Abstract Algebra A

`soupless`

January 23, 2024

Contents

Lecture 1: Sets and relations

Definition 1.1 (Cartesian product)

Let A and B be sets. The *Cartesian product* of A and B, denoted by $A \times B$, is defined as

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

Definition 1.2 (Relation)

A relation R between sets A and B is a subset of $A \times B$. That is, $R \subseteq A \times B$.

We let $aRb \equiv (a, b) \in \mathbb{R}$ for each $a \in A$ and $b \in B$ where R is a relation. It is an implicit assumption that A and B have to be nonempty, otherwise, the relation is trivial.

Theorem 1.1

If A and B are finite sets, then there are $2^{|A| \cdot |B|} - 1$ relations.

Proof: Let A and B be finite sets. Then, the question is equivalent to finding the number of subsets of $A \times B$, which is $|\mathcal{P}\left(A \times B\right)| - 1 = 2^{|A \times B|} - 1 = 2^{|A| \cdot |B|} - 1$. ■

Definition 1.3 (Function)

A function ϕ mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly one ordered pair $(x, y) \in \phi$ for all $y \in Y$.

Definition 1.4 (Domain, codomain, range)

Let $\phi : X \to Y$ be a function mapping X to Y. Then,

- X is the domain of ϕ,
- Y is the codomain of ϕ,
- $\phi[X]$ is the range of ϕ such that $\phi[X] = \{\phi(x) \ | \ x \in X\}$.

Another notation would be $X \xrightarrow{\phi} Y$ to denote the type signature, and $x \xmapsto{\phi} y$ to denote the function definition.

Definition 1.5 (Injective function)

A function $\phi : X \to Y$ is *injective* or one-to-one (1-1) if, for all elements x_1 and x_2 of X, $\phi(x_1) = \phi(x_2)$ implies $x_1 = x_2$.

Example: Let $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = 2x + 3$ for all $x \in \mathbb{R}$. Is f injective?

Let x_1 and x_2 be arbitrary elements of $\mathbb{R}$, and suppose that $f(x_1) = f(x_2)$. Then,

$$\begin{aligned} f(x_1) &= f(x_2) \\ 2x_1 + 3 &= 2x_2 + 3 \\ 2x_1 &= 2x_2 \\ x_1 &= x_2 \end{aligned}$$

Hence, f is injective.

Example: Let $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = x^2$ for all $x \in \mathbb{R}$. Is g injective?

No, because $g(-1) = 1$, and $g(1) = 1$, but $-1 \neq 1$.

Definition 1.6 (Surjective function)

A function $\phi : X \to Y$ is surjective or onto if $\phi[X] = Y$. Equivalently, $\forall y \in Y \; \exists x \in X (\phi(x) = y)$.

Example: Let $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = x^2$ for each $x \in \mathbb{R}$. Is F surjective?

Since $F(x) \geq 0$ for all $x \in \mathbb{R}$, then $F(x) = -1$ has no solution. Hence, F is not surjective.

Example: Let $G : \mathbb{N} \to \mathbb{N}$ such that $G(x) = x + 1$ for each $x \in \mathbb{N}$. We define $\mathbb{N} = \{1, 2, 3, \ldots\}$. Is G surjective?

No, because $G(x) = 1$ has no solution in $\mathbb{N}$. Hence, G is not surjective.

Example: Let $\phi : \mathbb{N} \to \mathbb{N}$ such that $\phi(n)$ is the nth prime number for each $n \in \mathbb{N}$. Then, ϕ is injective. However, it is not surjective, because $\phi(x) = 4$ has no solution.

Example: Let $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = x + 1$ for each $x \in \mathbb{R}$. Prove that g is surjective.

Let $y \in \mathbb{R}$ be arbitrary. Then, $g(x) = y \implies x + y = 1 \implies x = y - 1$. Since $g(y - 1) = y - 1 + 1 = y$, this means g is surjective.

Definition 1.7 (Bijective function)

If $\phi : X \to Y$ is both injective and surjective, then ϕ is bijective.

