MATH 110AH (Algebra)

October 10, 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 $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$, and
- the real numbers $\mathbb{R}$ contains $\mathbb{Q}$, $\sqrt{2}, \pi, \dots$, "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 $\boldsymbol{x < y}$ if $y - x = y + (-x)$ is positive (so x is positive iff $x > 0$).

Likewise $\boldsymbol{x \leq y}$ 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

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

□

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 1.6: 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 1.7

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 1.8: 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 $S = \varnothing$. □

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 $\overline{x}$ such that $x\left(\frac{1}{x}\right) = 1$. Then if $xy = xz$, then $\left(\frac{1}{x}\right) xy = \left(\frac{1}{x}\right) xz$, so $1 \cdot y = 1 \cdot z$, that is, $y = z$. □

<u>Proving things about the integer, gcd, prime factorization</u>

Definition 2.4

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

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

Also, if x is a nonzero integer then any integer m with $m | x$ 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, $\forall\, x \in \mathbb{R}\ \exists\, y \in \mathbb{Z} : y < x$.

<u>Notation</u> 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 form well-ordering that a subset of 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 $0 \le r \le x - 1$.

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

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

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 $1|x$ and $1|y$, and (if $y \neq 0$), any integer dividing y is $\le |y|$.

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 $x, y \ge 0$. By switching x and y if needed, assume $0 \le x \le y$ 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 $y \ge 2$ 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 $0 \le r \le x - 1$. 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. $\square$

<u>The Euclidean algorithm for the gcd</u>

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 $n = \prod_{i=1} = p_1 \cdots \cdots p_r$, where $p_1, \ldots, p_r$ are prime and $r \ge 0$.

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 $m|n$. 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 $p|m$ or $p|n$.

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

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 $p|n$. $\square$

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 $p_1, \ldots p_r$ 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 $p|m$ or $p|n$. 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 ≥ 1 prime number is ≥ 2 since each prime is ≥ 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. □

<u>**Equivalence relations**</u>

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 $f\colon A \to B$ 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** $f : \mathbb{R}^2 \to \mathbb{R}^2$ 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 $\frac{1}{3} = \frac{2}{6} = \frac{3}{9} = \cdots$. 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 $\overline{\boldsymbol{a}}$ or $[\boldsymbol{a}]$, the **equivalence class of $\boldsymbol{a}$**, be the set $\{b \in A : a \sim b\}$ $(\subseteq A)$.

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

Define a function $f : A \to \overline{A}$ (depending on $\sim$) by $f(a) = \overline{a} \in \overline{A}$. 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

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

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 $A = \bigsqcup_{u \in \overline{A}} u$.

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

Next we show that given $u, b \in \overline{A}$, if $u \neq v$ then $u \cap v = \varnothing$. Equivalently, we show that if $u, v \in \overline{A}$ and $u \cap v \neq \varnothing$ 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 $\overline{A}$, $u = \overline{b}$ and $v = \overline{c}$ for some $b, c \in A$. Since $a \in u = \overline{b}$ and $a \in v = \overline{c}$, $b \sim a$ and $c \sim a$. By symmetry and transitivity, $b \sim a \sim c \Rightarrow b \sim c$.

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

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 $m|(a-b)$.

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 $a \in \mathbb{Z}$,

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

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

Example 4.2.

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

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 $m|(a-a)$. 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 $m|(a-b)$, then $m|(b-a)$. Indeed, $\exists\, x \in \mathbb{Z}/m : x = a - b$, 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 $m|(a-b)$ and $m|(b-c)$. Here $a - c = (a-b) + (b-c)$, so $m|(a-c)$. Indeed, if $a - b = xm$ and $b - c = ym$, then $a - c = (x+y)m$ and $x + y \in \mathbb{Z}$. □

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

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

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 $0 \le r \le m - 1$. 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 $m | (a - b)$. If $a \neq b$, then $a - b \neq 0$, then $|m| \le |a - b|$, resulting in a contradiction. □

