

MATH 110AH (Algebra)

September 26, 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 1.1

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

Definition 1.2

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
 - $\forall x \in \mathbb{F} : x \neq 0 \Rightarrow \exists y \in \mathbb{F} : xy = 1$.
3. Distributive law: $\forall x, y, z \in \mathbb{F} : x(y + z) = xy + xz$.

Definition 1.3

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 1.4

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 1.5

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

$$a(b - c) \geq 0$$

$$ab - ac \geq 0$$

$$ab \geq ac.$$

□

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 1.6: Well-ordering principle

Let $\mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\} = \{1, 2, 3, 4, \dots\}$. 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 1.7

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

Proof. Let $S = \{n \in \mathbb{Z} : 0 < n < 1\}$. Let $S \neq \emptyset$, 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 $S = \emptyset$, that is, there is no integer $N \in (0, 1)$. \square

Theorem 1.8: 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 $S \neq \emptyset$, 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 $S = \emptyset$. \square

2 9.26 Monday Week 1

Lemma 2.1

For every $x \in \mathbb{R}$, $0 \cdot x = 0$.

Proof. By the distributive law, $0 = 0 + 0$, so for any $x \in \mathbb{R}$, we have

$$\begin{aligned} 0 \cdot x &= (0 + 0) \cdot x \\ 0 \cdot x + (-(0 \cdot x)) &= (0 + 0) \cdot x + (-(0 \cdot x)) \\ 0 &= 0 \cdot x. \end{aligned}$$

□

Lemma 2.2

For every $x \in \mathbb{R}$, $(-1) \cdot x = -x$.

Proof. Note that $0 = 0 \cdot x = (1 + (-1)) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x$. Adding $-x$ to both sides, we have $-x = (-1) \cdot x$. □

Lemma 2.3

For any $x, y, z \in \mathbb{R}$ with $x \neq 0$, if $xy = xz$, then $y = z$.

Proof. We know, since $x \neq 0$, there exists a real number \bar{x} such that $x(\frac{1}{x}) = 1$. Then if $xy = xz$, then $(\frac{1}{x})xy = (\frac{1}{x})xz$, so $1 \cdot y = 1 \cdot z$, that is, $y = z$. □

Proving things about the integer, gcd, prime factorization

Definition 2.4

For integers x and y , we say $x \mid y$ or “ x divides y ” or “ y is a multiple of x ” if $\exists z \in \mathbb{Z} : xz = y$. That is, if $x \neq 0$, $\frac{y}{x}$ is an integer.

Remark For any $x \in \mathbb{Z}$, $1 \mid x$. Also, for any $x \in \mathbb{Z}$, $x \mid 0$ since $x \cdot 0 = 0$.

Also, if x is a nonzero integer then any integer m with $m \mid x$ has $|m| \leq |x|$.

Example 2.5. The integers dividing $10 = 2 \cdot 5$ are $-10, -5, -2, -1, 1, 2, 5, 10$.

Remark One fact about \mathbb{R} is the Archimedean property: for every $x \in \mathbb{R}$, there exists an integer y with $x < y$. It follows, by multiplying by -1 , $\forall x \in \mathbb{R} \exists y \in \mathbb{Z} : y < x$.

Notation For any $x \in \mathbb{R}$, $\lfloor x \rfloor :=$ the largest integer $\leq x$ and $\lceil x \rceil :=$ the smallest integer $\geq x$.

This follows from well-ordering that a subset of \mathbb{Z} , bounded below and not empty, has a smallest element.

Definition 2.6

A subset $S \subset \mathbb{R}$ is **bounded below** if $\exists a \in \mathbb{R} \forall x \in S : x \geq a$.

Theorem 2.7: Division algorithm

Let x be a positive integer and y any integer. Then there are (unique) integers q and r such that $y = qx + r$, and $0 \leq r < x$.

Proof. Let $q = \left\lceil \frac{y}{x} \right\rceil (\in \mathbb{Z})$. Define $r = y - qx (\in \mathbb{Z})$. Clearly, $y = qx + r$. Here $q \leq \frac{y}{x}$, so $qx \leq y$ (since $x > 0$), so $r \geq 0$.

