Ch. 3 - Cartesian Products & Relations

§0. Introduction

We are all familiar with the many different kinds of relationships between human beings and we often say that two people are related in one way or the other - and sometimes we say they are not. For example we can say that a is the mother of b - and this is a relation. (We also have DNA tests which can ascertain to an extremely high degree of certainity whether or not a is the mother of b.).

We can also say that b is a sibling of c and that b is the spouse of d. Notice that if b is a sibling of c, then c is automatically a sibling of b. This is a special property of the relation of being a sibling. Notice also that the same is true for the relation of being the spouse - but here more is true - b can have at most one spouse (legally speaking) but b can have any (reasonable) amount of siblings. This notion of a sibling captures the essence of a symmetric relation and the notion of a spouse captures the essence of a special relation called a partial function. We can also say that b is a biological child of the man e and the woman a. This is called a ternary relation.

Finally we can say that b's mother is the lady named a. This relation captures the essence of a function because everyone (living today) has one and only one mother. In order to better understand all these kinds of relations, we shall introduce the notion of an <u>ordered pair</u> and study certain collections of ordered pairs and relations in general. In the next chapter we will study partial functions and functions.

§1 <u>Ordered pairs & the Cartesian product</u>

<u>Def.</u> A <u>pair</u> (or <u>unordered pair</u>) is any set which consists of exactly 2 distinct elements

<u>Ex. 1</u> (a) $\{1,2\}$ and $\{1,3\}$ are pairs
(b) $\{\emptyset, \{\{\emptyset\}\}\}$ is a pair.
(c) $\{\emptyset\}$, $\{1,2,4\}$, and $\emptyset$ are not pairs.

One of the axioms of ZFC Set Theory states that: "If A & B are sets, then $\{A,B\}$ is a set". Note that the axiom did not say that A & B must be distinct (different). If $A = B$, then $\{A,B\} = \{A,A\} = \{A\}$. So the axiom also says that "If A is a set, then $\{A\}$ is also a set." Starting from the empty set $Z_0 = \emptyset$, we can thus form the sets $Z_1 = \{\emptyset\}$, $Z_2 = \{Z_1\} = \{\{\emptyset\}\}$, $Z_3 = \{Z_2\} = \{\{\{\emptyset\}\}\}$ and so on. The sets Z_n are called <u>Zermelo sets</u>.

An ordered pair consists of two elements (which are not necessarily distinct) — one of which is designated as the first element and the other is designated as the second element.

We can use sets of a special form to capture this notion and best represent ordered pairs.

Def. An <u>ordered pair</u> is any set of the form $\{\{a\}, \{a,b\}\}$ — and we use the notation (a,b) to denote this set. In other words, $(a,b) = \{\{a\}, \{a,b\}\}$.

Note: In some textbooks an ordered pair is denoted by $\langle a,b \rangle$ but we will reserve these pointed brackets to denote <u>sequences</u> (which will be precisely defined in the next Chapter).

Ex. 2 (a) $(1,2) = \{\{1\}, \{1,2\}\}$ is an ordered pair.
(b) $(2,1) = \{\{2\}, \{2,1\}\}$ is an ordered pair.
(c) $(2,2) = \{\{2\}, \{2,2\}\} = \{\{2\}\}$ is an ordered pair.
(d) $\{\{1\}, \{2,3\}\}$ and $\{1, \{1,2\}\}$ are not ordered pairs.

Prop. 1: $(a,b) = (c,d) \iff (a=c \ \& \ b=d)$.

Proof: ($\Leftarrow$): Suppose $a=c$ and $b=d$. Then

$$\begin{aligned}(a,b) &= \{\{a\}, \{a,b\}\} \\ &= \{\{c\}, \{c,d\}\} \quad \text{because } a=c \ \& \ b=d \\ &= (c,d).\end{aligned}$$

So $(a=c \ \& \ b=d) \Rightarrow (a,b)=(c,d)$.

Proof. ($\Rightarrow$): Now suppose $(a,b)=(c,d)$. Then $\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}$. There are two cases: $a=b$ and $a\neq b$.

Case(i): $a=b$. In this case we have $\{\{c\},\{c,d\}\}=(c,d)=(a,b)=(a,a)=\{\{a\}\}$. Since $\{\{a\}\}$ has only one element, $\{\{c\},\{c,d\}\}$ must also have only one element. So we must have $\{c\}=\{c,d\}$. This means that we must have $c=d$. $\therefore \{\{a\}\}=\{\{c\},\{c,d\}\}=\{\{c\},\{c,c\}\}=\{\{c\},\{c\}\}$ $=\{\{c\}\}$. Hence $a=c$. Also $b=a=c=d$. Thus $a=c$ & $b=d$.

