

# MATH 110AH (Algebra)

September 30, 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  $p \mid n$ .  $\square$

### 3 9.28 Wednesday Week 1

#### Theorem 3.1: Unique factorization of integers, Euclid

Every positive integer  $n$  can be written *uniquely* as a product of prime numbers, that is,  $n = \prod_{i=1}^r p_i$  where  $p_1, \dots, p_r$  are prime. The uniqueness is up to reordering of the  $p_i$ 's.

*Proof.* We use (from last time) if a prime number  $p$  divides  $mn$  (for some  $m, n \in \mathbb{Z}$ ), then  $p \mid m$  or  $p \mid n$ . We showed existence of a prime factorization of  $n \in \mathbb{Z}^+$ .

For uniqueness: suppose  $n = \prod_{i=1}^r p_i = \prod_{i=1}^s q_i$  with  $p_i$ 's and  $q_i$ 's all prime and  $r, s \geq 0$ .

If  $r = 0$ , then  $n = 1$ . Then  $s = 0$ : a product of  $\geq 1$  prime number is  $\geq 2$  since each prime is  $\geq 2$ .

Otherwise,  $r > 0$ . Then  $p_1$  makes sense and it is prime. Then  $p_1$  divides  $n = \prod_{i=1}^s q_i$ . By previous result,  $p_1$  must divide  $q_i$  for some  $1 \leq i \leq s$ . By reordering the  $q_i$ 's, we can assume that  $i = 1$ . Since  $q_i$  is prime and  $p_1 > 1$ , we must have  $p_1 = q_1$ . Then

$$p_1 \left( \prod_{i=2}^r p_i \right) = q_1 \left( \prod_{i=2}^s q_i \right) = p_1 \left( \prod_{i=2}^s q_i \right).$$

Since  $p_1 \neq 0$ , it follows that  $\prod_{i=2}^r p_i = \prod_{i=2}^s q_i$ .

That finishes the proof, by induction on  $r$ . □

#### Equivalence relations

##### Definition 3.2

The **product** of two sets  $A$  and  $B$ ,  $A \times B$ , is the set of ordered pairs  $(a, b)$  where  $a \in A$  and  $b \in B$ . Here  $(a_1, b_1) = (a_2, b_2)$  iff  $a_1 = a_2$  and  $b_1 = b_2$ .

$|A \times B| = |A| |B|$  if  $A, B$  are finite sets.

##### Definition 3.3

A **relation** of a set  $A$  with a set  $B$  is a subset  $R \subseteq A \times B$ . We write  $aRb$  to mean that  $(a, b) \in R$ .

**Example 3.4.** A function  $f: A \rightarrow B$  determines a relation, the **graph**  $R = \{(a, f(a)) : a \in A\}$ .

##### Definition 3.5

An **equivalence relation** on a set  $A$  is a relation  $R \subseteq A \times A$  such that it is

1. reflexive ( $\forall a \in A : aRa$ ),
2. symmetric ( $\forall a, b \in A : aRb \Rightarrow bRa$ ), and
3. transitive ( $\forall a, b, c \in A : aRb \wedge bRc \Rightarrow aRc$ ).

**Example 3.6.** For any set  $A$ , **equality** is an equivalence relation on  $A$ .

**Example 3.7.** Triangles in  $\mathbb{R}^2$  under **congruence** (studied by Euclid): we say that a triangle  $a$  is “congruent”



to triangle  $b$  if there is an **isometry**  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  that maps  $a$  to  $b$ .

**Example 3.8.** The relation on  $\mathbb{Z} \times \{\mathbb{Z} \setminus \{0\}\}$  given by  $(a, b) \sim (c, d)$  if  $ad = bc$ . In fact this relation is equivalent to  $\frac{a}{b} = \frac{c}{d} \in \mathbb{Q}$ . This equivalence relation “ensures” that  $\frac{1}{3} = \frac{2}{6} = \frac{3}{9} = \dots$ . It is a way to constructing  $\mathbb{Q}$  from  $\mathbb{Z}$ .

### Definition 3.9

Let  $\sim$  be an equivalence relation on a set  $A$ . For each element  $a$  let  $\bar{a}$  or  $[a]$ , the **equivalence class of  $a$** , be the set  $\{b \in A : a \sim b\} (\subseteq A)$ .

Let  $\bar{A}$  be the set of subsets of  $A$  of the form  $\bar{a}$  for some  $a \in A$ .  $\bar{A}$ , or  $A/\sim$ , is called the set of **equivalence classes for  $\sim$** .