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. □

Corollary 4.7

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

Definition 4.8

A **commutative ring** R is a set with given elements $0 \in R$ and $1 \in R$ and functions $+\colon R \times R \to R$ and $\cdot\colon R \times R \to R$ 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 $a_0 + a_1 x + \cdots + a_n x^n$ 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

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

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

Let $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. We want to show that $\overline{a}$ 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 $ua \equiv 1 \pmod{m}$. ☐

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 $x \in 1, 2, \ldots, p-1$, we have $\gcd(x, p) = 1$, so x is *invertible* in $\mathbb{Z}/p$. ☐

Remark. We most oftenly write “$5 \in \mathbb{Z}/7$” to mean $\overline{5} \in \mathbb{Z}/7$. 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 $m_1, \ldots, m_r$ be positive integers that are *pairwise coprime* (that is, if $i \neq j$ then $\gcd(m_i, m_j) = 1$). Let $c_1, \ldots, c_r \in \mathbb{Z}$. Then there is an integer x such that $x \equiv c_1 \pmod{m_1}, \ldots,$ and $x \equiv c_r \pmod{m_r}$.

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

Corollary 4.19

For positve integers $m_1, \ldots, m_r$ that are pairwise coprime, there is a one-to-one correspondence $\mathbb{Z}/m \overset{\longrightarrow}{\cong} (\mathbb{Z}/m_1) \times \cdots \times (\mathbb{Z}/m_r)$: $\overline{a} \mapsto (\overline{a}, \ldots, \overline{a})$.

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

5 10.3 Monday Week 2

Frequently asked question

Q. *The ring $\mathbb{Z}/m$??*

A. This is $\mathbb{Z}$, but with some integers made equal to others.

Example 5.1. What is $\frac{1}{2} \in \mathbb{Z}/17$ (a field, since 17 is prime)?

9, since $2 \cdot 9 = 18 = 1 \in \mathbb{Z}/17$.

Notation: Sometimes we write $(a, b) := \gcd(a, b)$ for some $a, b \in \mathbb{Z}$.

Lemma 5.2

Let $m, n, a_1, \ldots, a_r$ be integers.

1. If $(a_i, m) = 1$, then $(a_1 \cdots a_r, m) = 1$.
2. If $(a_i, a_j) = 1$ for all $i \neq j$, and if $a_i | n$, then $a_1 \cdots a_r | n$.

Proof.

1. By induction, it suffices to prove this for $r = 2$.

   Use that we can write, $1 = x_1 a_1 + y_1 m = x_2 a_2 + y_2 m$ for some $x_1, y_1, x_2, y_2 \in \mathbb{Z}$. Then

   $$\begin{aligned} 1 &= (x_1 a_1 + y_1 m)(x_2 a_2 + y_2 m) \\ &= x_1 x_2 a_1 a_2 + km && \text{where } k \in \mathbb{Z}. \end{aligned}$$

   Then $(a_1 a_2, m) = 1$.

2. Use induction on r. By induction, $a_1 \cdots a_{r-1} | n$. By part 1, $(a_1 \cdots a_{r-1}, a_r) = 1$. So we can write

   $$1 = a_1 \cdots a_{r-1} x + a_r y$$

   for some $x, y \in \mathbb{Z}$. So (multiplying by n)

   $$n = a_1 \cdots a_{r-1} n x + a_r n y.$$

   Here $a_1 \cdots a_{r-1} a_r | a_1 \cdots a_{r-1} n x$ because $a_r | n$ and $a_1 \cdots a_{r-1} a_r | a_r n y$ since $a_1 \cdots a_{r-1} | n$. So $a_1 \cdots a_r | n$.

□

Theorem 5.3: Chinese remainder theorem

Let $m_1, \ldots, m_r$ be pairwise coprime positive integers. Let $c_1, \ldots, c_r \in \mathbb{Z}$. Then there is an integer x such that

$$\begin{aligned} x &\equiv c_1 \pmod{m_1}, \\ &\vdots \\ x &\equiv c_r \pmod{m_r}. \end{aligned}$$

Moreover, x is unique modulo $m_1 \cdots m_r$.