Case(ii): $a\neq b$. In this case we have $\{\{c\},\{c,d\}\}=\{\{a\},\{a,b\}\}$. So $\{c\}=\{a\}$ or $\{c\}=\{a,b\}$. Since $a\neq b$, $\{a,b\}$ has 2 elements and since $\{c\}$ has only one element, we must have $\{c\}\neq\{a,b\}$. Thus $\{c\}=\{a\}$. Hence $c=a$. Also since $\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}$ then $\{a,b\}=\{c\}$ or $\{a,b\}=\{c,d\}$. But $\{a,b\}\neq\{c\}$ because $\{a,b\}$ has 2 elements. So $\{a,b\}=\{c,d\}$. So $b=c$ or $b=d$. But $a=c$, and $a\neq b$, so $c\neq b$. Hence $b=d$. Thus $a=c$ & $b=d$.

Def. Let A and B be sets. We define the <u>Cartesian product</u>, $A\times B$, of A with B by

$$A\times B=\{(a,b): a\in A \wedge b\in B\}$$

Ex. 3 Let $A=\{1,2\}$ & $B=\{2,3\}$. Then $A\times B=\{(1,2),(1,3),(2,2),(2,3)\}$ and $B\times A=\{(2,1),(2,2),(3,1),(3,2)\}$.

Note: From Ex. 3, we can see that $A \times B \neq B \times A$ in general. Notice also that $\emptyset \times A = \emptyset$ & $A \times \emptyset = \emptyset$ for any set A.

Qu: Exactly when is $A \times B = B \times A$?

Prop 3 $A \times B = B \times A \iff (A = B \text{ or } A = \emptyset \text{ or } B = \emptyset)$.

Proof: ($\Leftarrow$): If $A = B$, then $A \times B = A \times A$ because $A = B$
$= B \times A$ because $B = A$

Also if $A = \emptyset$, then $A \times B = \emptyset \times B = \emptyset = B \times \emptyset = B \times A$
and if $B = \emptyset$, then $A \times B = A \times \emptyset = \emptyset = \emptyset \times A = B \times A$.
So $(A = B \text{ or } A = \emptyset \text{ or } B = \emptyset) \Rightarrow A \times B = B \times A$.

($\Rightarrow$): Suppose $A \times B = B \times A$ and $A \neq \emptyset$ & $B \neq \emptyset$.
We will show that $A = B$.
Let $a \in A$. Since $B \neq \emptyset$, there exists a $b \in B$.
So $(a, b) \in A \times B$. But $A \times B = B \times A$. So $(a, b) \in B \times A$. Hence $a \in B$ & $b \in A$. Thus $a \in B$.
$\therefore$ $A \subseteq B$ ... (1).
Now let $b \in B$. Since $A \neq \emptyset$, there exists an $a \in A$. So $(a, b) \in A \times B$. But $A \times B = B \times A$. So $(a, b) \in B \times A$. $\therefore$ $a \in B$ & $b \in A$. Thus $b \in A$.
$\therefore$ $B \subseteq A$ ... (2).
From (1) & (2) it now follows that $A = B$.

Hence $(A \times B = B \times A)$ and $(A \neq \emptyset \wedge B \neq \emptyset) \Rightarrow A = B$. $\therefore$ $(A \times B = B \times A) \Rightarrow (A = B \text{ or } A = \emptyset \text{ or } B = \emptyset)$.
bec. $(P \wedge Q \rightarrow R) \Leftrightarrow \neg(P \wedge Q) \vee R \Leftrightarrow \neg P \vee (\neg Q \vee R) \Leftrightarrow P \rightarrow (\neg Q \vee R)$.

Theorem 3: Let $A, B, C,$ and D be sets. Then

(a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$ (a′) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

(b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$ (b′) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

(c) $A \times (B - C) = (A \times B) - (A \times C)$ (c′) $(A - B) \times C = (A \times C) - (B \times C)$.

(d) $(A \cap D) \times (B \cap C) = (A \times B) \cap (D \times C)$

(e) $(A \cup D) \times (B \cup C) = (A \times B) \cup (A \times C) \cup (D \times B) \cup (D \times C)$

Proof: Do (a′), (b′), & (c′) for H.W. Note that (a) & (b) are special cases of (d) & (e) with $D = A$.

(a) Let $(a,b) \in A \times (B \cap C)$. Then $a \in A \wedge b \in B \cap C$. So $a \in A \wedge (b \in B \wedge b \in C)$. $\therefore$ $(a \in A \wedge b \in B) \wedge (a \in A \wedge b \in C)$ $\therefore$ $(a,b) \in A \times B$ and $(a,b) \in A \times C$. Hence $(a,b) \in (A \times B) \cap (A \times C)$. Thus

$$A \times (B \cap C) \subseteq (A \times B) \cap (A \times C) \quad \ldots (1)$$