Also, $q + 1 > \frac{y}{x}$. So (since $x > 0$) $qx + x > y$, so $r = y - qx < x$. Since $r \in \mathbb{Z}$, $r \leq x - 1$. \square

Definition 2.8

A positive integer p is **prime** if $p > 1$ and the only positive integers dividing p are 1 and p .

Definition 2.9

For integers x and y not both 0, the **greatest common divisor** = $\gcd(x, y)$ is the largest integer that divides x and y .

That makes sense because $1 \mid x$ and $1 \mid y$, and (if $y \neq 0$), any integer dividing y is $\leq |y|$.

Theorem 2.10: Euclid, 300 BCE

For any integers x, y , not both 0, there are integers m, n with $\gcd(x, y) = mx + ny$.

Proof. The hypothesis and conclusion do not change if x or y is multiplied by -1 . Assume $x, y \geq 0$. By switching x and y if needed, assume $0 \leq x \leq y$ and $y > 0$ since they are not both 0.

We prove this by induction on y .

For $y = 1$, we have $x = 0$ or $x = 1$, and the conclusion is true: $\gcd(0, 1) = 1 = 0 \cdot 0 + 1 \cdot 1$ and $\gcd(1, 1) = 1 = 0 \cdot 1 + 1 \cdot 1$.

Suppose now that $y \geq 2$ and the result holds for smaller y 's. If $x = 0$ then $\gcd(0, y) = y = 0 \cdot 0 + 1 \cdot y$. If $x = y$ then $\gcd(x, y) = y = 0 \cdot x + 1 \cdot y$.

Now assume $0 < x < y$. Then the division algorithm gives $y = qx + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < x$. Then $\gcd(x, y) = \gcd(r, x)$ because an integer divides both x and y iff it divides $r = y - qx$. Using induction, $\gcd(x, y) = \gcd(r, x) = mr + nx$ for some $m, n \in \mathbb{Z}$. Then $\gcd(x, y) = m(y - qx) + nx = (n - mq)x + my$.

Then induction is complete. \square

The Euclidean algorithm for the gcd

Let us compute $\gcd(45, 66)$. Here $66 = 1 \cdot 45 + 21$ where $q = 1$ and $r = 21$, so $\gcd(45, 66) = \gcd(21, 45)$. Next, $45 = 2 \cdot 21 + 3$, so $\gcd(21, 45) = \gcd(3, 21)$. Next, $21 = 7 \cdot 3 + 0$, so $\gcd(3, 21) = \gcd(0, 3) = 3$.

Theorem 2.11

Every positive integer can be written as a product of (finitely many) prime numbers $n = \prod_{i=1}^r p_i = p_1 \cdots p_r$, where p_1, \dots, p_r are prime and $r \geq 0$.

Note. By convention, 1 is the product of 0 prime numbers.

Proof. We use induction on $n \in \mathbb{Z}^+$.

The theorem is true for $n = 1$.

Suppose that $n > 1$ and that the theorem holds for smaller positive integers. If n is prime, we are done. Otherwise, there is an integer m , $1 < m < n$, with $m \mid n$. Then both m and $\frac{n}{m}$ are positive integers $< n$. So they are both products of primes. So $n = m \left(\frac{n}{m}\right)$ is a product of primes. \square

Lemma 2.12

If a prime number p divides the product mn of integers, then $p \mid m$ or $p \mid n$.

Proof. Suppose that $p \mid mn$ and $p \nmid m$. We want to show that $p \mid n$.

Since $p \nmid m$, $\gcd(p, m) = 1$. So by Euclidean algorithm, we write $1 = pu + mv$ for some integers u, v .

We can also write $mn = pw$ for some $w \in \mathbb{Z}$. So, multiplying $1 = pu + mv$ by n , we have $n = npu + mnv = p(nu + wv)$. So $p \mid n$. \square