Example 5.4. There is ans integer x which is $\equiv 1 \pmod 3$ and $\equiv 3 \pmod 4$.

Example 5.5. There is no integer x such that $x \equiv 5 \pmod 8$ (odd) and $x \equiv 4 \pmod{12}$ (even).

Proof. We first show existence.

Let $m = m_1 \cdots m_r$. For $i = 1, \ldots, r$, $n_i = \frac{m}{m_i} = \prod_{j \neq i} m_j$.

By the lemma, $(m_i, n_i) = 1$ for each i. So we can write (for each i) $1 = d_i m_i + e_i n_i$ for some $d_i, e_i \in \mathbb{Z}$. Let $b_i = e_i n_i$ for $i = 1, \ldots, r$. Then $1 = d_i m_i + b_i$ and for each $j \neq i$, $m_j | b$.

Here for each $1 \leq i \leq r$, b_i is $\equiv 1 \pmod{m_i}$ and is $\equiv 0 \pmod{m_j}$ for each $j \neq i$.

Define $x := c_1 b_1 + \cdots c_r b_r$.

We then show uniqueness. Suppose $y \in \mathbb{Z}$ also satisfies these r congruences. Then $x \equiv y \pmod{m_i}$ for each i, so $m_i | x - y$ for each $i = 1, \ldots, r$. Since $m_1, \ldots, m_r$ are pairwise coprime, Lemma 5.2 implies $m_1 \cdots m_r | x - y$. That is, $x \equiv y \pmod{m_1 \cdots m_r}$. □

Groups

Definition 5.6

A **group** G is a set with an element $1 \in G$ (or 1_G) and a function $\cdot : G \times G \to G$ such that

1. it is associative: $\forall\, x, y, z \in G : (xy)z = x(yz) \in G$,
2. 1 is the identity: $\forall\, x \in G : 1 \cdot x = x \wedge x \cdot 1 = x$, and
3. there are inverses: $\forall\, x \in G\ \exists\, y \in G : xy = 1 \wedge yx = 1$.

If the group operation is **commutative** (*i.e.* $\forall\, x, y \in G : xy = yx$), we call G an **abelian group** (Niels Henrik Abel, 1810).

Example 5.7 (The permutation group). Let S be a set. Define $\Sigma(S) := \{f : S \to S : f \text{ is bijective}\}$. This is a group under **composition** of functions. That is, if $f, g \in \Sigma(S)$, define $fg \in \Sigma(S)$ by $(fg)(s) = f(g(s)) \in S$ for any $s \in S$.

The element $1 \in \Sigma(S)$ is the **identity** function, $1_{\Sigma(S)}(s) = s$ for every $s \in S$.

Inverses are given by: for $f \in \Sigma(s)$, $f^{-1} \in \Sigma(S)$ is the function $f^{-1}(s) =$ the unique element $t \in S$ such that $f(t) = s$.

Proof of associativity for $\Sigma(S)$

Let $f, g, h \in \Sigma(S)$, what is $(fg)h$ and $f(gh)$?

For any $s \in S$,

$$\begin{aligned}((fg)h)(s) &= (fg)(h(s)) \\ &= f(g(h(s))) \in S\end{aligned}$$

and

$$\begin{aligned}(f(gh))(s) &= f((gh)(s)) \\ &= f(g(h(s))).\end{aligned}$$

So they are equal.

Note. If $|S| \geq 3$, then the group $\Sigma(S)$ is *not* abelian.

Definition 5.8

For $n \in \mathbb{Z}^+$, the **symmetric group** S_n means $\Sigma(\{1, 2, \ldots, n\})$.

