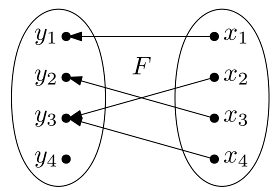
12 Transformations

Bijections

Definition. A *function* consists of a set called the *domain*, a set called the *codomain*, and a rule which assigns each element from the domain to one element of the codomain. If F is a function with domain X and codomain Y we write $F : X \to Y$.

Example: A function $F : \{x_1, \dots, x_4\} \to \{y_1, \dots, y_4\}$.

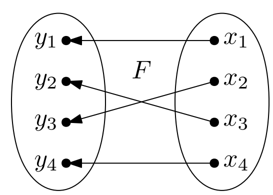


Definition. A function $F : X \to Y$ is *one-to-one* if every $x, x' \in X$ with $x \neq x'$ satisfy $F(x) \neq F(x')$. Equivalently, F is one-to-one if every $y \in Y$ is the image of at most element of X. We say that F is *onto* if every $y \in Y$ is the image of at least one element of X.

Note: The function in the previous example is not one-to-one since $f(x_2) = f(x_4) = y_3$. It is not onto since y_4 is not the image of any element in X.

Definition. A function $F : X \to Y$ is a *bijection* if it is both one-to-one and onto. Equivalently, F is a bijection if for every $y \in Y$ there is exactly one $x \in X$ with $F(x) = y$.

Example: A bijection $F : \{x_1, \dots, x_4\} \to \{y_1, \dots, y_4\}$.



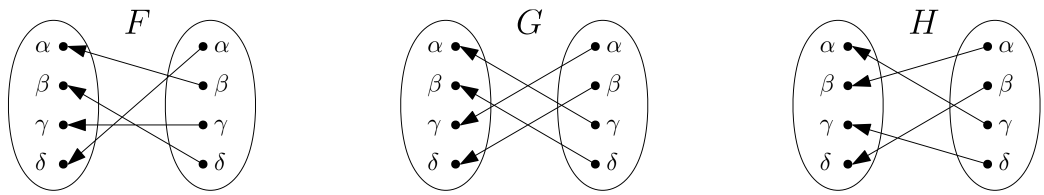
Notes:

- A bijection $F : X \to Y$ gives a correspondence between the elements of X and the elements of Y. Such a function can only exist when X and Y have the same size.
- If $F : X \to Y$ is a bijection, there is an inverse function $F^{-1} : Y \to X$ given by the rule that if $F(x) = y$ then $F^{-1}(y) = x$.

Transformations

Definition. For any set X a *transformation* of X is a bijection $F : X \to X$.[1] We define $\text{Trans}(X)$ to be the set of all transformations of X.

Example: Below are three transformations F, G, and H of the set $\{\alpha, \beta, \gamma, \delta\}$



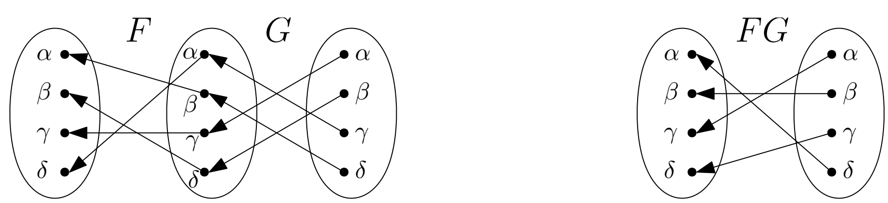
Features of $\text{Trans}(X)$**:**

Identity. We define the *identity* function on X to be the function $I_X : X \to X$ given by the rule $I_X(x) = x$ for every $x \in X$. Note that the identity is a bijection, so we have $I_X \in \text{Trans}(X)$. If the set X is clear from context we write I instead of I_X.

Product. If $F, G \in \text{Trans}(X)$ then the composition function $F \circ G$ is also a bijection from X to X. We use product notation for this composition, so we define $FG = F \circ G$. So, in short, if $F, G \in \text{Trans}(X)$ then $FG \in \text{Trans}(X)$. Since function composition is associative, we have $(FG)H = F(GH)$ whenever $F, G, H \in \text{Trans}(X)$.

Inverse. If $F \in \text{Trans}(X)$ then since F is a bijection it has an inverse function, denoted F^{-1} which is also in $\text{Trans}(X)$. Note that $FF^{-1} = I$ and $F^{-1}F = I$.

Example: Here we show the product of the transformations F, G from above



Note: An algebraic structure which has an identity, an associative product, and inverses is called a "group". Accordingly, we call $\text{Trans}(X)$ the *transformation group* of X.

[1]As a warning, this notation is not universal.

Algebra of Transformations

Lemma 12.1. *If* $A, B, B', C \in \text{Trans}(X)$ *and* $ABC = AB'C$*, then* $B = B'$

Proof. Starting with the equation $ABC = AB'C$ we may multiply both sides on the left by A^{-1}. This gives the equation $A^{-1}ABC = A^{-1}AB'C$ which simplifies to $BC = B'C$. Now multiplying both sides of this equation on the right by C^{-1} gives us $BCC^{-1} = B'CC^{-1}$ which simplifies to $B = B'$ giving us the result. □

Lemma 12.2. *If* $A, B \in \text{Trans}(X)$ *satisfy* $AB = I$ *then* $B = A^{-1}$.

Proof. This follows from the previous lemma and the equation $AB = I = AA^{-1}$. □

Lemma 12.3. *If* $A_1, \ldots, A_n \in \text{Trans}(X)$ *then* $(A_1A_2 \cdots A_n)^{-1} = A_n^{-1} \cdots A_2^{-1}A_1^{-1}$

Proof. This follows from the previous lemma and the equation

$$(A_n^{-1} \cdots A_2^{-1}A_1^{-1})(A_1A_2 \cdots A_n) = A_n^{-1} \cdots A_2^{-1}A_2 \cdots A_n = I.$$ □

Definition. Since we use multiplicative notation for composition, we make the following definitions for any $A \in \text{Trans}(X)$ and any positive integer n

(1) $A^n = \underbrace{AA \cdots A}_{n}$.

(2) $A^{-n} = \underbrace{A^{-1}A^{-1} \cdots A^{-1}}_{n} = (A^n)^{-1}$

(3) $A^0 = I$

So if $s, t \in \mathbb{Z}$ we have $(A^s)(A^t) = A^{s+t}$ (just like exponents for real numbers).