Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2020

Contents

Groups

Definitions(P115)

1. *group* $(G,\circ)$
   - group set G
   - group Operation $\circ$
   - associativity $(a \circ b \circ c = a \circ (b \circ c))$
   - unique identity element $(e_1 = e_1 \circ e_2 = e_2)$
   - unique inverse element $(y_2 = y_2 \circ e = y_2 \circ x \circ y_1 = e \circ y_1 = y_1)$
2. *abelian*: communitativity $(\forall x, y \in G, x \circ y = y \circ x)$

e.g.

- If $(G, \circ)$ is a group, then $G \neq \emptyset$ (existence of identity) (P160).
- $X = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is linear with non-zero slope}\}$. Then $(X, \circ)$ is a group that is not abelian.
- $X' = \{f \in X \mid f \text{ is with no-zero intersection}\}$. Then $(X, \circ)$ is not a group.
- $X'' = \{f \in X \mid f(0) = 0\}$. Then $(X'', \circ)$ is an abelian group.

Algebra in Groups

Lemma

Let $(G, \circ)$ be a group. If $a, b, c \in G$ and $a \circ b = a \circ c$, then $b = c$.

Proof.

Let $a, b, c \in G$ and suppose that $a \circ b = a \circ c$. Now,

$$\begin{aligned} b = e \circ b = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) \\ = a^{-1} \circ (a \circ c) = (a^{-1} \circ a) \circ c = e \circ c = c \end{aligned}$$

□

Corollary

Let $(G, \ )$ be a group and $a \in G$. If $a \circ a = a$, then $a = e$.

Relations

Definitions (P117)

1. *relation*: set of ordered pairs
2. *a relation on set M*
3. *domain*
4. *range*

e.g.(DMA P575)

- $R_1 = \{(a, b) | a \leq b\}$
- $R_2 = \{(a, b) | a > b\}$
- $R_3 = \{(a, b) || a| = |b|\}$
- $R_4 = \{(a, b) | a = b + 1\}$
- $R_5 = \{(a, b) | a \ mod \ 2 = b \ mod \ 2\}$

Properties of Relations (P119)

Definitions We say a relation R on M is

1. *reflexive*: if $\forall a \in M, (a, a) \in R$.
2. *symmetric*: if $\forall a, b \in M, (a, b) \in R$, then $(b, a) \in R$.
3. *antisymmetric*: if $\forall a, b \in M, (a, b) \in Mand(b, a) \in R$, then $a = b$.
4. *asymmetric*: if $\forall a, b \in M, (a, b) \in R$, then $(b, a) \notin R$.
5. *transitive*: if $\forall a, b, c \in M, (a, b) \in Rand(b, c) \in R$, then $(a, c) \in R$.

e.g.

- $R = \emptyset$ on $\emptyset$ is reflexive, symmetric, antisymmetric, asymmetric and transitive. If $M \neq \emptyset$, then R is symmetric, antisymmetric, asymmetric and transitive.
- $R = \{(1, 2), (3, 4)\}$ is antisymmetric, asymmetric and transitive.

Equivalence Relations

Definition

Equivalence Relation on M(P119):

A reflexive, symmetric and transitive relation on M

e.g.(P120)

Define the *integer sum* $I(n)$ as the sum of all integers that compose the number, e.g. $I(125) = 1 + 2 + 5 = 8$, $I(78) = 7 + 8 = 15$. Then the relation $R = \{(a, b) \in \mathbb{N}^2 : I(a) = I(b)\}$ is an equivalence relation on $\mathbb{N}$.

Equivalence Classes

Definitions(P121)

1. *a partition of set A*
2. *equivalence class*
3. *representative*

e.g.(P121)
$\mathcal{F} = \{[0], [1]\}$, where $2\mathbb{N} = [0], 2\mathbb{N} + 1 = [1]$, is a partition of $\mathbb{N}$.