Proof that S_3 is not abelian

Let $f, g \in S_3$ be $f(1) = 1$, $f(2) = 3$, $f(3) = 2$, and $g(1) = 2$, $g(2) = 1$, $g(3) = 3$. Then $(fg)(1) = 3$, $(fg)(2) = 1$, $(fg)(3) = 2$, and $(gf)(1) = 2$, $(gf)(2) = 3$, $(gf)(3) = 1$.

Lemma 5.9

The inverse of an element x in a group G is unique so we can call it x^{-1}. More strongly if $xy = 1 \in G$, then $y = x^{-1}$ (and so $yx = 1$). Likewise, if $yx = 1$, then $y = x^{-1}$ (and so $xy = 1$).

Proof. Suppose that y and z in G are both inverses of x in G. Then $y = 1 \cdot y = (zx)y = zxy = z(xy) = z \cdot 1 = z$. So $y = z$, *i.e.*, the inverse is unique.

Next, suppose $y \in G$ with $xy = 1$. Multiply both sides *on the left*, we have $y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = x^{-1} \cdot 1 = x^{-1}$. If $yx = 1$, then $(yx)x^{-1} = 1 \cdot x^{-1}$, so $y = x^{-1}$. $\square$

6 10.5 Wednesday Week 2

Lemma 6.1

The identity element in a group G is unique. More strongly, if there are elements $e, x \in G$ such that $ex = x$, then $e = 1$. (Likewise, if $xe = x$, then $e = 1$.)

Proof. Given $e, x \in G$ with $ex = x$, multiply on the *right* by x^{-1} and we get $e = exx^{-1} = xx^{-1} = 1$.

For the other direction, if $xe = x$, then, multiplying by x^{-1} on the *left*, we have $e = x^{-1}xe = x^{-1}x = 1$. ☐

Lemma 6.2

For any elements x, y in a group G, $(xy)^{-1} = y^{-1}x^{-1}$.

Proof. As we showed, it suffices to show that $(xy)y^{-1}x^{-1} = 1$. By associativity, $(xy)y^{-1}x^{-1} = x(yy^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = xx^{-1} = 1$. So $(xy)^{-1} = y^{-1}x^{-1}$. ☐

Definition 6.3

For an element a in a group G and $n \in \mathbb{Z}^+$ define $a^n := \underbrace{a \cdots a}_{n \text{ times}} \in G$. (This makes sense by associativity.)

Also, define $a^0 = 1$ (for any $a \in G$). Also, for $m \in \mathbb{Z}^+$, define $a^{-m} := (a^{-1})^m$.

One can check that $a^{m+n} = a^m a^n$ for all $a \in G$, $m, n \in \mathbb{Z}$.

Lemma 6.4

The **cancellation laws** hold in a group G: given $a, b, c \in G$ such that $ab = ac$, then $b = c$. Also if $ba = ca$, then $b = c$.

Proof. Given $a, b, c \in G$ with $ab = ac$, multiply on the *left* by a^{-1}, and we get $b = a^{-1}(ab) = a^{-1}(ac) = c$. Liksewise for the other direction. ☐

Remark. For an **abelian group**, we may write the opderation as + (not $\cdot$ and he idendity element is 0 no 1) and the inverse operation is $x \in G \mapsto -x$

Example 6.5. Any commutative ring is a group **under addition**. Enamples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/m$ for any $m \in \mathbb{Z}^+$

Example 6.6. For a commutative ring R, the subset R^* of **units** in R is abelian under multiplication. (If $a, b \in R^*$) then $ab \in R^*$ since $(ab)b^{-1}a^{-1} = 1$, by the axioms of a ring.

Definition 6.7

Let G, H be groups. A **homomorphism** $\boldsymbol{f\colon G \to H}$ **(of groups)** is a function from G to H such that $f(xy) = f(x) + f(y)$.

Definition 6.8

An **isomorphism** of groups is a **bijective** homomorphism $f\colon G \to H$. That is, it is injective, or for $x, y \in G$, if $f(x) = f(y) \in H$, then $x = y$.

We say G and H are **isomorphic** if there is an isomorphism $f\colon G \to H$ (write $G \cong H$).