Now let $(a,b) \in (A \times B) \cap (A \times C)$. Then $(a,b) \in A \times B$ and $(a,b) \in (A \times C)$. So $(a \in A \wedge b \in B) \wedge (a \in A \wedge b \in C)$ $\therefore$ $(a \in A) \wedge (b \in B \wedge b \in C)$. So $a \in A \wedge b \in (B \cap C)$. Hence $(a,b) \in (A \times B)$. Thus

$$(A \times B) \cap (A \times C) \subseteq A \times (B \cap C) \quad \ldots (2)$$

From (1) & (2), we get $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(b) Let $(a,b) \in A \times (B \cup C)$. Then $a \in A \wedge b \in (B \cap C)$. So $a \in A \wedge (b \in B \vee b \in C)$. $\therefore$ $(a \in A \wedge b \in B) \vee (a \in A \wedge b \in C)$. $\therefore$ $(a,b) \in (A \times B) \vee (a,b) \in (A \times C)$. So $(a,b) \in (A \times B) \cup (A \times C)$. Thus $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ $\ldots$ (1).

Now let $(a,b) \in (A \times B) \cup (A \times C)$. Then $(a,b) \in (A \times B) \vee (a,b) \in A \times C$. So $(a \in A \wedge b \in B) \vee (a \in A \wedge b \in C)$. Thus

3(b) $(a\in A)\wedge(b\in B\vee b\in C)$. $\therefore (a\in A)\wedge b\in(B\cup C)$. Hence $(a,b)\in A\times(B\cup C)$. Thus $(A\times B)\cup(A\times C)\subseteq A\times(B\cup C)$ ... (2)
From (1) & (2) we get $A\times(B\cup C)=(A\times B)\cup(A\times C)$.

3(b) again: We can prove 3(b) a little faster by going both ways at the same time – but this is dangerous.

$$\begin{aligned}(a,b)\in A\times(B\cup C) &\Leftrightarrow a\in A\wedge b\in(B\cup C)\\ &\Leftrightarrow a\in A\wedge(b\in B\vee b\in C)\\ &\Leftrightarrow (a\in A\wedge b\in B)\vee(a\in A\wedge b\in C)\\ &\Leftrightarrow (a,b)\in(A\times B)\vee(a,b)\in(A\times C)\\ &\Leftrightarrow (a,b)\in(A\times B)\cup(A\times C)\end{aligned}$$

Thus $A\times(B\cup C)=(A\times B)\cup(A\times C)$ again.

3(c) If we try to prove 3(c) this way, we will get into trouble. So let us go back to the one way routes.
Let $(a,b)\in A\times(B-C)$. Then $a\in A\wedge b\in(B-C)$. So $a\in A\wedge(b\in B\wedge b\notin C)$. $\therefore (a\in A\wedge b\in B)\wedge(a\in A\wedge b\notin C)$
$\therefore (a,b)\in A\times B$ and $(a,b)\notin(A\times C)$ because we need both $a\in A\wedge b\in C$ to ensure that $(a,b)\in A\times C$.
$\therefore (a,b)\in(A\times B)-(A\times C)$. Thus

$$A\times(B-C)\subseteq(A\times B)-(A\times C) \quad \ldots (1)$$

Now let $(a,b)\in(A\times B)-(A\times C)$. Then $(a,b)\in A\times B$ and $(a,b)\notin A\times C$. So $(a\in A\wedge b\in B)\wedge\neg(a\in A\wedge b\in C)$
$\therefore (a\in A\wedge b\in B)$ & $(a\notin A\vee b\notin C)$. But we know that $a\in A$, so it follows from $a\notin A\vee b\notin C$, that $b\notin C$. $\therefore a\in A\wedge(b\in B\wedge b\notin C)$. So $a\in A\wedge b\in(B-C)$.
Thus $(a,b)\in A\times(B-C)$. $\therefore (A\times B)-(A\times C)\subseteq A\times(B-C)$ ... (2).
From (1) & (2), we get $A\times(B-C)=(A\times B)-(A\times C)$.

3(d) $(a,b) \in (A \cap D) \times (B \cap C) \Leftrightarrow a \in A \cap D \wedge b \in B \cap C$

$\Leftrightarrow (a \in A \wedge a \in D) \wedge (b \in B \wedge b \in C)$

$\Leftrightarrow (a \in A \wedge b \in B) \wedge (a \in D \wedge b \in C)$

$\Leftrightarrow (a,b) \in A \times B \wedge (a,b) \in D \times C$

$\Leftrightarrow (a,b) \in (A \times B) \cap (D \times C)$.

$\therefore (A \cap D) \times (B \cap C) = (A \times B) \cap (D \times C)$.

3(e) $(A \cup D) \times (B \cup C) = (A \cup D) \times B \cup (A \cup D) \times C$ by part (b)

$= (A \times B) \cup (D \times B) \cup (A \times C) \cup (D \times C)$ by part (b')

$= (A \times B) \cup (A \times C) \cup (D \times B) \cup (D \times C)$.