Theorem
Every partition $\mathcal{F}$ of M induces an equivalence relation $\sim$ on a set M by

$$a \sim b \;\; :\Leftrightarrow \;\; a, b \in M \text{ are in the same equivalence class}$$

Properties of Equivalence Classes (P123-P124)

Theorem

Every equivalence relation $\sim$ on a set M induces a partition $\mathcal{F} = \{[a] : a \in M\}$ of M by

$$a \in [b] \;:\Leftrightarrow\; a \sim b$$

We write $\mathcal{F} = M/\sim$.

Proof.

1. Prove that the union of all classes in $\mathcal{F}$ is M.
2. Prove that all classes in $\mathcal{F}$ is mutually disjoint (proof by contraposition).

$\square$

$\mathbb{N}$ to $\mathbb{Z}$

$(\mathbb{N}, +)$ and $(\mathbb{N}, \times)$ are not groups both because that they do not have inverse elements (P116).

Preparations before the expansion of numbers:(P125)
Consider the set of ordered pairs

$$\mathbb{N}^2 = \{(n, m); n, m \in \mathbb{N}\}$$

$\mathbb{N}$ can be consider as a natural subset of $\mathbb{N}^2$ by replacing $n \in \mathbb{N}$ with $(n, 0) \in \mathbb{N}^2$. Define the following equivalence relation on $\mathbb{N}^2$:

$$(n, m) \sim (p, q) \quad :\Leftrightarrow \quad n + q = m + p$$

Construction of $\mathbb{Z}$ (P126)

1. Every pair of the form $(n, 0) \in \mathbb{N}^2, n \in \mathbb{N}$ is in a different equivalence class of this partition. We denote these equivalence classes by $[+n] \ni (n, 0)$.
2. Every pair of the form $(0, n) \in \mathbb{N}^2, n \in \mathbb{N}$ is in a different equivalence class of this partition. We denote these equivalence classes by $[-n] \ni (n, 0)$.
3. $\mathbb{Z} = \{[+n] : n \in \mathbb{N}\} \cup \{[-n] : n \in \mathbb{N} \setminus \{0\}\}$

Operations on $\mathbb{Z}$

Addition and Subtraction on $\mathbb{Z}$:(P127-P128)
Addition on $\mathbb{N}^2$ is defined by $(n, m) + (p, q) = (n + p, m + q)$ and

$$(n, m) + (0, 0) = (n, m) \quad (n, m) + (p, q) = (p.q) + (n, m)$$

which means that $(\mathbb{N}^2, +)$ is an abelian group, i.e. $(\mathbb{Z}, +)$ is an abelian group. Subtraction($-$) is then defined by

$$n - m = n + (-m)$$

Multiplication on $\mathbb{Z}$:(P130)
Based on $(m - n) \cdot (p - q) = m \cdot p + n \cdot q - m \cdot q - n \cdot p$, multiplication on $\mathbb{N}^2$ (i.e.) is defined by

$$(m, n) \cdot (p, q) := (m \cdot p + n \cdot q, m \cdot q + n \cdot p)$$

However, $(\mathbb{Z}, \cdot)$ is not a group still because that they do not have inverse elements.

$\mathbb{Z}$ to $\mathbb{Q}$ (P133-P134)

We define the equivalence relation

$$(n, m) \sim (p, q) :\Leftrightarrow n \cdot q = m \cdot p$$

for $(n, m), (p, q) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. Thus we denote the set of rational numbers by $\mathbb{Q} := \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ and $\mathbb{Z}$ is considered as a subset of $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ by associating $n \leftrightarrow (n, 1)$. We identify a representative (n, m) with its class $[(n, m)]$ and write

$$(n, m) =: \frac{n}{m} \in \mathbb{Q}$$

and the product and sum of two pairs of integers are defined by

$$(n, m) \cdot (p, q) := (n \cdot p, m \cdot q)$$
$$(n, m) + (p, q) := (n \cdot q + m \cdot p, m \cdot q)$$

$\mathbb{Z}$ to $\mathbb{Q}$ (P134)

- The neutral element of multiplication on $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ (i.e. on $\mathbb{Q}$) is $[(1,1)]$.
- Every element $[(n, m)] \in \mathbb{Q}$ except $[(0,1)]$ has a multiplicative inverse
$$[(n, m)]^{-1} = [(m, n)]$$
- $(\mathbb{Q}, +)$ is an abelian group.
- $(\mathbb{Q}, \cdot)$ is an abelian group.

