The Pidgeon Hole Principle

Let $P, H \subset \mathcal{U}$. If $|P| > |H|$ then here is no injective function $f : P \to H$; in other words, then for every function

$$f : P \to H$$

there are distinct points $p, p' \in P$ with $f(p) = f(p')$.

Example: If $S \subset \mathbb{Z}$ has $|S| \geq 37$ then there are two numbers $a, b \in S$ that have the same remainder modulo 36.
[**Writing $a = q36 + r$, $0 \leq r < 36$, r is the remainder of a modulo 36.**]

Example: **Any subset S of size 6 of the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ contains two numbers whose sum is 10.**
Proof: **Set $H \stackrel{\text{def}}{=} \{\{1, 9\}, \{2, 8\}, \{3, 7\}, \{4, 6\}, \{5\}\}$ and let the pidgeons fly.**

Example: **Let $S \subset \{1, 2, \ldots, 14\}$ with $|S| = 6$. For every $A \subseteq S$ set $s_A \stackrel{\text{def}}{=} \sum_{i \in A} i$. There are two subsets $A, B \subset S$ with $s_A = s_B$.**

Example: **A sequence $(a_1, a_2, \ldots, a_{n^2+1})$ of distinct reals contains an increasing or a decreasing subsequence of length $n + 1$.**

Example: **For $m \in \mathbb{N}$ odd there exists an $n \in \mathbb{N}$ with $m | (2^n - 1)$.**

Example: **During his 4–week vacation Herbert will play at least one set of tennis per day, but not more 40 sets total. Show that there exists a stretch of consecutive days during which he plays precisely 15 sets.**

Example: **During his 4–week vacation Herbert will play at least one set of tennis per day, but not more 40 sets total. Show that there exists a stretch of consecutive days during which he plays precisely 15 sets.**

Solution: **Let x_i denote the total number of sets played by the end of day i. Then**

$$1 \leq x_1 < x_2 < \ldots < x_{28} \leq 40 \leq 55 \quad \text{a}$$
$$1 \leq x_1{+}15 < x_2{+}15 < \ldots < x_{28}{+}15 \leq 40{+}15 = 55\,.$$

The two rows list a total of 56 blue numbers, all between 1 and 55. At least two of them must coincide. These two do not lie in the same row (why?). Thus there exist a x_j in the first row and a $x_i{+}15$ in the second row that are equal:

$$x_i{+}15 = x_j\,.$$

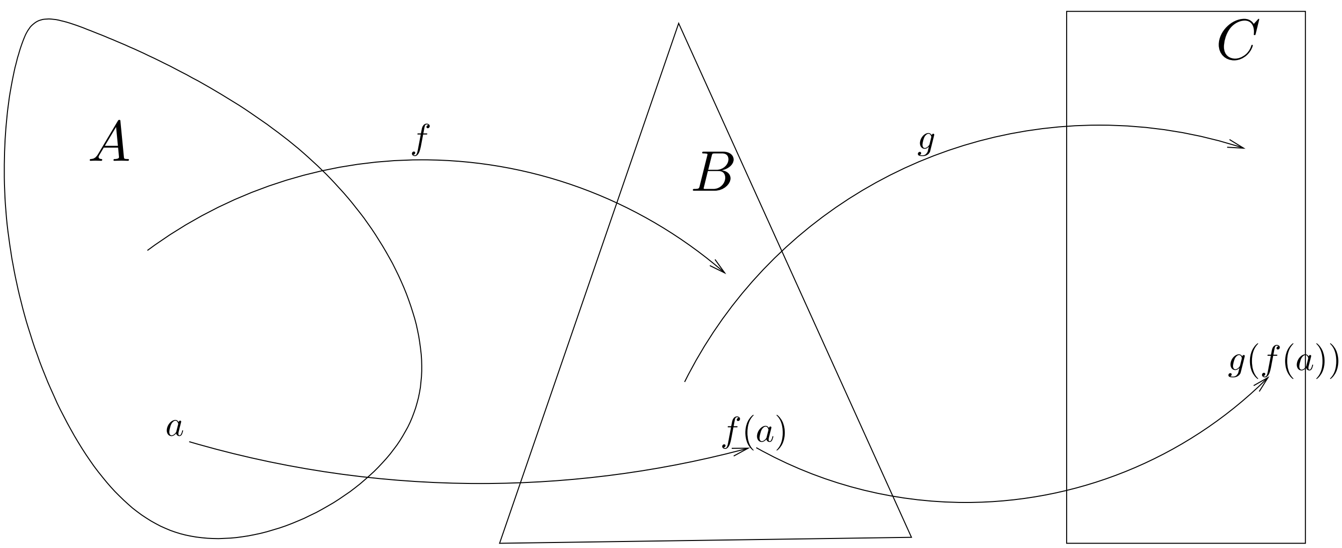
This means that on the (consecutive) days $i+1, \ldots, j$, Herbert played a total of 15 sets.