Define a function  $f: A \rightarrow \bar{A}$  (depending on  $\sim$ ) by  $f(a) = \bar{a} \in \bar{A}$ . This is the **natural** or **canonical surjection** associated to  $\sim$ .

**Example 3.10.** For the relation from Example 3.8 on  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$   $A$ , we can define  $\mathbb{Q} = A/\sim$ .

**Example 3.11.** Define an equivalence relation on  $\mathbb{Z}$  by  $a \sim b$  if  $a - b$  is even. Some equivalence classes are

$$\begin{aligned}\bar{0} &= \{b \in \mathbb{Z} : 0 \sim b\} = \{\dots, -4, -2, 0, 2, 4, \dots\} \\ \bar{1} &= \{\dots, -3, -1, 1, 3, \dots\} \\ \bar{5} &= \bar{1}.\end{aligned}$$

### Definition 3.12

$\mathbb{Z}/2 := \mathbb{Z}/\sim$  for the relation in Example 3.11. Note that this set has exactly 2 elements.

### Proposition 3.13

Let  $\sim$  be an equivalence relation on a set  $A$ . Then  $A = \bigsqcup_{u \in \bar{A}} u$ .

*Proof.* First we show that  $A = \bigcup_{u \in \bar{A}} u$ . For each  $u \in \bar{A}$ ,  $u$  is a subset of  $\bar{A}$ . Then  $\bigcup_{u \in \bar{A}} u \subseteq A$ . Conversely let  $a \in A$ . Then  $a \in \bar{a}$  by reflexivity of  $\sim$ . So  $A = \bigcup_{u \in \bar{A}} u$ .

Next we show that given  $u, v \in \bar{A}$ , if  $u \neq v$  then  $u \cap v = \emptyset$ . Equivalently, we show that if  $u, v \in \bar{A}$  and  $u \cap v \neq \emptyset$  then  $u = v$ . The assumption means that there is an element  $a \in A$  such that  $a \in u$  and  $a \in v$ . By definition of  $\bar{A}$ ,  $u = \bar{b}$  and  $v = \bar{c}$  for some  $b, c \in A$ . Since  $a \in u = \bar{b}$  and  $a \in v = \bar{c}$ ,  $b \sim a$  and  $c \sim a$ . By symmetry and transitivity,  $b \sim a \sim c \Rightarrow b \sim c$ .

To show that  $\bar{b} = \bar{c}$ , pick any element  $e \in \bar{b}$ , that is,  $b \sim e$ ,  $c \sim b \sim e$  so  $c \sim e$ . Then  $e \in \bar{c}$ . The same proof shows that any element in  $\bar{c}$  is also in  $\bar{b}$ . Then  $\bar{b} = u = v = \bar{c}$ .  $\square$

## 4 9.30 Friday Week 1

### Modular arithmetic (Elman section 6)

#### Definition 4.1

Let  $m \in \mathbb{Z}^+$ ,  $a, b \in \mathbb{Z}$ . We say  $a$  is **congruent to  $b$  modulo  $m$** , or  $a \equiv b \pmod{m}$ , if  $m \mid (a - b)$ .

For each  $m \in \mathbb{Z}^+$ , this is an equivalence relation on  $\mathbb{Z}$ . Given that we can define (given  $m \in \mathbb{Z}^+$ ), for  $a \in \mathbb{Z}$ ,

$$\begin{aligned}\bar{a} &= [a]_n \\ &= \{x \in \mathbb{Z} : x \equiv a \pmod{m}\} \\ &= \{a + km : k \in \mathbb{Z}\}\end{aligned}$$

is called the **residue class** of  $a$  modulo  $m$ . This subset is most often called  $a + m\mathbb{Z}$ .

#### Example 4.2.

$$\begin{aligned}\bar{0} &= 0 + m\mathbb{Z} = m\mathbb{Z} \\ &= \{\dots, -2m, -m, 0, m, 2m, \dots\}\end{aligned}$$

#### Proposition 4.3

For  $m \in \mathbb{Z}^+$ , congruence mod  $m$  is an equivalence relation on  $\mathbb{Z}$ .

*Proof.* Reflexive: To show that for any  $a \in \mathbb{Z}$ ,  $a \equiv a \pmod{m}$ , that is  $m \mid (a - a)$ . Here  $0 \cdot m = 0 = a - a$ .

Symmetric: To show that for any integers  $a, b \in \mathbb{Z}$ , if  $a \equiv b \pmod{m}$ , then  $b \equiv a \pmod{m}$ . That is, if  $m \mid (a - b)$ , then  $m \mid (b - a)$ . Indeed,  $\exists x \in \mathbb{Z} : x = a - b$ , then  $m(-x) = b - a$ .

Transitive: To show that for  $a, b, c \in \mathbb{Z}$ , if  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$  then  $a \equiv c \pmod{m}$ . That is, we are given that  $m \mid (a - b)$  and  $m \mid (b - c)$ . Here  $a - c = (a - b) + (b - c)$ , so  $m \mid (a - c)$ . Indeed, if  $a - b = xm$  and  $b - c = ym$ , then  $a - c = (x + y)m$  and  $x + y \in \mathbb{Z}$ .  $\square$

#### Definition 4.4

For  $m \in \mathbb{Z}^+$ , let  $\mathbb{Z}/m$  be the set of equivalence classes  $\mathbb{Z}/(\equiv \pmod{m})$ .

This concept was emphasized by Gauss circa 1800.

#### Proposition 4.5

The set  $\mathbb{Z}/m$  has exactly  $m$  elements.

Explicitly:  $\mathbb{Z}/m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$  and those  $m$  elements of  $\mathbb{Z}/m$  are all different.

Equivalently:  $\mathbb{Z}$  is the *disjoint* union of the subsets  $\bar{0}, \bar{1}, \dots, \overline{m-1}$ .

*Proof.* By the division algorithm, for any  $a \in \mathbb{Z}$ , we can write (uniquely)  $a = qm + r$  with  $q \in \mathbb{Z}$ , and  $r \in \mathbb{Z}$  with  $0 \leq r \leq m - 1$ . So every integer is equivalent to an integer  $\{0, 1, \dots, m - 1\}$ .

Suppose that  $a, b \in \{0, 1, \dots, m - 1\}$  with  $a \equiv b \pmod{m}$ . Then  $m \mid (a - b)$ . If  $a \neq b$ , then  $a - b \neq 0$ , then  $|m| \leq |a - b|$ , resulting in a contradiction.  $\square$

#### Proposition 4.6

Let  $a, b, c, d \in \mathbb{Z}$  and  $m \in \mathbb{Z}^+$ . If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$  and  $ac \equiv bd \pmod{m}$ .

*Proof.* Exercise on homework 2.  $\square$

#### Corollary 4.7

$+$  and  $\cdot$  are well-defined operations on  $\mathbb{Z}/m$ , that is, we have functions  $+: \mathbb{Z}/m \times \mathbb{Z}/m \rightarrow \mathbb{Z}/m$  and  $\cdot: \mathbb{Z}/m \times \mathbb{Z}/m \rightarrow \mathbb{Z}/m$  given by  $\bar{a} + \bar{b} = \overline{a + b}$  and  $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ . (We often write  $0 \in \mathbb{Z}/m$  to mean  $\bar{0}$  and  $1$  to mean  $\bar{1}$ .)

#### Definition 4.8

A **commutative ring**  $R$  is a set with given elements  $0 \in R$  and  $1 \in R$  and functions  $+: R \times R \rightarrow R$  and  $\cdot: R \times R \rightarrow R$  such that

1.  $+$  is associative, commutative, has  $0$  as its identity, and has additive inverses,
2.  $\cdot$  is associative, commutative, and has  $1$  as its identity, and
3. are distributive:  $\forall a, b, c \in R : a(b + c) = ab + ac$ .

**Remark.** A **field** is a commutative ring  $R$  such that  $1 \neq 0 \in R$ , and  $\forall x \in R : x \neq 0 \Rightarrow \exists y \in \mathbb{Z} : xy = 1$ .

**Example 4.9.** Every field (e.g.,  $\mathbb{Q}$ ,  $\mathbb{R}$ , or  $\mathbb{C}$ ) is a commutative ring.

**Example 4.10.**  $\mathbb{Z}$  is a commutative ring but *not* a field.

**Example 4.11.** For any  $m \in \mathbb{Z}^+$ ,  $\mathbb{Z}/m$  is a commutative ring with the operations  $+$  and  $\cdot$  that we defined.

**Example 4.12.** For any commutative ring  $R$ , the set of polynomials  $R[x]$  is also a commutative ring. Here an element of  $R[x]$  is an expression  $a_0 + a_1x + \dots + a_nx^n$  for some  $n \in \mathbb{N} = \{0, 1, 2, \dots\}$  and  $a_0, \dots, a_n \in R$ .  $+$  and  $\cdot$  are defined as expected.

#### Definition 4.13

For a commutative ring  $R$ , the set of **units** in  $R$  is  $R^* := \{a \in R : \exists x \in R : ax = 1\}$ .

**Example 4.14.** The **zero ring** is the ring  $\{0\}$  with 1 element. Then  $1 = 0$  in this ring. This is “isomorphic” to the ring  $\mathbb{Z}/1$ .

**Lemma 4.15**

$$\text{For any } m \in \mathbb{Z}^+, (\mathbb{Z}/m)^* = \left\{ \bar{a} : a \in \mathbb{Z} \wedge \underbrace{\gcd(a, m) = 1}_{\text{"}a \text{ and } m \text{ are relatively prime or coprime"}} \right\}.$$

*Proof.* Let  $\bar{a} \in (\mathbb{Z}/m)^*$ . That means that  $\exists x \in \mathbb{Z} : ax \equiv 1 \pmod{m}$ . That is,  $m \mid (ax-1)$ . So  $\exists y \in \mathbb{Z} : ax-1 = my$ . This implies that if  $g = \gcd(a, m)$ , then  $g \mid 1$ . So  $g = 1$ .

Let  $a \in \mathbb{Z}$  with  $\gcd(a, m) = 1$ . We want to show that  $\bar{a}$  is a unit in  $\mathbb{Z}/m$ . That is, we want to find  $x \in \mathbb{Z}$  such that  $ax \equiv 1 \pmod{m}$ . We know (by Euclid) that we can write  $1 = ua + vm$  for some  $u, v \in \mathbb{Z}$ . So  $ua \equiv 1 \pmod{m}$ .  $\square$

**Corollary 4.16**

For any prime number  $p$ , the ring  $\mathbb{Z}/p$  is a **field**.

*Proof.*  $1 \not\equiv 0 \pmod{p}$  (since  $p \geq 2$ ) and for every  $x \in 1, 2, \dots, p-1$ , we have  $\gcd(x, p) = 1$ , so  $x$  is invertible in  $\mathbb{Z}/p$ .  $\square$

**Remark.** We most oftenly write " $5 \in \mathbb{Z}/7$ " to mean  $\bar{5} \in \mathbb{Z}/7$ . So, for example, " $5 = 12$  in the field  $\mathbb{Z}/7$ ."

**Example 4.17.** What is  $\frac{1}{2} \in \mathbb{Z}/7$ ?

This makes sense because  $2 \neq 0$  in  $\mathbb{Z}/7$ , and  $\mathbb{Z}/7$  is a field. We have  $\frac{1}{2} = 4$  in  $\mathbb{Z}/7$ , since  $4 \cdot 2 = 8 = 1 \in \mathbb{Z}/7$ .

**Theorem 4.18: Chinese remainder theorem (Sun-Tzu, 3rd century CE; Aryabhata, 6th century CE)**

Let  $m_1, \dots, m_r$  be positive integers that are *pairwise coprime* (that is, if  $i \neq j$  then  $\gcd(m_i, m_j) = 1$ ). Let  $c_1, \dots, c_r \in \mathbb{Z}$ . Then there is an integer  $x$  such that  $x \equiv c_1 \pmod{m_1}, \dots$ , and  $x \equiv c_r \pmod{m_r}$ .

Moreover,  $x$  is unique modulo  $\prod m_i$  (i.e., if  $y$  is any integer satisfying the same  $r$  congruences, then  $x \equiv y \pmod{m_1 \cdots m_r}$ ).

**Corollary 4.19**

For positive integers  $m_1, \dots, m_r$  that are pairwise coprime, there is a one-to-one correspondence  $\mathbb{Z}/m \xrightarrow{\sim} (\mathbb{Z}/m_1) \times \cdots \times (\mathbb{Z}/m_r)$ :  $\bar{a} \mapsto (\bar{a}, \dots, \bar{a})$ .

So we can mostly reduce studying  $\mathbb{Z}/p_1^{e_1} \cdots p_r^{e_r}$  (with  $p_1, \dots, p_r$  are *distinct* primes,  $e_1, \dots, e_r \geq 1$ ) to the ring  $\mathbb{Z}/p_1^{e_1}, \dots, \mathbb{Z}/p_r^{e_r}$ .