Modulus of a rational numbers:

$$|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

Rings (P131-P132,P135)

Definitions

1. *ring*:
   - two binary operations $+$ and $\cdot$.
   - existence of a multiplicative unit element
   - associativity
   - distributivity
2. *communitativity*
3. *integral domain*
4. *field*: $(F, +, \cdot)$ is a field if $(F, +)$ and $(F \setminus \{0\}, \cdot)$ are abelian groups, $0 \neq 1$ and the law of distributivity holds.

$\mathbb{Q}$ is a field.

Functions

Definitions

1. *function* (P138)
   - relation
   - uniqueness
2. *injective functions* (P139)
3. *surjective functions* (P139)
4. *bijection*: both injective and surjective (P139)
5. *inverses & inverse functions* (P140)

Sequence (P141-P142)

Definitions

1. *sequences of rational numbers*
2. *convergent sequences*
3. *Cauchy sequence*

Since $|a_n - a_m| \leq |a_n - a| + |a_m - a|$, every convergent sequence must be a Cauchy sequence, but not every Cauchy sequence of rational numbers converges.

Construction of $\mathbb{R}$ (P144)

Consider the set of all sequences in $\mathbb{Q}$ that converge to a limit, denote this set by $\mathrm{Conv}(\mathbb{Q})$. Each sequence $(a_n) \in \mathrm{Conv}(\mathbb{Q})$ is associated uniquely to a number $a \in \mathbb{Q}$, namely its limit. Two sequences are said to be equivalent it they have the same limit, i.e.

$$(a_n) \sim (b_n) \quad :\Leftrightarrow \quad \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$$

which is an equivalence relation, and

$$\mathbb{Q} \simeq \mathrm{Conv}(\mathbb{Q})/\sim$$

Construction of $\mathbb{R}$ (P145-P146)

Denote the Cauchy sequences of rational numbers as Cauchy($\mathbb{Q}$) and two Cauchy sequences are equivalent if their difference converges to 0, i.e.

$$(a_n) \sim (b_n) \quad :\Leftrightarrow \quad \lim_{n\to\infty}(a_n - b_n) = 0$$

Thus

$$\mathbb{Q} \simeq \mathrm{Conv}(\mathbb{Q})/\sim \subset \mathrm{Cauchy}(\mathbb{Q})/\sim$$

and we can then define

$$\mathbb{R} := \mathrm{Cauchy}(\mathbb{Q})/\sim$$

which is the completion of $\mathbb{Q}$, and $\mathbb{R}$ is also a field.

Division Algorithm (P149-P158)

Definitions

- quotient & remainder
- uniqueness (proof by contraposition)
- existence (proof by well-ordering principle)
- $0 \leq r < |b|$
- divsor(factor) & multiple

Theorem

1. $a|b$ *and* $c|d$ *implies* $ac|bd$
2. $a|b$ *and* $b|c$ *implies* $a|c$
3. $a|b$ *with* $b \neq 0$ *implies* $|a| \leq |b|$
4. $a|b$ *and* $a|c$ *implies* $a|(xb + yc)), \forall x, y \in \mathbb{Z}$

GCD, LCM & Bézout's Lemma

Definition

- greatest common divisor (two definitions (P159,P170))
- least common multiple (P180)

Theorem

(Bézout's Lemma) Let $a, b \in \mathbb{Z}$ *with* $|a| + |b| \neq 0$*. Then there exists* $x, y \in \mathbb{Z}$ *such that* $\gcd(a, b) = ax + by$*.*

Proof.

