring* (剰余類環).

- The addition on R/I is defined as

  $$(r + I) + (s + I) \triangleq \{(r + i) + (s + i') \mid i, i' \in I\},$$

  and it holds $(r + I) + (s + I) = (r + s) + I$.
- If R is commutative, then R/I is also commutative.

The Integers Modulo n: $\mathbb{Z}/n\mathbb{Z}$, again and again

As a residue class ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

- Binary operation, addition "+", on $\mathbb{Z}/n\mathbb{Z}$:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \triangleq \{a + \alpha + b + \beta \mid \alpha, \beta \in n\mathbb{Z}\},$$

  which results in $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$, because $n\mathbb{Z} \lhd \mathbb{Z}$.
- Note: $(a + b) + n\mathbb{Z} = (a + b \bmod n) + n\mathbb{Z}$.

- Binary operation, multiplication "$\cdot$", on $\mathbb{Z}/n\mathbb{Z}$:

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) \triangleq \{(a + \alpha) \cdot (b + \beta) \mid \alpha, \beta \in n\mathbb{Z}\},$$

  which results in $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (a \cdot b) + n\mathbb{Z}$, since $n\mathbb{Z}$ is an *ideal*.
- Note: $(a \cdot b) + n\mathbb{Z} = (a \cdot b \bmod n) + n\mathbb{Z}$.

Ring Product

Let $R_1, \ldots, R_n$ be rings. Define the product of them as

$$R_1 \times \cdots \times R_n \triangleq \{(x_1, \ldots, x_n) \mid x_1 \in R_1, \ldots, x_n \in R_n\}.$$

Define binary operations on it as

$$(x_1, \ldots, x_n) + (x_1', \ldots, x_n') \triangleq (x_1 + x_1', \ldots, x_n + x_n')$$
$$(x_1, \ldots, x_n) \cdot (x_1', \ldots, x_n') \triangleq (x_1 \cdot x_1', \ldots, x_n \cdot x_n')$$

Then it is a ring.

The zero element 0 in $R_1 \times \cdots \times R_n$ is $(0_{R_1}, \ldots, 0_{R_n})$. If each ring, R_i, has 1_i, The product also has 1, which is $(1_{R_1}, \ldots, 1_{R_n})$.

Properties of Ring Product

Proposition 6

$(R_1 \times \cdots \times R_n)^\times = R_1^\times \times \cdots \times R_n^\times$.

Generally, for monoid $G_1, \ldots, G_n$, $(G_1 \times \cdots \times G_n)^\times = G_1^\times \times \cdots \times G_n^\times$.

Proposition 7

If $R \cong R_1 \times \cdots \times R_n$, then $R^\times = R_1^\times \times \cdots \times R_n^\times$.

Show $R^\times \cong (R_1 \times \cdots \times R_n)^\times$. Then it holds by Proposition (6).

Proposition 8

$(0_{R_1}, \ldots, R_i, \ldots, 0_{R_n})$ is an ideal in product ring $(R_1 \times \cdots \times R_n)$.

Even for non-commutative $R_1, \cdots, R_n$, $(0_{R_1}, \ldots, R_i, \ldots, 0_{R_n})$ is a (two-sided) ideal.

Today's Contents

Ring Homomorphism (環の準同型)

Let R and R' be rings with multicative identities, 1 and $1'$, respectively. Let $f : R \to R'$ be a map from R to R'.

Definition 9 (Ring Homomorphism)

for all $x, y \in R$, if

$$f(x+y) = f(x) + f(y), \quad f(x \cdot y) = f(x) \cdot f(y), \text{ and } f(1) = 1',$$

then f is called a ring homomorphism map. In particular, f is called an isomorphism map (同型写像) if it is bijective. If $f : R \to R'$ is isomorphic, we say that R, R' are isomorphic, denote by $R \cong R'$.

- NOTE: It is not led by the first two equations that $f(1) = 1'$. Hence needed.
- $\text{Im}(f) = \{f(x) \mid x \in R\}$ is the image of f.
- $\text{Ker}(f) = \{x \in R \mid f(x) = 0' \in R'\}$ is the kernel of f.

Fundamental Ring Homomorphism Theorem (環の準同型定理)

Theorem 5 (Fundamental Ring Homomorphism Theorem)

Let $f : R \to R'$ be ring homomorphic. Then,

1. $\mathrm{Im}(f) = \{f(x) \mid x \in R\}$ is a subring of R'.
2. $\mathrm{Ker}(f) = \{x \in R \mid f(x) = 0' \in R'\}$ is a (two-sided) ideal of R.
3. $\bar{f} : x + \mathrm{Ker}(f) \in R/\ker(f) \mapsto f(x) \in R'$ is ring homomorphic and it holds that
$$R/\mathrm{Ker}(f) \cong \mathrm{Im}(f).$$
If $\mathrm{Im}(f) = R'$ (全射), then $G/\mathrm{Ker}(f) \cong R'$.

$\mathbb{Z}/n\mathbb{Z}$

Let $n = p_1 \cdots p_\ell$, where $p_1 \ldots p_\ell$ are relatively prime.
For $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/p_1\mathbb{Z}$, $\ldots$, $\mathbb{Z}/p_\ell\mathbb{Z}$, by Fundamental Homomorphism Theorem and Proposition 7,

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z} \\ (\mathbb{Z}/n\mathbb{Z})^\times &\cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^\times \end{aligned}$$

Therefore, for

$$x \in (\mathbb{Z}/n\mathbb{Z})^\times \leftrightarrow (x_1, \ldots, x_\ell) \in (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^\times$$

and

$$y \in (\mathbb{Z}/n\mathbb{Z})^\times \leftrightarrow (y_1, \ldots, y_\ell) \in (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^\times,$$

it holds that

$$x \cdot y \leftrightarrow (x_1 \cdot y_1, \ldots, x_\ell \cdot y_\ell).$$

Today's Contents

Reminder: Chinese Remainder Theorem (中国人の剰余定理)

- In Sunzi Suanjing (「孫子算経」): What is that integer when divided by 3 is remainder 2; divided by 5 is remainder 3; and divided by 7 is remainder 2.

$$x = 2 \bmod 3$$
$$x = 3 \bmod 5$$
$$x = 2 \bmod 7$$

- For $n = p_1 p_2 \cdots p_k$ (such that for every p_i, p_j $(i \neq j)$, $(p_i, p_j) = 1$), it holds

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}. \quad \text{(isomorphism)}$$

The CRT gives the concrete map ψ.

$$\psi : \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

CRT

Thanks to Fundamental Ring Homomorphism theorem, we can show

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

- Define $f : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ as

  $$f(x) := \Big([x]_3, [x]_5, [x]_7\Big),$$

  where $[x]_n \triangleq x + n\mathbb{Z}$.
- Show f is ring homomorphic.
- Show $\mathrm{Im}(f) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ and $\mathrm{Ker}(f) = 105\mathbb{Z}$ $(105 = 3 \cdot 5 \cdot 7)$.
- Then, the above holds.

Solution

For $n = p_1 \cdot p_2 \cdots p_\ell$ such that each p_i is relatively prime, let $\chi_1, \ldots, \chi_\ell$ be integers such that

$$\frac{n}{p_1}\chi_1 + \frac{n}{p_2}\chi_2 + \cdots + \frac{n}{p_\ell}\chi_\ell = 1 \tag{1}$$

In general, for any $a_1, \ldots, a_n \in \mathbb{Z}$ such that $(a_1, \ldots, a_n) = 1$, the following equation has a solution of integers,

$$a_1 X_1 + \cdots + a_n X_n = 1.$$

Since each p_i is relatively prime, it holds that $(\frac{n}{p_1}, \ldots, \frac{n}{p_\ell}) = 1$ and hence, there are $\chi_1, \ldots, \chi_\ell \in \mathbb{Z}$, satisfying (1).
Then, $f^{-1} : \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_\ell\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is led by

$$f^{-1}(x_1, \ldots, x_\ell) = x_1 \frac{n}{p_1}\chi_1 + x_2 \frac{n}{p_2}\chi_2 + \cdots + x_n \frac{n}{p_\ell}\chi_\ell.$$

Solution (Cont.)

f^{-1} is indeed the inverse map of f.

$$x \in \mathbb{Z}/n\mathbb{Z} \quad \overset{f}{\longrightarrow} \quad \underset{\longleftarrow}{f^{-1}} \quad (x_1, \ldots, x_\ell) \in \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z}$$

It can be shown as follows: Since

$$\frac{n}{p_i}\chi_i = 1 \pmod{p_i}, \qquad \frac{n}{p_j}\chi_j = 0 \pmod{p_i} \quad (j \neq i),$$

it holds that

$$x_i \equiv x_1\frac{n}{p_1}\chi_1 + \cdots + x_i\frac{n}{p_i}\chi_i + \cdots + x_n\frac{n}{p_\ell}\chi_\ell \pmod{p_i}$$

Therefore, for $x = x_1\frac{n}{p_1}\chi_1 + x_2\frac{n}{p_2}\chi_2 + \cdots + x_i\frac{n}{p_i}\chi_i + \cdots + x_n\frac{n}{p_\ell}\chi_\ell$, it holds that $f(x) = ([x_1]_{p_1}, \ldots, [x_\ell]_{p_\ell})$.

Solution of Sunzi Suanjing

Let $f : \mathbb{Z}/105\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ be a canonical isomorphism map. Then, f^{-1} is shown as

$$f^{-1}(x_3, x_5, x_7) = \left[-35x_3 + 21x_5 + 15x_7\right]_{105},$$

where we use $35 \cdot (-1) + 21 \cdot 1 + 15 \cdot 1 = 1$.
Since $x_3 = 2$, $x_5 = 3$, $x_7 = 2$,

$$f^{-1}(2, 3, 2) = [23]_{105} = 23 + 105\mathbb{Z}.$$

Extension

Let X be an integer such that divided by 3 is remainder 2; divided by 5 is remainder 3; divided by 7 is remainder 2. Let Y be an integer such that divided by 3 is remainder 1; divided by 5 is remainder 2; divided by 7 is remainder 5. Then, what is $XY \bmod 105$?

Extension

Let X be an integer such that divided by 3 is remainder 2; divided by 5 is remainder 3; divided by 7 is remainder 2. Let Y be an integer such that divided by 3 is remainder 1; divided by 5 is remainder 2; divided by 7 is remainder 5. Then, what is $XY \bmod 105$?

By Fundamental Ring Homomorphism Theorem, it can be easily computed.

Extension

Let X be an integer such that divided by 3 is remainder 2; divided by 5 is remainder 3; divided by 7 is remainder 2. Let Y be an integer such that divided by 3 is remainder 1; divided by 5 is remainder 2; divided by 7 is remainder 5. Then, what is XY mod 105 ?

By Fundamental Ring Homomorphism Theorem, it can be easily computed.

$$\begin{aligned} &(2 \cdot 1 \bmod 3) \cdot (-35) + (3 \cdot 2 \bmod 5) \cdot 21 + (2 \cdot 5 \bmod 7) \cdot 15 \\ =&2 \cdot (-35) + 1 \cdot 21 + 3 \cdot 15 = -4. \end{aligned}$$

The answer is $[-4]_{105} = [101]_{105}$.

Today's Contents

Euclidean Algorithm (ユークリッドの互除法)

The Euclidean Algorithm is a famous algorithm that takes $a, b \in \mathbb{N}$ as input, and outputs (a, b). For all $k \in \mathbb{Z}$ such that $a - kb \geq 0$, it holds that

$$(a, b) = (a - kb, b).$$

By definition, it is obvious that $(a, b) = (b, a)$.