Example 6.9. We will classify all groups of order 2 up to isomorphism. Such a group G has elements $1, x$. Then $1 \cdot 1 = 1$, $1 \cdot x = x$, and $x \cdot 1 = x$. We claim that $x \cdot x = 1$. Otherwise we have $x \cdot x = x$. Multiplying on the right by x^{-1}, we get $x = 1$, a contradiction. So *every* group of order 2 is isomorphic to $(\mathbb{Z}/2, +)$.

Example 6.10. We then classify all groups of order 3. Such a group G has elements $1, x, y$. Note that xy and yx cannot be x or y since that would imply one of x, y is equal to 1. Then $xy = yx = 1$. Then $x \cdot x = y$ and $y \cdot y = x$. Furthermore note that $x^3 = x^2 \cdot x = yx = 1$. So *every* group of order 3 is isomorphic to $\mathbb{Z}/3$. We see that $y = x^2$, so $G = \left\{1, x, x^2\right\}$.

Definition 6.11

A **subgroup H of a group G** is a subset of G such that

1. $1_G \in H$,
2. $\forall\, x, y \in H : xy \in H$, and
3. $\forall\, x \in H : x^{-1} \in H$.

Lemma 6.12

A subgroup of a group G is a group (with the group operation of G, restricted to H).

Proof. By (2), the product gives a function $\cdot\colon H \times H \to H$. Clearly $(xy)z = x(yz)$ for all $x, y, z \in H$ by the same fact for G. Also, $1_G \in H$, so $1_G x = x 1_G = x$ for all $x \in H$. Inverses are given by (3). $\square$

Example 6.13. For any field $\mathbb{F}$ and any $n \in \mathbb{Z}^+$, the **general linear group $GL(n, \mathbb{F})$** is the group of *invertible $n \times n$ matrices over* $\mathbb{F}$ is a group (under multiplication) $\{A \in M(n, \mathbb{F}) : \det A \neq 0 \in F\}$.

7 10.7 Friday Week 2

Definition 7.1

The **general linear group $GL(n,\mathbb{F})$** for $n \in \mathbb{Z}^+$, F a field, is the set of *invertible* $n \times n$ matrices over F, with group operation multiplication of matrices.

Note that the identity is given by $1 = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}$.

Why is matrix multiplication associative?

A matrix $A \in M(n,\mathbb{F})$ defines an F-linear map $F^n \to F^n := \underbrace{F \times \cdots \times F}_{n \text{ copies}}$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}.$$

Matrix multiplication corresponds to the *composing* of these linear maps. That explains why $A(BC) = (AB)C$.

Another way to say this is that $GL(n,\mathbb{F})$ is a subgroup of $\sum(F^n)$ the permutation group

Example 7.2. Rotation in $\mathbb{R}^2$ by θ:

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Example 7.3. Reflection across the x-axis:

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Example 7.4. The **special linear group $SL(n,\mathbb{F}) = \{A \in GL(n,\mathbb{F}) : \det A = 1\}$** is a subgroup of $GL(n,\mathbb{F})$ since $\det(AB) = (\det A)(\det B)$.

Geometrically, $SL(n,\mathbb{R})$ is the subgroup of $GL(n,\mathbb{R})$ of *volume-preserving* linear maps (and orientation-preserving).

Example 7.5. The **orthogonal group $O(n) := O(n,\mathbb{R}) = \{A \in M(n,\mathbb{R}) : A(A^{\mathsf{T}}) = I\}$** is a subgroup of $GL(n,\mathbb{R})$.

This is the set of *length-preserving* linear maps. Examples include rotations and reflections.

Example 7.6. The **special orthogonal group $SO(n) := O(n) \cap SL(n,\mathbb{R})$** is a subgroup of $GL(n,\mathbb{R})$.

Reflections $\notin SO(n)$.

