Lecture 1, 8/26/21
Material corresponds to Ross, §$1-3$ and Appendix on Set Notation.

Numbers

Sets	Axioms
$\mathbb{N} = \{1, 2, 3, ...\}$	Induction Axiom
$\cap$	
$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$	
$\cap$	
$\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$	Ordered Field Axioms
$\cap$	
$\mathbb{R} = ...$	Ordered Field Axioms, Completeness Axiom

Ordered Field Axioms

The following hold with $\mathbb{Q}$ replaced by $\mathbb{R}$ as well:

Let $a, b \in \mathbb{Q}$. Then $a + b \in \mathbb{Q}$ and $ab \in \mathbb{Q}$.

- Addition is Commutative, Associative, has 0, and has additive inverses:
  $a + b = b + a$, $(a + b) + c = a + (b + c)$, $a + 0 = a$ and $a + (-a) = 0$.

- Multiplication is commutative, associative, distributive, has 1, and has multiplicative inverses (except 0):
  $ab = ba$, $(ab)c = a(bc)$, $a \cdot 1 = a$ and if $a \neq 0$, and $a(a)^{-1} = 1$.

For all $a, b \in \mathbb{Q}$ either $a \leq b$, $b \leq a$, or both.

- If $a \leq b$ and $b \leq a$ then $a = b$.
- If $a \leq b$ and $b \leq c$ then $a \leq c$.
- If $a \leq b$ then $a + c \leq b + c$
- If $a \leq b$ and $0 \leq c$ then $ac \leq bc$.

Induction Axiom

Let $S \subseteq \mathbb{N}$ be a set with the following properties:

- $1 \in S$
- If $n \in S$ then $n + 1 \in S$

Then $S = \mathbb{Z}$.

This is the basis for proof by induction. Suppose $P_1, P_2, P_3, ..., P_n, ...$ are a list of statements, for each $n \in \mathbb{N}$. If we can show that P_1 is true, and that if we assume P_n we can prove P_{n+1}, then we can conclude that P_n is true for all $n \in \mathbb{N}$. This follows because if $S = \{n \in \mathbb{N} | P_n \text{ is true } \}$ satisfies the bullet points in the Induction Axiom, and thus $S = \mathbb{N}$.

Algebraic Numbers

Rational Zeros Theorem:

Let $r \in \mathbb{Q}$ be a solution to the polynomial in x

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0$$

where $a_n, a_{n-1}, ..., a_1, a_0 \in \mathbb{Z}$. Then $r = p/q$ where p divides a_0 and q divides a_n.

Corollary:

Let $n, m \in \mathbb{Z}$ such that $n^{1/m} \in \mathbb{Q}$. Then $n = p^m$ for some $p \in \mathbb{Z}$.

Thus if n is not equal to p^m for any $p \in \mathbb{Z}$, it follows that $n^{1/m}$ is irrational (this is the "contrapositive" to the corollary).

Proof of corollary:

$n^{1/m}$ satisfies $x^m - n = 0$. By the rational zeros theorem, if $n^{1/m} \in \mathbb{Q}$, then $n^{1/m} = p/q$, $p, q \in \mathbb{Z}$, such that q divides 1. Thus $n^{1/m} = \pm p$ and $n = (\pm p)^m$.