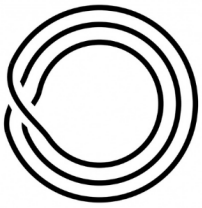

Informal Notes on Mathematics
2021.02.06

Relations, Products and Intergers

This chapter includes Section 0.4 to 0.6 of the original book.

Definition 2.0.1. The *Cartesian product* of sets (or classes) A and B is the set (class)

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

A subset (subclass) of R is a relation on $A \times B$.

Definition 2.0.2. A relation R on $A \times A$ is an equivalence relation on A provided R is

(i) reflexive: $(a, a) \in R$ for all $a \in A$.

(ii) symmetric: $(a, b) \in R$ implies $(b, a) \in R$.

(iii) transitive: $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$.

If $(a, b) \in R$ for equivalence relation R then we denote this as $a \sim b$. For $a \in A$, the *equivalence class* if a is the class $\overline{a}$ of all elements of A which are equivalent to a. The class of all equivalence classes in A is denoted A/R (called the *quotient class* of A by R).

Proposition 2.0.3 Since R is reflexive, $a \in \overline{a}$ for every $a \in A$; then

$$\overline{a} \neq \emptyset \text{ for every } a \in A \tag{2.1}$$

$$\bigcup_{a \in A} \overline{a} = A = \bigcup_{\overline{a} \in A/R} \overline{a} \tag{2.2}$$

And also,

$$\overline{a} = \overline{b} \iff a \sim b \tag{2.3}$$

Lemma 2.0.4
For $a, b \in R$ and R an equivalence relation on $A \times A$, we have either $\overline{a} \cap \overline{b} = \emptyset$, or $\overline{a} = \overline{b}$.

Definition 2.0.5. Let A be a nonempty class and $\{A_i \mid i \in I\}$ a family of subsets of A such that:

(i) $A_i \neq$ for all $i \in I$

(ii) $\bigcup_{i \in I} A_i = A$

(iii) $A_i \cap A_j = \emptyset$ for all $i \neq j$ where $i, j \in I$

Then $\{A_i \mid i \in I\}$ is a *partition* of A.

Note 2 — This is one of the most useful properties of an equivalence relation. We will meet it again when we study Section I.4.

Definition 2.0.6. Let $\{A_i \mid i \in I\}$ be a family of sets indexed by a nonempty set I (1.0.4). The *Cartesian product* of the sets A_i is the set of all functions $f : I \to \bigcup_{i\in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$. The set of functions is denoted $\prod_{i\in I} A_i$

If $I = \{1, 2, ..., n\}$, the product $\prod_{i\in I} A_i$ is often denoted by $A_1 \times A_2 \times ... \times A_n$ and is identified with the set of all ordered n-tuples $(a_l, a_2, ..., a_n)$, where $a_i \in A_i$ for $i = 1, 2, ...,$ n just as in the case mentioned above, where $I = \{1, 2\}$.

Note 3 — If $I = \{1, 2\}$ and we have sets A_1 and A_2, then the Cartesian product $A_1 \times A_2$ consists of all pairs$\{(a1, a2) \mid a_1 \in A_1, a_2 \in A_2\}$. We can associate this with a function $f : I \to A_1 \cup A_2$ where $f(1) \in A_1$ and $f(2) \in A_2$.So function f is "associated" with pair $(f(1), f(2))$ (and conversely).

Definition 2.0.7. Let $\prod_{i\in I} A_i$ be a Cartesian product. For each $k \in I$ define a map $\pi_k : \prod_{i\in I} A_i \to A_k, f \mapsto f(k)$ (or in another notation, $\{a_i\} \to a_k$), then π_k is called the *(canonical) projection* of the product onto its k_{th} component.

