[I216e] Computational Complexity and Discrete Mathematics

Ryuhei Uehara, and Eiichiro Fujisaki

Japan Advanced Institute of Science and Technology

November 15th, 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

Reminder: Lagrange's Theorem

Theorem 1 (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, $|G| = [G : H]|H|$. □

Fermat's Little Theorem

Theorem 2 (Fermat's Little Theorem)

Let p be a prime. For $a \in \mathbb{N}$, the following holds.

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof.

$(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$ and $\langle a \rangle$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's Theorem, the order of a (i.e., the order of $\langle a \rangle$) divides $p-1$. Hence, $a^{p-1} = 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$. □

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

- Binary operations, addition "$+$" and multiplication "$\cdot$", on $\mathbb{Z}/n\mathbb{Z}$:

$$a + b \triangleq a + b \bmod n \quad \text{and} \quad a \cdot b \triangleq a \cdot b \bmod n.$$

- $(\mathbb{Z}/n\mathbb{Z})^\times$: The set of *invertible elements* in $\mathbb{Z}/n\mathbb{Z}$ under the multiplication "$\cdot$" (An element a is invertible if and only if there is the inverse a^{-1} such that $a \cdot a^{-1} = 1$).
- $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible (under $\cdot$) if and only if $(a, n) = 1$.
- The inverse of $a \in \mathbb{Z}/n\mathbb{Z}$ can be efficiently computed via Extended Euclidian Algorithm.
- Finding (X, Y) such that $aX + nY = 1$ implies finding the inverse of $a \in \mathbb{Z}/n\mathbb{Z}$. Indeed, $a^{-1} = X \pmod{n}$.
- The order of $(\mathbb{Z}/n\mathbb{Z})^\times$ can be commputed by Euler's totient function.

Euler's Totient Function (オイラー関数)

Definition 1

- $\phi(n) \triangleq \{x \in \mathbb{N} \,|\, 1 \leq x \leq n \text{ and } (x, n) = 1\}$ is called *Euler's ϕ function* or *Euler's totient function*.
- Equivalently, Euler's totient function $\phi(n)$ is the number of positive integers up to n that are relatively prime to n.

Proposition 1

- For $(m, n) = 1$, it holds that $\phi(mn) = \phi(m)\phi(n)$.
- For prime p and positive integer e, it holds that $\phi(p^e) = p^{e-1}(p-1)$.
- Let $n = \prod_{i=1}^{s} p_i^{e_i}$. Then, it holds that

$$\phi(n) = n \prod_{i=1}^{s} (1 - \frac{1}{p_i}).$$

Euler's Theorem (オイラーの定理)

Theorem 3 (Euler's Theorem)

For $a, n \in \mathbb{N}$,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof.

From the fact that the order of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is $\phi(n)$. □

Application: (Textbook) RSA

The RSA cryptosystem

- Alice generates two large primes, p and q, and make (e, n) public, where $n = pq$ and e is some prime. Let $pk = (e, n)$, which called public-key.
- Bob who wants to secrelty sends message m $(0 \leq m < n)$, computes $c = m^e \bmod n$ and sends it to Alice.
- Alice computes c^d to retrieve m, where $d = e^{-1} \pmod{\phi(n)}$, where $\phi(n) = (p-1)(q-1)$. Here d is called secret key.

Here, note that

$$c^d = (m^e)^d = m^{ed} = m^{1+k\phi(n)} = m \cdot (m^{\phi(n)})^k = m \pmod{n},$$

since $d = e^{-1} \bmod \phi(n)$ implies that $ed = 1 + k\phi(n)$ for some integer k.

[Remark] The RSA cryptosystem is one of the earliest public-key cryptosystems and widely used for internet, which was proposed by Ron Rivest, Adi Shamir, and Reonald Adleman (so, called "RSA"). All of them are Turing award winers (at 2002) for their contribution of finding RSA.

Today's Contents

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 2 (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 4

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 5

$G/N(= G\backslash N)$ 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, $aN \circ bN \subset (a \circ b)N$.

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

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

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

Proof of Theorem 5.

$G/H(= G\backslash H)$ 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.

Today's Contents

Map (写像)

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

Definition 3 (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 4 (Surjective (全射))

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

Definition 5 (Injective (単射))

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

Definition 6 (Bijective (全単射))

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

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 7 (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 2

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

Proposition 3

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

Proposition 4

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

Proofs

Proof of Propostion 2.

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 3.

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 4.

Omit. Prove by yourself. □

Group Isomorphism (群の同型)

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

Definition 8 (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 9 (Kernel (核))

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

Proposition 5

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

Proof of Proposition 5

It surfices 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 6 (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 $N := \mathrm{Ker}(f)$ 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 $\bar{f}(xN) = \bar{f}(yN) \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x \circ y^{-1}) = e' \Leftrightarrow$ $x \circ y^{-1} \in N(:= \mathrm{Ker}(f)) \Leftrightarrow x \in yN \Leftrightarrow xN = yN$. Hence,

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

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

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 this problem.

- 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 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 7

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 8

$\langle a \rangle$ 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 $\langle a \rangle$.

Reminder: 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 9

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

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.

□

Definition 14

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

Ring (環)

Definition 15 (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 [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 $(R, +)$.
- Denote by 1 the identity of $(R, \cdot)$ (if it exists).

Commutative Ring (可換環)

Definition 16

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 17

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.