Euclidean Algorithm:

- (Step 0) Take (a, b) $(a \geq b)$.
- (Step 1) Set $(a, b) := (b, a \bmod b)$.
- (Step 2) By iterating Step1, a, b go smaller.
- (Step 3) Finally when it goes to $(d, 0)$, output d, which is (a, b).

Extended Euclidean Algorithm

It solves $aX + bY = d$ for $a, b \in \mathbb{N}$. There are solution $(X, Y) \in \mathbb{Z}^2$ if and only if $d = (a, b)$.

Extended Euclidean Algorithm

- (Step 0) Take (a, b) $(a \geq b)$ as input. Set $(a_0, b_0) := (a, b)$ and $i := 0$.
- (Step 1) Set $(X_i, Y_i) = (1, 0)$ and $(X_i', Y_i') = (0, 1)$, which implicitly represents $a = a_0 X_i + b_0 Y_i$ $(X = 1, Y = 0)$ and $b = a_0 X_i' + b_0 Y_i'$ $(X' = 0, Y' = 1)$ when $i = 0$.
- (Step 2) Compute quotient k and remainder $r (= a \bmod b)$ such that $a = kb + r$, which implies $r = a - kb = a(X_i - kX_i') + b(Y_i - kY_i')$. Set $(a, b) := (b, r)$.
- (Step 3) Set as follows:

$$(X, Y) := (X_i', Y_i'), \quad (X', Y') := (X_i - kX_i', Y_i - kY_i')$$

  Note that $a = a_0 X + b_0 Y$, $b = a_0 X' + b_0 Y'$.
- (Step 4) Set $i := i + 1$. Set $(X_i, Y_i) := (X, Y)$ and $(X_i', Y_i') := (X', Y')$.
- Repeat from (Step 2) to (Step 4). a, b go smaller.
- Finally when (a, b) goes to $(d, 0)$ where $d = (a, b)$, output d along with (X, Y), which satisfying $d = a_0 X + b_0 Y$.

What Extended Euclidean Algorithm means

What Extended Euclidean Algorithm solves

- Solution of linear equation $aX + bY = d$ for $d = (a, b)$.
- Soultion of the inverse of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Indeed, X such that $aX \equiv 1 \pmod{n}$ can be obtained by the solution of $aX + nY = 1$.

It can be extended for the solution of $a_1X_1 + \cdots + a_nX_n = d$ where $d = (a_1, \ldots, a_n)$.

- By observing $(a_1, \ldots, a_{n-1}, a_n) = \Big((a_1 - k_1a_n), \ldots, (a_{n-1} - k_{n-1}a_n), a_n\Big)$, you can apply the similar technique to that case.
- Let's set variables as above.

Today's Contents

Group (群)

Definition 10 (Axiom of Group)

Let G be a set associated with a binary operation $\circ$. G is called a *group* if the it satisfies the following axioms:

- G_0 (Binary Operation) $\circ : G \times G \to G$ is a binary operation on G.
- G_1 (Associative) $\forall a, b, c \in G \quad [(a \circ b) \circ c = a \circ (b \circ c)]$.
- G_2 (Identity) $\exists e \in G, \forall a \in G \quad [a \circ e = e \circ a = a]$.
- G_3 (Invertible) $\forall a \in G, \exists a^{-1} \in G \quad [a \circ a^{-1} = a^{-1} \circ a = e]$.

- 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)

Definition 11

Group G is called *abelian* or *commutative* if the following condition holds:

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

Subgroup (部分群)

Definition 12

H is called a *subgroup* of group G 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).
- $\forall a \in H \quad [a^{-1} \in H]$.

Theorem 6

H is a subgroup of G if and only if

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

Cyclic Group (巡回群)

Let G be a group. For $a \in G$, define $a^n \triangleq \overbrace{a \circ \cdots \circ a}^{n}$ and write $\{\ldots, a^{-1}, a^0, a^1, \ldots\}$ as $\langle a \rangle$, i.e., $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

Theorem 7

$\langle a \rangle$ is a subgroup of G.

- Even for non-commutative G, $\langle a \rangle$ is a commutative group.
- $\langle a \rangle$ is called *a cyclic group*.
- a is called *a generator* of $\langle a \rangle$. In general, a is not unique.

Definition 13

The smallest positive number n such that $a^n = 1$ (where 1 is the identity) is called *the order* of a. If such a positive number does not exist, the order of a is said *infinite*.

The order of a is equivalent to the order of $\langle a \rangle$.

Left/Right Cosets and Quoticient Sets

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

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

We call aH *a left coset* (左剰余類) of H and Ha *a right coset* (右剰余類) of H. The collection of all the left/right cosets of H, $\{aH\}_{a\in G}$ and $\{Ha\}_{a\in G}$, *partition* G, under the corresponding equivalent relations, $\sim_{H,left}$ and $\sim_{H,right}$.

- $\sim_{H,left} \iff a^{-1} \circ b \in H$ (or equivalently $aH = bH$).
- $\sim_{H,right} \iff a \circ b^{-1} \in H$ (or equivalently $Ha = Hb$).

Then, We write the quotient sets, $G/{\sim_{H,left}}$ and $G/{\sim_{H,right}}$ as follows:

- G/H to denote $\{aH\}_{a\in G}$.
- $G\backslash H$ to denote $\{Ha\}_{a\in G}$.

Index (指数) of Subgroup

Theorem 8

$$|G/H| = |G\backslash H|.$$

If G is commutative, then trivial. However, the above holds even for any group G and any subgroup H.

Proof.

1. $a \in G \mapsto a^{-1} \in G$ is bijective (全単射) (due to the uniquenss of inverse in Monoid).
2. So, $ah \mapsto (ah)^{-1} = h^{-1} \circ a^{-1}$ is bijective and hence $aH = Ha^{-1}$.
3. There is a subset A of G such that $\{aH\}_{a \in A}$ partitions G and for all $a, b \in A$ $(a \neq b)$, $aH \bigcap bH = \emptyset$.
4. By $aH = Ha^{-1}$, $\{Ha^{-1}\}_{a \in A}$ also partions G. Since $aH = Ha^{-1}$, $\{aH\}_{a \in A}$ and $\{Ha^{-1}\}_{a \in A}$ are the same partion of G.
5. Hence, $|A| = |G/H| = |G\backslash H|$. Regardless of the choice of A, G/H and $G\backslash H$ are unique.

□

NOTE: A is called a complete system of representatives for the left coset of H in G.

Definition 14

We say that $[G : H] \triangleq |G/H| = |G\backslash H|$ is *the index of H in G*.

Theorem 9 (Lagrange's Theorem)

Let H be a subset of G. Then,

- $|G| = [G : H]|H|$.
- Let G be a finite group. Then, the order of H divides the order of G, i.e., $|H|$ divides $|G|$.

Proof.

Let $\{aH\}_{a \in A}$ be the partion of G by the left coset of H such that for all $a, b \in A$ $(a \neq b)$, $aH \bigcap bH = \emptyset$. Then $[G : H] = |A|$. For all $a \in A$, $h (\in H) \mapsto ah (\in aH)$ is bijective. Therefore, $|G| = [G : H]|H|$. □

Map (写像)

Let S and S' be sets. Denote by $f : S \to S'$ to show a map from S to S'.

Definition 15 (Image (像))

Let $\mathrm{Im}(f) \triangleq \{f(x) \mid x \in S\}$, which is called *the image* of S by f.

By definition, $\mathrm{Im}(f) \subseteq S'$.

Definition 16 (Surjective (全射))

If $\mathrm{Im}(f) = S'$, f is called *surjective*.

Definition 17 (Injective (単射))

For all $x, x' \in S$ $(x \neq x')$, if $f(x) \neq f(x')$, then f is called *injective*.

Definition 18 (Bijective (全単射))

If f is both surjective and injective, then it is called *bijective*.

Field (体)

Definition 19

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.