§2. Relations, relations from A to B & relations on A

Def. A set R is a <u>relation</u> if each of its elements is an ordered pair. We define the <u>domain</u> and <u>range</u> of R by

$$\mathrm{dom}(R) = \{a : (a,b) \in R\}$$
$$\mathrm{ran}(R) = \{b : (a,b) \in R\}.$$

Ex. 1 (a) Let $R = \{(1,2), (1,3), (2,3)\}$. Then R is a relation. Also

$\mathrm{dom}(R) = \{1,2\}$ and $\mathrm{ran}(R) = (2,3)$.

(b) Let $S = \{1, \{2\}, (1,2)\}$. Then S is not a relation.

(c) $\emptyset$ and $\{(1,1)\}$ are both relations.

Def. A <u>relation from A to B</u> is a 3-tuple $\langle \mathcal{R}, A, B \rangle$ such that $\mathcal{R}$ is a relation with $\mathrm{dom}(\mathcal{R}) \subseteq A$ & $\mathrm{ran}(\mathcal{R}) \subseteq B$. A & B are called the <u>source</u> & <u>target</u> space.

Note: If A & B are sets then the minimal & maximal relations from A to B are $\emptyset$ and $A \times B$.

Def. Let R & S be relations. We define the <u>inverse</u> R^{-1} of R by

$$R^{-1} = \{(b,a) : (a,b) \in R\}$$

We also define the <u>composition</u> $S \circ R$ of R with S by

$$S \circ R = \{(a,c) : (\exists b)\{(a,b) \in R \wedge (b,c) \in S\}.$$

Ex. 2 Let $R = \{(1,2), (1,3), (2,3)\}$ and $S = \{(3,2), (3,4), (4,2)\}$.

(a) Then $R^{-1} = \{(2,1), (3,1), (3,2)\}$
and $S^{-1} = \{(2,3), (4,3), (2,4)\}$

(b) $S \circ R = \{(1,2), (1,4), (2,2), (2,4)\}$
$R \circ S = \{(3,3), (4,3)\}$

Note: $(A \times B)^{-1} = \{(b,a) : (a,b) \in A \times B\} = B \times A$
$S \circ R \neq R \circ S$ in general by Ex. 2(b).

Prop. 4 Let R, S, and T be relations. Then

(a) $dom(R^{-1}) = ran(R)$ & $ran(R^{-1}) = dom(R)$

(b) $(R^{-1})^{-1} = R$ (c) $(S \circ R)^{-1} = (R^{-1}) \circ (S^{-1})$

(d) $(T \circ S) \circ R = T \circ (S \circ R)$

Proof: (a) $dom(R^{-1}) = \{a : (a,b) \in R^{-1}\}$
$= \{a : (b,a) \in R\} = ran(R)$

$ran(R^{-1}) = \{b : (a,b) \in R^{-1}\}$
$= \{b : (b,a) \in R\} = dom(R)$.

4 (b) $(a,b) \in (R^{-1})^{-1} \Leftrightarrow (b,a) \in R^{-1}$

$\Leftrightarrow (a,b) \in R$

$\therefore (R^{-1})^{-1} = R$

(c) $(c,a) \in (S \circ R)^{-1} \Leftrightarrow (a,c) \in (S \circ R)$

$\Leftrightarrow (\exists b)[(a,b) \in R \wedge (b,c) \in S]$

$\Leftrightarrow (\exists b)[(b,c) \in S \wedge (a,b) \in R]$

$\Leftrightarrow (\exists b)[(c,b) \in S^{-1} \wedge (b,a) \in R^{-1}]$

$\Leftrightarrow (c,a) \in (R^{-1}) \circ (S^{-1})$.

$\therefore (S \circ R)^{-1} = (R^{-1}) \circ (S^{-1})$.

(d) $(a,d) \in (T \circ S) \circ R \Leftrightarrow (\exists b)\{(a,b) \in R \wedge (b,d) \in T \circ S\}$

$\Leftrightarrow (\exists b)\{(a,b) \in R \wedge (\exists c)[(b,c) \in S \wedge (c,d) \in T]\}$

$\Leftrightarrow (\exists c)(\exists b)\{(a,b) \in R \wedge [(b,c) \in S \wedge (c,d) \in T]\}$

$\Leftrightarrow (\exists c)\{(\exists b)[(a,b) \in R \wedge (b,c) \in S] \wedge (c,d) \in T]\}$

$\Leftrightarrow (\exists c)\{(a,c) \in (S \circ R) \wedge (c,d) \in T\}$

$\Leftrightarrow (a,d) \in T \circ (S \circ R)$

$\therefore (T \circ S) \circ R = T \circ (S \circ R)$.

<u>Def.</u> A <u>relation on A</u> is any relation $\mathcal{R}$ from A to A. So a relation on A is a 3-tuple $\langle \mathcal{R}, A, A \rangle$ with $dom(\mathcal{R}) \subseteq A$ & $ran(\mathcal{R}) \subseteq A$.

<u>Notation</u>: If R is a relation, then we often write aRb to denote the fact that $(a,b) \in R$.