P161-P163 □

Corollary

Let $a, b \in \mathbb{Z}$ *with* $|a| + |b| \neq 0$*. Then*

$$T(a, b) = \{n \in \mathbb{Z} : n = ax + by, x, y \in \mathbb{Z}\}$$

is the set of all integers multiples of $\gcd(a, b)$*. (P163)*

Relatively Prime Numbers (P164)

Definition

relatively prime: $gcd(a, b) = 1$

Theorem

Let $a, b \in \mathbb{Z}$ *with* $|a| + |b| \neq 0$. *Then* a *and* b *are relatively prime if and only if there exists* $x, y \in \mathbb{Z}$ *such that*

$$ax + by = 1$$

Proof.

1. $(\Rightarrow)$ Apply Bézout's Lemma
2. $(\Leftarrow)$ Suppose that there exist x and y with $ax + by = 1$ and that $d = gcd(a, b)$, then $d \mid (ax + by)$, i.e. $d \mid 1$, then $d = 1$.

$\square$

Results from Bézout's Lemma

Corollary

(P165) If $gcd(a, b) = d$, then

$$gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Corollary

(P168) Let $a, b, c \in \mathbb{Z}$ with $gcd(a, b) = 1$. Then

$$a \mid c \text{ and } b \mid c \quad \text{implies} \quad a \cdot b \mid c$$

Lemma

(Euclid's Lemma)(P169) Let $a, b, c \in \mathbb{Z}$ with $gcd(a, b) = 1$. Then

$$a \mid bc \quad \text{implies} \quad a \mid c$$

Euclidean Algorithm (P172-P179)

Lemma

Let $a, b, q, r \in \mathbb{Z}$ *with* $a = bq + r$, *then* $gcd(a, b) = gcd(b, r)$

Proof.

Let $d = gcd(a, b)$ and $a = bq + r$, then $d \mid a - bq$, i.e. $d \mid r$. Suppose that $c \mid b$ and $c \mid r$, then $c \mid bq + r$, i.e. $c \mid a$, which means that c is also a common divisor of a, b. Since $d = gcd(a, b)$, then $c \leq d$ for any c that divides b and r. Thus $d = gcd(b, r)$. $\square$

Lemma

Let $a, b \in \mathbb{Z}$ *with* $|a| + |b| \neq 0$ *and* $k \neq 0$. *Then*

$$gcd(ka, kb) = |k| \cdot gcd(a, b)$$

Linear Diophantine Equation

Definition

A Linear Diophantine Equation in two variables has the form

$$ax + by = c, \qquad a, b, c \in \mathbb{Z}, |a| + |b| \neq 0$$

with the solution pair $(x_0, y_0) \in \mathbb{Z}^2$ such that $ax_0 + by_0 = c$.

Theorem

The linear Diophantine Equation $ax + by = c$ has solution(s) if and only if $d \mid c$, where $d = gcd(a, b)$, furthermore, if (x_0, y_0) is a solution, then for any $t \in \mathbb{Z}$, we obtain all the solution pairs in the form of

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t$$

Exercise

Find all solutions for the Linear Diophantine Equation:

$$12x + 34y = 56$$

Solution

- Check whether solutions exist:

$$\begin{aligned}34 &= 2 \times 12 + 10\\12 &= 1 \times 10 + 2\\10 &= 5 \times 2\end{aligned}$$

thus $\gcd(12, 34) = 2,\ 2|56$. The equation has solutions.

- Apply Euclidean Algorithm in reverse step:

$$2 = 12 - 1 \times 10 = 12 - 1 \times (34 - 2 \times 12) = 3 \times 12 - 34$$

We obtain $12 \times 3 - 34 = 2$.

- Multiplied by $\frac{c}{gcd(a,b)}$ to find the special solution (x_0, y_0):

$$12 \times (3 \times 28) - 34 \times 28 = 2 \times 28 = 56$$

we obtain $(x_0, y_0) = (84, -28)$, thus all the solution pairs: $(84 + 17t, -28 - 6t)(t \in \mathbb{Z})$