Composition of Functions

Definition: **Let** A, B, C **be sets and let** $f : A \to B$ **and** $g : B \to C$ **be functions. The** **Composition of** g **with** f **is the function**

$$g \circ f : A \to C \ , \ a \mapsto g(f(a)) \ .$$

It is pronounced "g **after** f**."**



Lemma: **Let** $A \xrightarrow{\text{f}} B \xrightarrow{\text{g}} C$**. Then**

a) $g \circ f$ injective $\Longrightarrow$ **f** injective

b) $g \circ f$ surjective $\Longrightarrow$ **g** surjective

Proof: **a) Let** $a, \overline{a} \in A$**. Then**

$$\begin{aligned} f(a) = f(\overline{a}) &\Longrightarrow g(f(a)) = g(f(\overline{a})) \\ &\Longleftrightarrow g \circ f(a) = g \circ f(\overline{a}) \\ &\Longrightarrow a = \overline{a} \ . \end{aligned}$$

b) Let $c \in C$**. As** $g \circ f$ **is surjective there is an** $a \in A$ **with** $c = g \circ f(a)$**. Then** $b \stackrel{\text{def}}{=} f(a) \in B$ **and** $g(b) = c$**.** **QED**

Theorem: **Let $A \xrightarrow{\text{f}} B \xrightarrow{\text{g}} C \xrightarrow{\text{h}} D$. Then**

$$(h \circ g) \circ f = h \circ (g \circ f) \; .$$

Proof: **Let $a \in A$. Then**

$$\begin{aligned} \big[\big(h \circ g\big) \circ f\big](a) &= \big(h \circ g\big)(f(a)) \\ &= h\big(g(f(a))\big) \\ &= h\big(g \circ f(a)\big) \\ &= \big[h \circ \big(g \circ f\big)\big](a) \; . \end{aligned}$$

Inverses

First recall the Identity Function I_A:

$$I_A : A \longrightarrow A \ , \ a \mapsto a \qquad \forall\, a \in A \ .$$

Clearly I_A is both injective and surjective.
Observation: If $f : A \longrightarrow B$ is a function then $\quad f \circ I_A = f \quad$ **and** $\quad I_B \circ f = f$.

Definition: Let $f : A \longrightarrow B$ be a function. A function $g : B \longrightarrow A$ is an Inverse of f if both

$$g \circ f = I_A \quad \text{and} \quad f \circ g = I_B \ .$$

Lemma: A function $f : A \longrightarrow B$ has at most one inverse.

Proof: If $g, \overline{g}$ are two inverses of f then

$$\begin{aligned} \overline{g} &= \overline{g} \circ I_B \\ &= \overline{g} \circ (f \circ g) \quad = (\overline{g} \circ f) \circ g \\ &= I_A \circ g = g \;. \end{aligned}$$

Definition: If a function $f : A \to B$ has an inverse we call f **invertible** and we may and will talk about **THE Inverse** of f, and denote it by f^{-1}.

Remark: $f^{-1} : \mathcal{P}[B] \to \mathcal{P}[A]$ is defined always, $f^{-1} : B \to A$ only if f is invertible.

Theorem: A function $f : A \to B$ is invertible if and only if it is bijective.

Proof of $\Longrightarrow$:

$$I_A = f^{-1} \circ f \text{ injective} \quad \Longrightarrow \quad f \text{ is injective} \;.$$

$$I_B = f \circ f^{-1} \text{ surjective} \quad \Longrightarrow \quad f \text{ is surjective} \;.$$

Proof of $\Longleftarrow$: **Assume then that** $f : A \to B$ **is bijective. We need a candidate for the inverse. The transposed relation comes to mind:**

$$g \stackrel{\text{def}}{=} f^T \stackrel{\text{def}}{=} \{(b,a) \in B \times A \,,\; (a,b) \in f\} \,.$$

g **certainly is a relation from** B **to** A**. Is it a function? Let** $b \in B$**. Since** f **is surjective, there exists an** $a \in A$ **with** $f(a) = b$**, i.e.,** $(b,a) \in g$**; since** f **is injective, there is only one such** $a \in A$**:** g **is, indeed a function.**
Is it an inverse of f**? Let** $a \in A$ **and set** $b \stackrel{\text{def}}{=} f(a)$**. Since** $(a,b) \in f$**,** $(b,a) \in g$**, i.e.,** $g(b) = a$**. That is to say** $g(f(a)) = a$**. Since this is true for abitrary** $a \in A$**, we get** $g \circ f = I_A$**.**
Let $b \in B$ **and set** $a \stackrel{\text{def}}{=} g(b)$**. That is,** $(b,a) \in$

g, which says $(a, b) \in f$ or $b = f(a)$. In other words $b = f(g(b))$ or $b = (f \circ g)(b)$. Since this is true for abitrary $b \in B$, we get $f \circ g = I_B$. Thus g is an (and then THE) inverse of f and deserves the name f^{-1}. QED

Theorem: **If** $f : A \to B$ **and** $g : B \to C$ **are both invertible then** $g \circ f : A \to C$ **is invertible and**

$$\left(g \circ f\right)^{-1} = f^{-1} \circ g^{-1} .$$

Proof:

Theorem: **If** $f : A \to B$ **and** $g : B \to C$ **are both invertible then** $g \circ f : A \to C$ **is invertible and**

$$\big(g \circ f\big)^{-1} = f^{-1} \circ g^{-1} \,.$$

Proof:

Set $h \stackrel{\text{def}}{=} f^{-1} \circ g^{-1} : C \to A$. **Then**

$$\begin{aligned}(g \circ f) \circ h &= (g \circ f) \circ (f^{-1} \circ g^{-1}) \\ &= g \circ \big(f \circ (f^{-1} \circ g^{-1})\big) \\ &= g \circ \big((f \circ f^{-1}) \circ g^{-1}\big) \\ &= g \circ \big(I_B \circ g^{-1}\big) \\ &= g \circ (g^{-1}) = I_C \,.\end{aligned}$$

Also,

$$\begin{aligned} h \circ (g \circ f) &= (f^{-1} \circ g^{-1}) \circ (g \circ f) \\ &= f^{-1} \circ \big(g^{-1} \circ (g \circ f)\big) \\ &= f^{-1} \circ \big((g^{-1} \circ g) \circ f\big) \\ &= f^{-1} \circ \big(I_B \circ f\big) \\ &= f^{-1} \circ f = I_A \,. \end{aligned}$$

The function h is therefore an (and then THE) inverse of $g \circ f$. **QED**