<u>Def.</u> Let R be a relation. We say that

(a) R is <u>reflexive</u> on A if $(\forall x \in A)[xRx]$

(b) R is <u>symmetric on A</u> if $(\forall x,y \in A)[xRy \rightarrow yRx]$

(c) R is <u>transitive on A</u> if $(\forall x,y,z \in A)[xRy \wedge yRz \rightarrow xRz]$.

(d) R is <u>circular</u> if $(\forall x,y,z \in A)[xRy \wedge yRz \rightarrow zRx]$

(e) R is <u>connected</u> if $(\forall x \neq y \in A)[xRy \vee yRx]$

Ex 3 Let R be the relation on $\mathbb{Z}$ defined by aRb if $a \leq b$.

(a) Then for each $a \in \mathbb{Z}$, $a \leq a$. So $(\forall a \in \mathbb{Z})\, aRa$. $\therefore$ R is a reflexive relation on $\mathbb{Z}$.

(c) Also for $a, b, c \in \mathbb{Z}$, if $a \leq b$ & $b \leq c$, then $a \leq c$. So $(\forall a, b, c \in \mathbb{Z})[aRb \wedge bRc \rightarrow aRc]$ $\therefore$ R is a transitive relation on $\mathbb{Z}$.

(b) We know that $2 \leq 5$ but $5 \not\leq 2$. So $2R5$ but $\neg(2R5)$. So $(\exists a, b \in \mathbb{Z})[aRb \wedge \neg(bRa)]$. $\therefore$ $\neg(\forall a, b \in \mathbb{Z})[aRb \rightarrow bRa]$. $\therefore$ R is not a symmetric relation on $\mathbb{Z}$

(d) R is not circular on $\mathbb{Z}$ because $1 \leq 2 \wedge 2 \leq 3$ but $3 \not\leq 1$.

Ex 4 Let R be the relation on $\mathbb{Z}$ defined by aRb if $a+b$ is an integer multiple of 3

(a) Then $2+2 \neq$ a multiple of 3. So $\neg(2R2)$. $\therefore$ $\neg(\forall a \in \mathbb{Z})(aRa)$. $\therefore$ R is not reflexive on $\mathbb{Z}$.

(b) Now for each $a, b \in \mathbb{Z}$, if $a+b$ is a multiple of 3, then $b+a$ is a multiple of 3. So for each $a, b \in \mathbb{Z}$ $aRb \rightarrow bRa$. $\therefore$ $(\forall a, b \in \mathbb{Z})[aRb \rightarrow bRa]$. So R is a symmetric relation on $\mathbb{Z}$.

(c) We know that $2+4 =$ a multiple of 3 and $4+5 =$ a multiple of 3. But $2+5 \neq$ a multiple of 3. So $2R4 \wedge 4R5$ but $\neg 2R5$. So $\neg(\forall a, b, c \in \mathbb{Z})[aRb \wedge bRc \rightarrow aRc]$. Hence R is not a transitive relation on $\mathbb{Z}$.

(d) R is not a circular relation on $\mathbb{Z}$ also.

Def. Let A be a set. We define the identity relation i_A on A by $i_A = \{(a, a) : a \in A\}$.

Theorem 5: Suppose R is a relation on A. Then

(a) R is reflexive on $A \Leftrightarrow i_A \subseteq R$

(b) R is symmetric on $A \Leftrightarrow R^{-1} = R$

(c) R is transitive on $A \Leftrightarrow R \circ R \subseteq R$

Proof (a) R is reflexive on $A \Leftrightarrow (\forall a \in A)[aRa]$

$\Leftrightarrow (\forall a \in A)[(a,a) \in R] \Leftrightarrow i_A \subseteq R$.

(b) R is symmetric on $A \Leftrightarrow (\forall a,b \in A)[aRb \to bRa]$

Now if R is symmetric on A, $bRa \to aRb$. So

R is symmetric on $A \Leftrightarrow (\forall a,b \in A)[aRb \leftrightarrow bRa]$

$\Leftrightarrow (\forall a,b \in A)[(a,b) \in R \leftrightarrow (b,a) \in R]$

$\Leftrightarrow (\forall a,b \in A)[(a,b) \in R \leftrightarrow (a,b) \in R^{-1}] \Leftrightarrow R = R^{-1}$.

(c) Suppose R is transitive on A. Then for any $a,b,c \in A$

$aRb \wedge bRc \to aRc$, i.e., $(a,b) \in R \wedge (b,c) \in R \to (a,c) \in R$ (*)

Now if $(a,c) \in R \circ R$, then $(\exists b)[(a,b) \in R \wedge (b,c) \in R]$.

So by (*) $(a,c) \in R$. Hence $R \circ R \subseteq R$.

$\therefore$ R is transitive $\Rightarrow R \circ R \subseteq R$.

Now suppose $R \circ R \subseteq R$. We will show that R is transitive. Now if for any $a,b,c \in A$ $aRb \wedge bRc$, then $(a,b) \in R \wedge (b,c) \in R$. So $(a,c) \in R \circ R$ bec. $(\exists b)[(a,b) \in R \wedge (b,c) \in R]$. But $R \circ R \subseteq R$, so $(a,c) \in R$. Thus aRc. $\therefore$ $(\forall a,b,c \in A)[aRb \wedge bRc \to aRc]$. Hence R is transitive $\therefore$ $R \circ R \subseteq R \Rightarrow R$ is transitive on A

Hence R is transitive on $A \Leftrightarrow R \circ R \subseteq R$

§3. Equivalence relations & partitions

Def. A relation R on A is an <u>equivalence relation on A</u> if R is reflexive, symmetric, and transitive on A

Ex.1 Let R be the relation on $\mathbb{Z}$ defined by aRb if $a-b$ is an integer multiple of 4. Prove that R is an equivalence relation on A

Proof: (a) For each $a \in \mathbb{Z}$, $a-a = 0 = 4(0)$. So $(\forall a \in \mathbb{Z})[aRa]$. $\therefore$ R is reflexive on $\mathbb{Z}$

(b) Suppose aRb. Then $a-b = 4k$ for some integer $k \in \mathbb{Z}$. So $b-a = -4k = 4(-k)$ = an integer multiple of 4, because $k \in \mathbb{Z}$. bRa. So $(\forall a,b \in \mathbb{Z})[aRb \to bRa]$. Hence R is symmetric on $\mathbb{Z}$

(c) Suppose aRb and bRc. Then $a-b = 4k$ and $b-c = 4l$ for some integers $k, l \in \mathbb{Z}$.

So $a-c = (a-b)+(b-c)$

$$= 4k + 4l = 4(k+l).$$

Since $k+l$ is an integer, it follows that aRc.

So $(\forall a,b,c \in \mathbb{Z})[aRb \wedge bRc \to aRc]$. Hence R is transitive on $\mathbb{Z}$.

$\therefore$ R is an equivalence relation on $\mathbb{Z}$.

Ex.2 Let S be the relation on $\mathbb{Z}$ defined by aSb if a^2-b^2 is an integer multiple of 8. Then S is an equivalence relation on $\mathbb{Z}$

Proof: Do for Homework.

Ex.3 Let $R = \{(1,1), (2,2), (2,3), (3,2), (3,3)\}$. Then

(a) R is an equivalence relation on $\{1,2,3\}$, but

(b) R is <u>not</u> an equivalence relation on $\{1,2,3,4\}$ because R is not reflexive on $\{1,2,3,4\}$.

Def Let R be an equivalence relation on A and $a \in A$. We define the <u>equivalence class</u> $[a]_R$ of a by

$$[a]_R = [a] = \{x \in A : xRa\}$$

Ex.3 Let R be the equivalence on $\mathbb{Z}$ defined by aRb if $a-b$ is a multiple of 4. Then

$$[0] = \{x \in \mathbb{Z} : xR0\} = \quad x \in$$
$$= \{x \in \mathbb{Z} : a-0 \text{ is a multiple of } 4\}$$
$$= \{4k : k \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$

Similarly,

$$[1] = \{4k+1 : k \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$[2] = \{4k+2 : k \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$[3] = \{4k+3 : k \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

We will later see that these are all the equivalence classes of R, i.e., if $x \in \mathbb{Z}$, then $[x] = [0], [1], [2]$, or $[3]$.

Def A family $\mathcal{F}$ of subsets of the set A is a <u>partition of A</u> if

(a) each element of $\mathcal{F}$ is non-empty, i.e. $(\forall x \in \mathcal{F})(x \neq \emptyset)$,

(b) the union of $\mathcal{F}$ is A, i.e. $\bigcup_{x \in \mathcal{F}} x = A$.

and (c) the elements of $\mathcal{F}$ are pair-wise disjoint, i.e., $(\forall x, y \in \mathcal{F})\,[x \neq y \rightarrow x \cap y = \emptyset]$.

Ex 4 Let $A = \{1,2,3,4\}$ and put
$\mathcal{F}_1 = \{\{1,2\},\{3\},\{4\}\}$, $\mathcal{F}_2 = \{\{1,2\},\{4\}\}$,
$\mathcal{F}_3 = \{\{1,2\},\{2,3\},\{4\}\}$, & $\mathcal{F}_4 = \{\{1\},\{2,3,4\},\emptyset\}$.
Then $\mathcal{F}_1$ is a partition of A — but $\mathcal{F}_2$, $\mathcal{F}_3$ & $\mathcal{F}_4$ are not partitions of A.

Note: The set of equivalence classes $\mathcal{F} = \{[0],[1],[2],[3]\}$ of K in Ex. 3 is a partition of $\mathbb{Z}$.

Prop. 7 Let R be an equivalence relation on A and $a, b \in A$. Then $a \in [b] \Leftrightarrow [a] = [b]$.

Proof: ($\Leftarrow$): Suppose $[a] = [b]$. Since R is an equivalence relation, R is reflexive. So aRa. $\therefore$ $a \in [a] = \{x : xRa\}$. But $[a] = [b]$, so $a \in [b]$. $\therefore$ $[a] = [b] \Rightarrow a \in [b]$.

($\Rightarrow$): Now suppose $a \in [b]$. Then aRb by the definition of $[b]$. Since R is symmetric it follows that bRa. We will show that $[a] = [b]$. Let $x \in [a]$. Then xRa by definition of $[a]$. So $xRa \wedge aRb$ (from above). Since R is transitive, it follows that xRb. $\therefore$ $x \in [b]$. Hence $[a] \subseteq [b]$ --- (1)
Now let $x \in [b]$. Then xRb by the definition of $[b]$. So $xRb \wedge bRa$ (from above). Since R is transitive, it follows that xRa. $\therefore$ $x \in [a]$ Hence $[b] \subseteq [a]$ .... (2). From (1) & (2), we get $[a] = [b]$ $\therefore$, $a \in [b] \Rightarrow [a] = [b]$.

$\therefore \quad a \in [b] \Leftrightarrow [a] = [b]$

<u>Def.</u> Let R be an equivalence relation on A. We define $A \pmod R$ by $A/R = \{[a] : a \in A\}$.

<u>Ex.5</u> Let R be the relation defined on $\mathbb{Z}$ by aRb if $a-b$ is an integer multiple of 6. Then R is an equivalence relation and $\mathbb{Z}/R = \{[0], [1], [2], [3], [4], [5]\}$.

<u>Theorem 8</u> Let R be an equivalence relation on A. Then A/R is a partition of A.

<u>Proof:</u> (a) Let $X \in A/R$. Then $X = [a]$ for some $a \in A$. Since R is reflexive, aRa. So $a \in [a]$. $\therefore a \in X$. Thus $X \neq \emptyset$. $\therefore$ each element of A/R is non-empty.

(b) Now suppose $X, Y \in A/R$ and $X \neq Y$. Then we can find an $a \in A$ and a $b \in B$ such that $X = [a]$ & $Y = [b]$. Now if $X \cap Y \neq \emptyset$, then we can find a $c \in X \cap Y = [a] \cap [b]$. So $c \in [a]$ & $c \in [b]$. But from Prop. 7, it will follow that $[c] = [a]$ & $[c] = [b]$. Hence $[a] = [b]$, i.e., $X = Y$ — a contradiction. So if $X \neq Y$, then $X \cap Y = \emptyset$. Thus the elements of A/R are all pairwise disjoint.

(c) Finally, suppose $c \in A$. Then $c \in [c]$ and $[c] \in A/R$. So $c \in \bigcup_{X \in A/R} X$. $\therefore A \subseteq \bigcup_{X \in A/R} X$.

(c) Also if $c \in \bigcup_{X \in A/R} X$, then $c \in X$ for some $X \in A/R$. Since $X = [a]$ for some $a \in A$, $X \subseteq A$. So $c \in X \subseteq A$ and thus $c \in A$. $\therefore \bigcup_{X \in A/R} X \subseteq A$.
$\therefore A = \bigcup_{X \in A/R} X$. Hence A is the union of the elements of A/R.
From (a), (b), & (c) we can conclude that A/R is a partition of A.

<u>Ex. 6</u> Let S be the equivalence relation on $\mathbb{Z}$ defined by aSb if $a^2 - b^2$ is an integer multiple of 9. Find the equivalence classes into which S partitions $\mathbb{Z}$.

<u>Sol.</u> First observe that if $a-b$ is an integer multiple of 9, then $a^2-b^2 = (a-b)(a+b)$ will also be an integer multiple of 9. So we only need to look at the equivalence classes

$[0]_R$, $[1]_R$, $[2]_R$, $[3]_R$, $[4]_R$, $[5]_R$, $[6]_R$, $[7]_R$, $[8]_R$

$aRb \Leftrightarrow a-b$ is an integer multiple of 9

Now $8^2 - 1^2 = 64 - 1 = 63 = 9(7)$. $\therefore 8 S 1$
$7^2 - 2^2 = 49 - 4 = 45 = 9(5)$. $\therefore 7 S 2$
$6^2 - 3^2 = 36 - 9 = 27 = 9(3)$. $\therefore 6 S 3$
$5^2 - 4^2 = 25 - 16 = 9 = 9(1)$. $\therefore 5 S 4$
$3^2 - 0^2 = 9 - 0 = 9 = 9(1)$. $\therefore 3 S 0$.

$\therefore [8] = [1]$, $[7] = [2]$, $[6] = [3] = [0]$, and $[5] = [4]$.
Since $[0]$, $[1]$, $[2]$, & $[4]$ are all disjoint, $\mathbb{Z}/S$ is

$[0]_S = \{3k : k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}$
$[1]_S = \{9k \pm 1 : k \in \mathbb{Z}\} = \{\ldots, -8, -1, 1, 8, 10, 17, \ldots\}$
$[2]_S = \{9k \pm 2 : k \in \mathbb{Z}\} = \{\ldots, -7, -2, 2, 7, 11, 16, \ldots\}$
$[4]_S = \{9k \pm 4 : k \in \mathbb{Z}\} = \{\ldots -5, -4, 4, 5, 13, 14, \ldots\}$.

Ex.6. Since $\{[0], [1], [2], [4]\}$ is indeed a partition of $\mathbb{Z}$, we can be sure that these are the equivalence classes into which S partitions $\mathbb{Z}$.

Ex.7 Let T be the equivalence relation on $\mathbb{Z}$ defined by aTb if $a^3 - b^3$ is an integer multiple of 8. Find the equivalence classes into which T partitions $\mathbb{Z}$.

Sol. $\mathbb{Z}/T = \{[0]_T, [1]_T, [3]_T, [5]_T, [7]_T\}$ where

$[0]_T = \{2k : k \in \mathbb{Z}\} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, 8, \cdots\}$

$[1]_T = \{8k+1 : k \in \mathbb{Z}\} = \{\cdots, -15, -7, 1, 9, 17, \cdots\}$

$[3]_T = \{8k+3 : k \in \mathbb{Z}\} = \{\cdots, -13, -5, 3, 11, 19, \cdots\}$

$[5]_T = \{8k+5 : k \in \mathbb{Z}\} = \{\cdots, -11, -3, 5, 13, 21, \cdots\}$

$[7]_T = \{8k+7 : k \in \mathbb{Z}\} = \{\cdots, -9, -1, 7, 15, 23, \cdots\}$

Theorem 9: Let $\mathcal{P}$ be any partition of the set A. Then there is a unique equivalent relation R such that $A/R = \mathcal{P}$.

Proof: Let $R = \bigcup_{X \in \mathcal{P}} X \times X$. Then we just have to verify that R is an equivalence relation and that the equivalence classes turn out to be the elements of the partition $\mathcal{P}$. But this will take a long time – so we'll skip it.

Ex.8 Let $\mathcal{P} = \{\{1,2\}, \{3\}, \{4,5\}\}$. Then $\mathcal{P}$ is a partition of $\{1,2,3,4,5\}$. If we let

$R = \{(1,1), (1,2), (2,1), (2,2)\} \cup \{(3,3)\} \cup \{(4,4), (4,5), (5,4), (5,5)\}$

then we can check that R is an equivalence relation & $\{1,2,3,4,5\}/R = \mathcal{P}$.

§4. Modulo Arithmetic

Def. Let $n \in \mathbb{N}$ be fixed. Define the relation R_n on $\mathbb{Z}$ by aR_nb if $a-b$ is an integer multiple of n. Then R_n is an equivalence relation on $\mathbb{Z}$ and the set of equivalence classes into which R_n partitions $\mathbb{Z}$ are given by

$$\mathbb{Z}/R_n = \mathbb{Z}_n = \{[0],[1],[2],\ldots,[n-1]\} \text{ for } n \geq 1$$

and $\mathbb{Z}/R_0 = \mathbb{Z}_0 = \{\ldots,[-1],[0],[1],[2],\ldots\}$.

Note Although $\mathbb{Z}\,(\text{mod}\,R_n) = \mathbb{Z}/R_n = \{[a] : a \in \mathbb{Z}\}$ might look like an infinite set, it is actually a finite set for all $n \geq 1$. Only $\mathbb{Z}_0$ is finite.

Notation: We usually call the relation R_n, the modulo n relation and write aR_nb as $a \equiv_n b$. We also often use the elements between 0 & $n-1$ to denote the equivalence $[a] = \{nk+a : a \in \mathbb{Z}\}$. So, for example, we say that $23 \equiv 5 \pmod 6$, instead of $23 \equiv_6 5$, and that $[23]_6 = 5$.

We can define the operations $+$, $-$, and $\cdot$ on $\mathbb{Z}_n$ and $\mathbb{Z}_n$ with these operations is called modulo n arithmetic. We define $[a]+[b]=[a+b]$, $[a]-[b]=[a-b]$, and $[a]\cdot[b]=[a\cdot b]$. Note that exponentiation is not defined on $\mathbb{Z}_n$ because $[a]^{[b]} \not\equiv_n [a^b]$ in general. For example, $2^5 = 32 \equiv 2 \pmod 3$ but $2^{5 \pmod 3} = 2^2 = 4 \equiv 1 \pmod 3$. So if $b \equiv c \pmod n$, it does not always follow that $a^b \equiv a^c \pmod n$. If $b \equiv c \pmod n$ and $k \geq 0$, then we always have that $b^k \equiv c^k \pmod n$.

END