Definition 1.8 (Inverse)

Let $\phi : X \to Y$ be a bijective function. The inverse of ϕ, denoted by ϕ^{-1}, is the function $\phi^{-1} : Y \to X$ such that $\phi^{-1}(y) = x \Leftrightarrow \phi(x) = y$ for all $x \in X$ and $y \in Y$.

A representation for finite domain maps would be through a matrix representation like

$$\phi : \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ \phi(x_1) & \phi(x_2) & \cdots & \phi(x_n) \end{bmatrix}$$

Definition 1.9 (Function composition)

Let $\phi : A \to B$ and $\theta : B \to C$ be functions. The composition $\theta\phi$ is the function $\theta\phi : A \to C$ defined by $\theta\phi(a) = \theta(\phi(a))$ for each $a \in A$.

Definition 1.10 (Function equality)

Let $f : X \to Y$ and $g : X \to Y$. Then, $f = g$ if $\forall x \in X \, (f(x) = g(x))$.

Theorem 1.2

Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then:

1. $(\gamma\beta)\alpha = \gamma(\beta\alpha)$. That is, function composition is associative.
2. If α and β are both injective, then $\beta\alpha$ is injective.
3. If α and β are both surjective, then $\beta\alpha$ is also surjective.

Proof: We prove each property listed in the theorem:

- Suppose we have the functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$. Let $a \in A$ be arbitrary. Then,

$$(\gamma\beta)\alpha(a) = \gamma\beta(\alpha(a))$$

$$(\gamma\beta)\alpha(a) = \gamma\left(\beta\left(\alpha(a)\right)\right)$$

$$\begin{aligned}\gamma(\beta\alpha)(a) &= \gamma\left(\beta\alpha(a)\right)\\ \gamma(\beta\alpha)(a) &= \gamma\left(\beta\left(\alpha(a)\right)\right)\end{aligned}$$

Hence, $(\gamma\beta)\alpha(a) = \gamma(\beta\alpha)(a)$. Therefore, $(\gamma\beta)\alpha = \gamma(\beta\alpha)$.

- Let $\alpha : A \to B$ and $\beta : B \to C$ be injective functions. Then, $\beta\alpha : A \to C$. Suppose that for all $a_1, a_2 \in A$, $\beta\alpha(a_1) = \beta\alpha(a_2)$. We get the following derivation:

$$\begin{aligned}\beta\alpha(a_1) &= \beta\alpha(a_2)\\ \beta\left(\alpha(a_1)\right) &= \beta\left(\alpha(a_2)\right)\\ \alpha(a_1) &= \alpha(a_2)\\ a_1 &= a_2\end{aligned}$$

  Therefore, $\beta\alpha$ is injective.

- Let $\alpha : A \to B$ and $\beta : B \to C$ be surjective functions. Let $c \in C$ be arbitrary. Then, there exists $b \in B$ such that $\beta(b) = c$. Since α is surjective, there exists $a \in A$ such that $\alpha(a) = b$. Then, $\beta(b) = \beta(\alpha(a)) = \beta\alpha(a) = c$. Hence, there exists $a \in A$ such that $\beta\alpha(a) = c$, and so for all $c \in C$, there exists $a \in A$ such that $\beta\alpha(a) = c$. Therefore, $\beta\alpha$ is surjective. ■

Lecture 2: Sets and relations, continued

Theorem 2.1

Let $\alpha : A \to B$ be a bijective function. Then there exists a function $\theta : B \to A$ such that $\forall a \in A\,(\theta\alpha(a) = a)$ and $\forall b \in B\,(\alpha\theta(b) = b)$. The function θ is called the inverse of α and is denoted by $\theta = \alpha^{-1}$.

Proof: Suppose $\alpha : A \to B$ is a bijective function. Construct a function $\theta : B \to A$ satisfying the properties $\forall a \in A\,(\theta\alpha(a) = a)$ and $\forall b \in B\,(\alpha\theta(b) = b)$. We define $\theta : B \to A$ by $\theta(b) = a$ iff $\alpha(a) = b$.

Let $a \in A$ be arbitrary. Consider $\theta\alpha(a)$. Suppose $\alpha(a) = b$. Then, $\theta\alpha(a) = \theta(\alpha(a)) = \theta(b) = a$.

Let $b \in B$ be arbitrary. Consider $\alpha\theta(b)$. Suppose $\theta(b) = a$. Then, $\alpha\theta(b) = \alpha(\theta(b)) = \alpha(a) = b$. ■

Definition 2.1 (Identity function)

The identity function is a function having the same domain and codomain such that $x \mapsto x$ for all x in the domain.

Theorem 2.2

Let $\alpha : A \to B$ be a bijective function. Then, $\alpha^{-1} : B \to A$ is bijective.

Proof: We first prove that α^{-1} is injective. Let b_1, b_2 be arbitrary elements from B, and suppose that $\alpha^{-1}(b_1) = \alpha^{-1}(b_2)$. Then,

$$\alpha^{-1}(b_1) = \alpha^{-1}(b_2)$$
$$\alpha\alpha^{-1}(b_1) = \alpha\alpha^{-1}(b_2)$$
$$b_1 = b_2$$

Hence, α^{-1} is injective.

We now prove that α^{-1} is surjective. Let $a \in A$. We know that $\alpha^{-1}\alpha(a) = a$. Since $\alpha(a) \in B$, this means that there is an element $b \in B$ such that $\alpha^{-1}(b) = a$. Hence, for all $a \in A$, there exists an element $b \in B$ such that $\alpha^{-1}(b) = a$, and so α^{-1} is surjective.

Therefore, α^{-1} is surjective. ■

Definition 2.2 (Equivalence relation)

R is called an equivalence relation on a set S if R is a relation from S to S and it satisfies the following:

1. $\forall a \in S(aRa)$.
2. $\forall a, b \in S(aRb \implies bRa)$.
3. $\forall a, b, c \in S(aRb \wedge bRc \implies aRc)$.

Example: Define R on $\mathbb{R}^*$ such that $aRb \Leftrightarrow ab > 0$ for all $a, b \in \mathbb{R}^*$. Let $a, b, c \in \mathbb{R}^*$ be arbitrary. Since $a \in \mathbb{R}^*$, we have $a \neq 0$, and since $x^2 > 0$ for all nonzero real numbers, we get $aa > 0$ which is equivalent to aRa. Thus, R is reflexive. Now, suppose aRb. Then, $ab > 0$. Multiplication under real numbers is commutative, hence, $ba > 0$, and so bRa. This means R is symmetric. Lastly, suppose aRb and bRc. Then, $ab > 0$ and $bc > 0$. We get $ab^2c > 0$, and dividing both sides by b^2, we get $ac > 0$. Hence, aRc, and so R is transitive.

Therefore, R is an equivalence relation.

Example: Define $\sim$ on $\mathbb{Z}$ by $a \sim b \Leftrightarrow a \equiv b \pmod 4$. We verify if $\sim$ is an equivalence relation on $\mathbb{Z}$.

We have $4 \mid 0 \implies 4 \mid a - a$, and so $a \equiv a \pmod 4$. Hence, $\sim$ is reflexive. Now, suppose $a \sim b$. Then, $4 \mid a - b \implies 4 \mid (-1)(a-b) \implies 4 \mid b - a$. Hence, $b \sim a$, and $\sim$ is symmetric. Lastly, suppose $a \sim b$ and $b \sim c$. Then, $4 \mid a - b$ and $4 \mid b - c$. We have $4 \mid a - b + b - c \implies 4 \mid a - c$. Hence, aRc, and so R is transitive.

Therefore, $\sim$ is an equivalence relation on $\mathbb{Z}$.

Definition 2.3 (Equivalence class)

Let $\sim$ be an equivalence relation on S. Let $a \in S$, The equivalence containing a, denoted by $[a]$, is the set defined by

$$[a] := \{x \in S \mid a \sim x\}.$$

Example: We have shown that R is an equivalence relation on $\mathbb{R}^*$. Finding the equivalence class containing 2,

$$\begin{aligned}
[2] &= \{x \in \mathbb{R}^* \mid 2Rx\}\\
[2] &= \{x \in \mathbb{R}^* \mid 2x > 0\}\\
[2] &= \{x \in \mathbb{R}^* \mid x > 0\}\\
[2] &= \mathbb{R}^+
\end{aligned}$$

Finding the equivalence class containing $\sqrt{2}$,

$$\begin{aligned}
[\sqrt{2}] &= \{x \in \mathbb{R}^* \mid \sqrt{2}Rx\}\\
[\sqrt{2}] &= \{x \in \mathbb{R}^* \mid \sqrt{2}x > 0\}\\
[\sqrt{2}] &= \{x \in \mathbb{R}^* \mid x > 0\}\\
[\sqrt{2}] &= \mathbb{R}^+
\end{aligned}$$

Finding the equivalence class containing $-e$,

$$\begin{aligned}
[-e] &= \{x \in \mathbb{R}^* \mid -eRx\}\\
[-e] &= \{x \in \mathbb{R}^* \mid -ex > 0\}\\
[-e] &= \{x \in \mathbb{R}^* \mid x < 0\}\\
[-e] &= \mathbb{R}^-
\end{aligned}$$

Example: We have shown that $\sim$ is an equivalence relation on $\mathbb{Z}$ where $a \sim b \Leftrightarrow a \equiv b \pmod 4$.

Finding the equivalence class containing a,

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} \mid x \sim a\}\\
[a] &= \{x \in \mathbb{Z} \mid x \equiv a \pmod 4\}\\
[a] &= \{x \in \mathbb{Z} \mid 4 \mid x - a\}\\
[a] &= \{x \in \mathbb{Z} \mid 4 \mid x - a\}\\
[a] &= \{x \in \mathbb{Z} \mid 4k = x - a, k \in \mathbb{Z}\}\\
[a] &= \{x \in \mathbb{Z} \mid 4k + a = x, k \in \mathbb{Z}\}\\
[a] &= \{4k + a \mid k \in \mathbb{Z}\}
\end{aligned}$$

Hence, the equivalence class containing 0 is just $\{4k \mid k \in \mathbb{Z}\}$. The equivalence class containing 1 is $\{4k+1 \mid k \in \mathbb{Z}\}$, $\{4k+2 \mid k \in \mathbb{Z}\}$ for the equivalence class containing 2, and $\{4k+3 \mid k \in \mathbb{Z}\}$ for the equivalence class containing 3. The equivalence class containing 5 is just $[1]$ since $5 \in [1]$. Finally, $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$.

Definition 2.4 (Partition, cells)

A partition P of a set S is a collection of nonempty disjoint subsets of S whose union is S. Each element of P is called a *cell*.

Example: In $\mathbb{Z}$, one such partition is $\left\{\mathbb{Z}^-, \mathbb{Z}^+, \{0\}\right\}$

Example: Let $S = \{1, 2, 3, 4, 5\}$. One partition would be $P_1 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$. Another partition would be $P_2 = \{\{1, 2\}, \{3\}, \{4\}, \{5\}\}$. The number of 2-cell partitions of S would be $\binom{5}{2}$.

Theorem 2.3

The equivalence classes of an equivalence relation on a set S constitute a partition of S.

Proof: Let $\sim$ be an equivalence relation on S. For any $a \in S$, we have $a \in [a]$. Let $a, b \in S$ such that $[a] \neq [b]$. There will be two cases:

- The intersection of $[a]$ and $[b]$ is nonempty. This means that there exists an element x in both $[a]$ and $[b]$. Then, $x \sim a$ and $x \sim b$, so $a \sim b$. Let $y \in S$ be arbitrary. Suppose $y \in [a]$. Then, $y \sim a$. Since $a \sim b$, then $y \sim b$, so $y \in [b]$. Hence, $[a] \subseteq [b]$. Similarly, suppose $y \in [b]$. Then, $y \sim b$. Then, $a \sim b$ implies $b \sim a$, so $y \sim a$. Hence, $y \in [a]$, and so $[b] \subseteq [a]$. Hence, $[a] = [b]$. This contradicts our assumption that $[a] \neq [b]$. Hence, $[a] \cap [b] = \emptyset$.
- The intersection of $[a]$ and $[b]$ is empty. Hence, $[a] \cap [b] = \emptyset$.

In either case, we get $[a] \cap [b] = \emptyset$.

Since each equivalence class is disjoint to another, and every element belongs to an equivalence class containing it, this means that the collection of all equivalence classes of S is a partition of S. ■