Lecture 5

05 February 2024 14:05

Last time:

- Subrings of $2\mathbb{Z}$ are exactly subsets of the form $m2\mathbb{Z}$ for some $m \in \mathbb{Z}$.
- We defined the ring $M_{n\times n}(R)$ of $n\times n$ matrices with entries in any ring R.

The ring of subsets of a set (CW1, Q1b)

Consider the set $\mathcal{P}(X)$ of all subsets of a set X.

Eg: $X = 2\mathbb{Z}$ $\quad \mathcal{P}(2\mathbb{Z}) = \{\emptyset, \{1\}, \{2,4,6,\dots\}, \{\text{prime numbers}\}, \{1,2,3\}, \dots\}$

Consider the binary operations:

$$A \text{ "}+\text{" } B \overset{\text{def}}{=} A \triangle B = (A \cup B) \setminus (A \cap B).$$

Eg: $\{\text{odd numbers}\} + \{\text{prime numbers}\} = \{2, \text{composite odd numbers}\}$

$$A \text{ "}\cdot\text{" } B \overset{\text{def}}{=} A \cap B$$

Eg: $\{\text{odd numbers}\} \cdot \{\text{prime numbers}\} = \{\text{odd prime numbers}\}$

Fact (CW1): This defines a ring whose elements are $P(X)$.

These rings are examples of **Boolean rings**

(CW1 Problem 2).

a ring in which $a \cdot a = a$ for all $a \in R$

The zero element of $P(X)$ is

$$? + A = A$$

$$? \triangle A = A$$

↳ empty set is the zero.

Does $P(X)$ have a multiplicative identity?

$$? \cdot A = A$$

$$? \cap A = A$$

↳ X is the multiplicative identity.

Example: $X = \{a, b\}$. The ring $P(X)$ is $P(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

$+$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a,b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\emptyset$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\emptyset$

$\cdot$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$

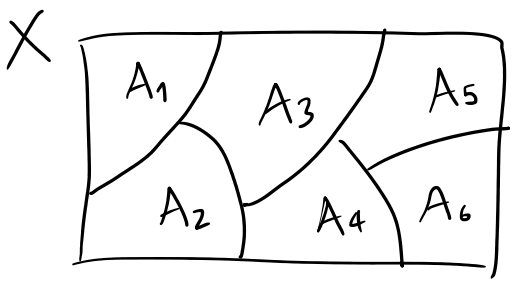
11

Equivalence relations and partitions

A <u>partition</u> of a set X is a collection of subsets $\{A_1, A_2, \dots\}$ of X such that

- $A_i \neq \emptyset$
- Every $i \in X$ is in some part A_i
- $A_i \cap A_j = \emptyset$ if $i \neq j$.

<u>Picture</u>



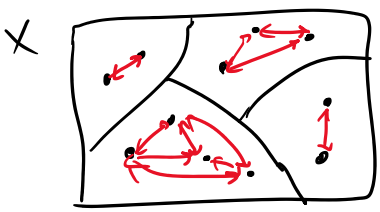
Given a partition of X, we can define a relation on X by

$a \sim b$ if and only if a and b are in the same part A_i.

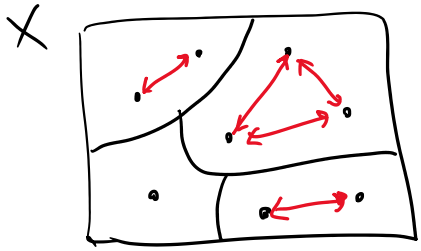
This relation is:

- Reflexive: $a \sim a$ since a and a are in the same part.
- Symmetric: If $a \sim b \Rightarrow b \sim a$ because if a and b are in the same part, then b and a are in the same part.
- Transitive: $a \sim b$ and $b \sim c$ then $a \sim c$. because if a and b are in the same part and b and c are in the same part, then a and c are in the same part.

Conclusion: Any partition of X defines an equivalence relation on X.



You can recover the partition just from the equivalence relation:



The parts in this partition are called equivalence classes:

equivalence classes:

$$[a]_\sim := \{ b \in X \mid a \sim b \}.$$ → the equivalence class of a.

Takeaway message

There is a correspondence

$$\left\{ \begin{array}{c} \text{partitions} \\ \text{of } X \end{array} \right\} \longleftrightarrow \text{bijection} \longleftrightarrow \left\{ \begin{array}{c} \text{equivalence relations} \\ \text{on } X \end{array} \right\}$$

Cosets:

Suppose R is a ring and S a subring of R. We can define the binary relation on R:

$$a \sim_S b \iff a - b \in S$$

elements of R

Proposition. This binary relation is an equivalence relation.

- **Reflexive**: $a \sim a$ because $a - a = 0 \in S$.
- Symmetric: If $a \sim b$ then $a - b \in S$.

- Symmetric: If $a \sim b$ then $a - b \in S$.

This implies that $-(a-b) \in S$. But

$-(a-b) = b - a \in S$, so $b \sim a$.

(We are using $-(a+b) = (-a) + (-b)$ Exercise!)

- Transitive: If $a \sim b$ and $b \sim c$, this means that $a - b \in S$ and $b - c \in S$. Since S is closed under addition,

$$a - c = \underbrace{(a-b)}_{\in S} + \underbrace{(b-c)}_{\in S} \in S.$$

meaning that $a \sim c$. ∎

Example: $R = \mathbb{Z}$ $S = 5\mathbb{Z}$

Two elements of $\mathbb{Z}$ are related

$a \sim b \iff a - b \in 5\mathbb{Z}$

$\iff a$ and b have the same remainder modulo 5.

Definition: Given a ring R and a subring S,

Definition: Given a ring R and a subring S, there is a partition of R into the equivalence classes of the equivalence relation $\sim_S$:

$$[a]_S = \{ b \in R \mid a - b \in S \}.$$

These equivalence classes are called the **cosets of S in R**.

Example: $R = \mathbb{Z}$ $\quad S = 5\mathbb{Z}$

$\mathbb{Z}$

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15				

In this example, there are 5 cosets of $5\mathbb{Z}$ in $\mathbb{Z}$. (only one coset is a subring!).

Proposition: The equivalence class $[a]_S$ can also be written as

$$[a]_S = a + S = \{ a + s \mid s \in S \}$$

(+ notation)

$$[a]_S = a + S = \{ a + s \mid s \in S \}$$

Proof: We want to show $[a]_S = a + S$.

Let's prove the two inclusions.

"$\subseteq$" Suppose $b \in [a]_S$. This means that $b - a \in S$, so $b - a = s$ where $s \in S$.

$\Rightarrow b = a + s \in a + S$.

"$\supseteq$" Suppose $b \in a + S$. This means $b = a + s$ where $s \in S$. Then $b - a = s \in S$, so $b \in [a]_S$. ∎

Example: $R = \mathbb{Z}$ $S = 5\mathbb{Z}$

$\mathbb{Z}$

⋮	⋮	⋮	⋮	⋮
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
⋮	⋮	⋮	⋮	⋮
S	$1+S$	$2+S$	$3+S$	$4+S$
	$\|\|$	$\|\|$	$\|\|$	$\|\|$
	$6+S$	$7+S$	⋮	$9+S$
	$\|\|$	$\|\|$		$\|\|$
	$-4+S$	$-3+S$		⋮

In general, if $R = 2\mathbb{Z}$ and $S = m \cdot 2\mathbb{Z}$ we will get m many cosets corresponding to the different equivalence classes modulo m, that is, the m different remainders an integer can have modulo m.