Announcements

Tentative chapter guide available on Piazza

Sets of Numbers

$\mathbb{N}$ = the natural numbers

$= \{1, 2, 3, 4, 5, \ldots\}$

$\mathbb{Z}$ = the integers

$= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$= \{\mathbb{N}, \{0\}, -\mathbb{N}\}$

$\mathbb{Q}$ = rational numbers

$= \left\{ \frac{a}{b} \;\middle|\; a, b \text{ are integers}, b \neq 0 \right\}$

$\mathbb{R}$ = "completion" of $\mathbb{Q}$

$= \{ \mathbb{Q}, \text{ irrational numbers} \}$

$\sqrt{2} \in \mathbb{R}, \quad \sqrt{2} \notin \mathbb{Q}$

$\mathbb{C}$ = complex or imaginary numbers

$$= \{ x + iy \mid x, y \text{ real}, i = \sqrt{-1} \}$$

$$i \in \mathbb{C}, \quad i \notin \mathbb{R}$$

Mathematical Notation

"$\forall$" = for every

"$\exists$" = there exists

"$\in$" = is an element of

"$\subseteq$" or "$\subset$" = is contained in

We have

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

and all inclusions are strict.

Techniques of Proof

1) Mathematical Induction

Bootstrap method:

Given a statement indexed by $\mathbb{N}$. Prove first for $n=1$, use that to prove $n=2$, use $n=2$ to prove $n=3$, etc.

2 Step Shortening

1) Prove for $n=1$.

2) Assume for $k=n$ (or equivalently, $\forall\, k \leq n$) in $\mathbb{N}$. Then prove for $k=n+1$.

Proposition: Suppose every polynomial with integer coefficients has a root. Then every polynomial of degree n has n roots (possibly repeated)

Proof:

1) $n=1$

A degree one polynomial is linear:

$$p(x) = ax+b, \quad a \neq 0.$$

A root is $-\frac{b}{a}$.

2) Assume true for $k=n$. Let p be a polynomial of degree $n+1$. By our initial assumption (hypothesis of proof), p has a root, call it α.

We may then factor

$$p(x) = (x-\alpha)\, q(x)$$

But q has degree n, so by our induction hypothesis, q has n roots. Therefore p has $n+1$ roots, and we are done. $\square$

Remark: The assumption that a polynomial of degree n has a root is true if the root is allowed to be complex, false otherwise! (see: Fundamental Theorem of Algebra)

Functions

If S and T are sets, a function $f: S \to T$ (read "f goes from S to T) is a rule that assigns to each $s \in S$ exactly one element $t \in T$.

S is called the domain of f.

T is called the codomain of f.

The set

$$f(S) = \{ t \in T \mid \exists\, s \in S,\ f(s) = t \}$$

is called the range of f.

Example: $f : \mathbb{R} \to \mathbb{R}$,

$$f(x) = x^2.$$

Domain of $f = \mathbb{R}$

Range of $f = \{x \in \mathbb{R},\ x \geq 0\}$

Codomain of $f = \mathbb{R}$

So range and codomain can be different!

Mapping Properties

$f: S \to T$ is injective

if for all $s_1, s_2 \in S$,

$f(s_1) = f(s_2)$ implies

$s_1 = s_2$.

Also called one-to-one or

monomorphism.

$f: S \to T$ is called surjective if for all $t \in T$, there exists $s \in S$, $f(s) = t$.

(codomain = range)

Also called onto or an epimorphism.

$f: S \to T$ is called a bijection if f is both injective and surjective.

Up to bijection, the cardinality of a given set is (roughly) the number of elements in the set, denoted by either $|S|$ or $\mathrm{Card}(S)$.

Two sets have the same cardinality whenever there exists a bijection between them.

2) Proof by Contradiction

Given a statement, assume the negation of its conclusion. Show this assumption leads to logical absurdities and so cannot be true. Therefore, your statement is true!

Theorem: If S is any set, then $\mathcal{P}(S)$ has cardinality greater than S.

Here, $\mathcal{P}(S)$ is the power set of S, the set of all subsets of S.

Proof: If $|S| = n < \infty$, then $|\mathcal{P}(S)| = 2^n$, and so the result is true trivially (try proving $|\mathcal{P}(S)| = 2^n$ by yourself, maybe using induction).

We then reduce to the case where $|S|$ is infinite.

By way of contradiction, suppose $|S|$ is infinite and $\exists$ bijection $f: S \to P(S)$.

Let $\boxed{T = \{x \in S \mid x \notin f(x)\}}$

i) $T = \{\emptyset\}$. Then $\forall x \in S$, $x \in f(x)$. So $f(x)$ is never the empty set, which implies $T \neq f(x)$

for any $x \in S$, contradicting the assumption that f is bijective.

ii) $T \neq \{\phi\}$. Then $T = f(y)$ for some $y \in S$.

Is $y \in T$?

If $y \in T$, then $y \in T = f(y)$

But $T = \{x \mid x \notin f(x)\}$, so

$y \notin T$, contradiction.

If $y \notin T = f(y)$,

then $y \in T$ by definition

of T, contradiction.

Therefore, there is no

$y \in S$ with $f(y) = T$

and so $|P(S)|$ is

greater than $|S|$. $\square$