Example 7.7. $D(n,\mathbb{F})$:= subgroup of *diagonal matrices* in $GL(n,\mathbb{F})$ $= \left\{ \begin{bmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{bmatrix} : a_1, \ldots, a_n \in F^* \right\}$.

Note that $\det = a_1 \cdots a_n$.

Remark. This is an **abelian** group.

Example 7.8. $UT(n,\mathbb{F})$:= group of invertible upper-triangular matrices in $GL(n,\mathbb{F})$

$$= \left\{ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{bmatrix} : a_{ij} \in F, a_{ii} \neq 0 \right\}.$$

Geometrically, $UT(n, \mathbb{F})$ is the subgroup of $GL(n, \mathbb{F})$ that preserves the standard *flag* in F^n: $0 \subseteq F \subseteq F^2 \subseteq \cdots \subseteq F^n$.

Example 7.9. $SUT(n, \mathbb{F})$:= group of strictly upper-triangular matrices in $GL(n, \mathbb{F}) = \left\{ \begin{bmatrix} 1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} : * \in F \right\}$.

Definition 7.10

For a subset S of a group G, the **subgroup $\langle S \rangle$ generated by S** is the intersection of all subgroups of G that contain S.

It is easy to show that *any* intersection of subgroups of G, even infinitely many, is a subgroup.

Lemma 7.11

For a group G and a subset S, the subgroup $\langle S \rangle \subseteq G$ is the set of elements of G that can be written as $a_1^{\pm 1}, \dots, a_n^{\pm 1}$ for some $n \geq 0$ and $a_1, \dots, a_n \in S$ (and some signs).

Proof. *Exercise on homework 3.* □

Remark. If $n = 0$, we interpret $a_1^{\pm 1}, \dots, a_n^{\pm 1}$ as being $1 \in G$.

Definition 7.12

A group G is **finitely generated** if there is a finite subset $S \subseteq G$ with $G = \langle S \rangle$.

Definition 7.13

A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$.

Example 7.14. The group $\mathbb{Z}$ (= $(\mathbb{Z}, +)$) is infinite but finitely generated (in fact cyclic) since $G = \langle 1 \rangle$.

Also the additive group $\mathbb{Z}/m$ is cyclic, for any $m \in \mathbb{Z}^+$, since $\mathbb{Z}/m = \langle 1 \rangle$.

Theorem 7.15: Classification of cyclic groups

Let G be a cyclic group. That is, there is an $a \in G$ such that $G = \langle a \rangle$. Then G is isomorphic to either $\mathbb{Z}$ or to $\mathbb{Z}/m$ for some $m \in \mathbb{Z}^+$. So if G is infinite cyclic, then $G \cong \mathbb{Z}$, and if G has m elements, then $G \cong \mathbb{Z}/m$.

Proof. Define a function $f : \mathbb{Z} \to G$ by $f(n) = a^n \in G$. Because $a^{m+n} = a^m a^n$, f is a homomorphism (thatis, $f(m+n) = f(m)f(n) \in G$ for all $m, n \in \mathbb{Z}$). Since $G = \langle a \rangle$, $f : \mathbb{Z} \to G$ is *surjective*.

Consider the **kernel** of f, $H := \ker(f) = \{m \in \mathbb{Z} : f(m) = 1\}$. This is a *subgroup* of $\mathbb{Z}$.

Suppose that $H = \{0\}$. Then we claim that f is *injective* as well as surjective (so f is an isomorphism). Suppose $m, n \in \mathbb{Z}$ with $f(m) = f(n)$. Then $f(m-n) = f(m)f(n)^{-1} = 1$. So $m - n \in H$. So $m - n = 0$, *i.e.*, $m = n$. So f is injective.

Otherwise $H \neq \{0\}$. Then H must contain some *positive* integer. So we can define n to be the smallest positive integer in H (by well-ordering). Then we can define a homomorphism $\overline{f}\colon \mathbb{Z}/n \to G$ by $\overline{f}\left(\overline{i}\right) = f(i) \in G$ for $i \in \mathbb{Z}$, where $\overline{i}$ is the equivalence class of i. This makes sense because if $i \equiv j \pmod{n}$, then $f(i) = f(j) \in G$. Indeed, since $f(j) = f(i)f(j-i) = f(i)$. This function, $\overline{f}\colon \mathbb{Z}/n \to G$, is also a homomorphism since $\overline{f}\left(\overline{i} + \overline{j}\right) = f(i+j) = f(i)f(j) = \overline{f}\left(\overline{i}\right)\overline{f}\left(\overline{j}\right)$. It is surjective since f was surjective.

We claim that $\overline{f}$ is also injective (hence an isomorphism). Suppose there are $\overline{i}, \overline{j} \in \mathbb{Z}/n$ with $\overline{f}\left(\overline{i}\right) = \overline{f}\left(\overline{j}\right) \in G$. Since $\overline{f}$ is a homomorphism, this means $\overline{f}\left(\overline{i} - \overline{j}\right) = 1 \in G$. So $f(i-j) = 1 \in G$. So $i - j \in H = \{m \in \mathbb{Z} : m \equiv 0 \pmod{n}\}$. So $\overline{i} = \overline{j}$. So f is injective.

To show that $H = \{m \in \mathbb{Z} : m \equiv 0 \pmod{n}\}$, let $m \in H$. By division, we can write $m = qn + r$ for some $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Note that $qn \in H$ since $n \in H$. Then $r \in H$. But n is the *smallest* positive integer in H. So $r = 0$. So $m \equiv 0 \pmod{n}$. $\square$

8 10.10 Monday Week 3

Lemma 8.1

Let $f\colon G \to H$ be a group homomorphism. Then $f(1) = 1$ and $f\left(x^{-1}\right) = f(x)^{-1}$ for all $x \in G$.

Proof. We are given that $f(xy) = f(x)f(y)$ for all $x, y \in G$. So $f(1) = f(1 \cdot 1) = f(1)f(1) \in H$. Multiplying on the left by $f(1)^{-1}$, we get $1 = f(1) \in H$ as desired. Also, for any $x \in G$, $1 = f(1) = f\left(xx^{-1}\right) = f(x)f\left(x^{-1}\right)$. So $f\left(x^{-1}\right) = f(x)^{-1}$. □

Lemma 8.2

Let $f\colon G \to H$ be a group homomorphism. Then the *kernel* of f ($\ker(f) = \{x \in G : f(x) = 1\}$) is a subgroup of G and the *image* of $\operatorname{im}(f) = f(G) = \{f(x) : x \in G\} \subseteq H$ is a subgroup of H.

Proof. If $x, y \in \ker(f)$, ...

... by Lemma 8.2.

One can check oneself for the image. □

Lemma 8.3

A group homomorphism $f\colon G \to H$ is injective iff $\ker(f) = \{1\} \subseteq G$.

Proof. The $\Rightarrow$ direction is easy. If $f\colon G \to H$ is a group homomorphism and injective then $f(1) = 1$. Injectivity implies if $x \in G$ has $f(x) = f(1) = 1$, then $x = 1$. So $\ker(f) = \{1\}$.

Now we show the $\Leftarrow$ direction. Suppose f is a group homomorphism with $\ker(f) \neq \{1\}$. Let $x, y \in G$ such that $f(x) = f(y) \in H$. Since f is a group homomorphism, we have $f\left(xy^{-1}\right) = f(x)f\left(y^{-1}\right) = f(x)f(y)^{-1} = 1 \in H$. So $xy^{-1} \in \ker(f)$. So $xy^{-1} = 1$. Multiplying on the right by y, we get $x = y$. So f is injective. □

Definition 8.4

The **product group** of groups G and H is the product set $G \times H = \{(g, h) : g \in G, h \in H\}$ with multiplication given by $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \in G \times H$.

It is easy to see that this is a group. The identity is $(1_G, 1_H)$. Inverses are $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Note. $G \times H$ contains subgroups $G \times \{1\} \cong G$ and $\{1\} \times H \cong H$. Note that $(g, 1)(1, h) = (g, h) = (1, h)(g, 1)$. Therefore many but not all elements of $G \times H$ commute with each other.

Example 8.5. $\mathbb{Z}/2 \times \mathbb{Z}/2$ is the "Klein four-group" (Felix Klein, 19th century) has order 4. It is the smallest group that is not cyclic.

The elements of G are $(0, 0), (0, 1), (1, 0), (1, 1)$. We use multiplication notation for this group: $1 = (0, 0)$, $x =$

$(0,1), y = (1,0), (1,1) = xy$. The multiplication table is 2nd factor:

	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	xy	1	x
xy	xy	y	x	1

We can see that this group is *not* cyclic: we have $\langle x\rangle = \{1, x\}$, $\langle y\rangle = \{1, y\}$, $\langle xy\rangle = \{1, xy\}$, and $\langle 1\rangle = \{1\}$

Theorem 8.6: Cyclic subgroup theorem, from homework 3

Let G be a cyclic group, so $G = \langle a\rangle$ for some $a \in G$. Then every subgroup of G is also cyclic. In more detail:

1. Every subgroup of $\mathbb{Z}$ is either $\{0\}$ or $\langle n\rangle$ for some positive integer n.
2. For $m \in \mathbb{Z}^+$, every subgroup of $\mathbb{Z}/m$ is equal to $\langle k\rangle$ where k is a positive integer dividing m.

Example 8.7. What is the subgroup of $\mathbb{Z}/7$ generated by 5?

Note that $\mathbb{Z}/7 = \{0, 1, 2, \ldots, 6\}$. The subgroup $\langle 5\rangle$ contains $0, 5, 10 = 3, 8 = 1, 6, 11 = 4, 9 = 2 \in \mathbb{Z}/7$. Then $\langle 5\rangle = \langle 1\rangle = \mathbb{Z}/7$.

In fact, the Theorem 8.6 implies every subgroup of $\mathbb{Z}/7$ is either $\langle 1\rangle = \mathbb{Z}/7$ or $\langle 7\rangle = \{0\}$.

Example 8.8. Theorem 8.6 implies for any $a, b \in \mathbb{Z}$, not both zero, the subgroup $\langle a, b\rangle = \{ma + nb : m, n \in \mathbb{Z}\} \subseteq \mathbb{Z}$ must be generated by 1 element. Indeed, Euclid proved this: $\langle a, b\rangle = \langle \gcd(a, b)\rangle$. For instance, $\langle 5, 7\rangle = \langle \gcd(5, 7)\rangle = \langle 1\rangle = \mathbb{Z}$.

Cycle notation for the symmetric groups

Recall that the symmetric group $S_n = \sum(\{1, \ldots, n\})$, the group of permutations of $\{1, \ldots, n\}$ for $n \in \mathbb{Z}^+$.

Note. The *order* of S_n is $n! = 1 \cdot 2 \cdots n$.

Proof. Note that $f(1)$ could be any number in $\{1, \ldots, n\}$ (n possibilities). Then $f(2)$ can be any number $\neq f(1)$, so $n - 1$ possibilities, and so on, and $f(n)$ has 1 possibility. Then $|S_n| = n(n-1)\cdots 2 \cdot 1 = n!$. □

Definition 8.9

Let $r \geq 2$ and let $a_1, \ldots, a_r$ be *distinct elements* of $\{1, \ldots, n\}$. The **cycle $(a_1\ a_2\ \ldots\ a_r) \in S_n$** is the permutation

$$f(a_1) = a_2, f(a_2 = a_3), \ldots, f(a_{r-1}) = a_r, f(a_r) = a_1$$

and $f(u) = u$ for all $u \notin \{1, \ldots, n\} = \{a_1, \ldots, a_r\}$.

This is called a **cycle of length r**.

Remark. A cycle of length 2 is called a **transposition**.

Remark. