MATH 110AH (Algebra)

September 24, 2022

1 9.23 Friday Week 0

Groups were invented by Évariste Galois circa 1830 to discuss symmetries in mathematical objects. For instance, the group G of "symmetries of equilateral triangles" contains a total of $3 \cdot 2 = 6$ elements consisting of rotations and reflections.

Theorem 1.0.1: 20th Century

Finite simple groups are classified.

Proving things about the integers

Try to use "simple" facts about the integers to prove complicated ones. Recall the number systems:

- the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$,
- the rational numbers $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$, and
- the real numbers $\mathbb{R}$ contains $\mathbb{Q}$, $\sqrt{2}, \pi, \ldots$, "all the points on the line."

Definition 1.0.2

A field $\mathbb{F}$ (e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, not $\mathbb{Z}$) is a set with elements $0, 1 \in \mathbb{F}$, $0 \neq 1$, and operators $+$ (addition) and $\cdot$ (multiplication), where for all $x, y \in \mathbb{F}$, $x + y, xy \in \mathbb{F}$, such that

1. $+$ is associative, commutative, 0 is its identity, and has inverses. That is,
   - $\forall\, x, y, z \in \mathbb{F} : (x + y) + z = x + (y + z)$,
   - $\forall\, x, y \in \mathbb{F} : x + y = y + x$,
   - $\forall\, x \in \mathbb{F} : 0 + x = x$, and
   - $\forall\, x \in \mathbb{F}\ \exists\, y \in \mathbb{F} : x + y = 0$, and writing $y = -x$.
2. $\cdot$ is associative, commutative, 1 is its identity, and nonzeros have inverse. That is,
   - $\forall\, x, y, z \in \mathbb{F} : (xy)z = x(yz)$,
   - $\forall\, x, y \in \mathbb{F} : xy = yx$,
   - $\forall\, x \in \mathbb{F} : 1 \cdot x = x$, and
   - $\forall\, x \in \mathbb{F} : x \neq 0 \implies \exists\, y \in \mathbb{F} : xy = 1$.
3. Distributive law: $\forall\, x, y, z \in \mathbb{F} : x(y + z) = xy + xz$.

Definition 1.0.3

An ordered field (for example, $\mathbb{R}, \mathbb{Q}$, not $\mathbb{C}$) $\mathbb{F}$ is a field with a given subset $P \subset \mathbb{F}$ called the positive elements such that

1. for all $x \in \mathbb{F}$, exactly one of $x \in P$, $x = 0$, $-x \in P$ is true (we say $x \in \mathbb{F}$ is negative if $-x \in P$), and
2. for all $x, y \in P$, $x + y, xy \in P$.

How to use these axioms to prove inequalities

Definition 1.0.4

For an ordered field $\mathbb{F}$, we say for $x, y \in \mathbb{F}$ that $x < y$ if $y - x = y + (-x)$ is positive (so x is positive iff $x > 0$).

Likewise $x \leq y$ if $y - x$ is positive or 0.

Lemma 1.0.5

1. For any $x, y \in \mathbb{R}$, exactly one of $x < y$, $x = y$, $x > y$ is true.
2. 1 is positive.
3. For $a, b, c \in \mathbb{R}$, if $a < b$ then $a + c < b + c$.
4. If $a, b, c \in \mathbb{R}$, $a \geq 0$, and $b \geq c$, then $ab \geq ac$.

Proof.

1. $y - x$ is either positive, negative, or 0.
2. Note that $1 \neq 0$. Then either 1 is positive or -1 is positive. If -1 is positive then $(-1)^2 = 1$ is positive, resulting in a contradiction.
3. Note that $(b + c) - (a + c) = b - a$ is positive.
4. Note that for all $a \in \mathbb{R}$ we have $0 \cdot a = 0$. Then

$$\begin{aligned} a(b - c) &\geq 0 \\ ab - ac &\geq 0 \\ ab &\geq ac. \end{aligned}$$

□

The big property of the integers is the inductive or well-ordering principle

The integers $\mathbb{Z}$ are a subset of $\mathbb{Q}$ (or $\mathbb{R}$). There are $0, 1 \in \mathbb{Z}$ and if $x, y \in \mathbb{Z}$ then $x + y, xy, -x \in \mathbb{Z}$.

Theorem 1.0.6: Well-ordering principle

Let $\mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\} = \{1, 2, 3, 4, \ldots\}$. Let S be a nonempty subset of $\mathbb{Z}^+$. Then S contains a smallest element, that is,

$$\exists\, x \in S\ \forall\, y \in S : x \leq y.$$

An example of what we can prove using this is:

Proposition 1.0.7

There is no integer N with $0 < N < 1$.

Proof. Let $S = \{n \in \mathbb{Z} : 0 < n < 1\}$. Let $S \neq \varnothing$, then by the well-ordering principle S has a smallest element N. Since $N < 1$, $N^2 < N \cdot 1 = N$. Since N^2 is also an integer, this is a contradiction. Then $S = \varnothing$, that is, there is no integer $N \in (0, 1)$. □

Theorem 1.0.8: Induction

For each $n \in \mathbb{Z}^+$, let $P(n)$ be a statement that could be true or false. Suppose $P(1)$ is true and that for any $n \in \mathbb{Z}^+$, if $P(n)$ is true then $P(n+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proof. Let $S = \{n \in \mathbb{Z}^+ : P(n) \text{ is false}\}$. Suppose $S \neq \varnothing$, then by the well-ordering principle S has a smallest element N. Since $P(1)$ is true, $N \neq 1$. Then $N > 1$. Then $N \geq 2$ since there are no integers in $(1, 2)$. Then $N - 1 \in \mathbb{Z}^+$. Since $P(N)$ would be true if $P(N-1)$ were true, $P(N-1)$ is not true. Then $N - 1 \in S$, a contradiction. Then $S = \varnothing$. □