Example 2.0.8

Let $i = \mathbb{R}$ and $A_i = \mathbb{C}$ for all $i \in I$. Then an element of $\prod_{k\in I} A_k = \prod_{k\in I} \mathbb{C}$ is a function f that maps $\mathbb{R} \to \mathbb{C}$. Say $f(x) = ix$. Applying π_k to f (where $k \in I = \mathbb{R}$) gives $\pi_k(f) = f(k) = ik$.

Theorem 2.0.9

Let $\{A_i \mid i \in I\}$ be a family of sets indexed by I. Then there exists a set D, together with a family of maps $\pi_i : D \to A_i \mid i \in I$ with the following property: For any set C and family of maps $\phi_i : C \to A_i \mid i \in I$, there exists a unique map $\phi : C \to D$ such that $\pi_i\phi = \phi_i$ for all $i \in I$. Furthermore, D is uniquely determined up to a bijection.

Note 4 — Appears! Universal property! It will have much use when we start learning category (in Section I.7, but we'll meet it in Jacky's salon later). The proof is a bit long and difficult to understand in a short time, so we may put off it until we have the systematic learning.

Now we comes to the integers. The system we use is that of five axioms by Italian mathematician Giuseppe Peano in 1899.

Axiom 1. 0 is a number.

Axiom 2. The immediate successor of a number is a number.

Axiom 3. 0 is not the immediate successor of a number.

Axiom 4. No two numbers have the same immediate successor.

Axiom 5. Any property belonging to 0, and also to the immediate successor of every number that has the property, belongs to all numbers.

Axiom 5 is called the Principle of Mathematical Induction.

Theorem 2.0.10 (Principle of Mathematical Induction)

If S is a subset of the set $\mathbb{N} \cup \{0\}$ such that $0 \in S$ and either

(i) $n \in S$ implies $n + 1 \in S$ for all $n \in \mathbb{N} \cup \{0\}$, or

(ii) $m \in S$ for all $0 \leq m < n$ implies $n \in S$ for all $n \in \mathbb{N} \cup \{0\}$, then $S = \mathbb{N} \cup \{0\}$.

Proof. If $\mathbb{N} - S \neq \emptyset$, let $n \neq 0$ be its least element. Then for every $m < n$, we must have $m \notin \mathbb{N} - S$ and hence $m \in S$. Consequently either (i) or (ii) implies $n \in S$, which is a contradiction. Therefore $\mathbb{N} - S = \emptyset$ and $\mathbb{N} = S$. □

Theorem 2.0.11 (Division Algorithm)

If $a, b \in \mathbb{Z}$ and $a \neq 0$, then there exist unique integers q and r such that $b = aq+r$,and $0 \leq r < |a|$.

Definition 2.0.12. Integer $a \neq 0$ *divides* an integer b(written $a|b$) if there is an integer k such that $ak = b$. If a does not divide b we write $a \nmid b$.

Definition 2.0.13. The positive integer c is *the greatest common divisor* of the integers $a_1, a_2, ..., a_n$ if

- $c|a_i$ for $1 \leq i \leq n$
- $d \in \mathbb{Z}$ and $d|a_i$ for $1 \leq i \leq n$ implies $d|c$.

c is denoted $(a_1, a_2, ..., a_n)$

Definition 2.0.14. Let $m > 0$ be a fixed integer. If $a, b \in \mathbb{Z}$ and $m|(a - b)$ then a is *congruent to b modulo m.*

Theorem 2.0.15

Let $m > 0$ be an integer and $a, b, c, d \in \mathbb{Z}$.

(i) Congruence modulo m is an equivalence relation on $\mathbb{Z}$, which has precisely m equivalence classes.

(ii) If $a \equiv b(\text{mod}m)$ and $c \equiv d(\text{mod}m)$, then $a + c \equiv b + d(\text{mod}m)$ and $ac \equiv bd(\text{mod}m)$.

(iii) If $ab \equiv ac(\text{mod}m)$ and a and m are relatively prime, then $b \equiv c(\text{mod}m)$.

Proof. Left as exercise. □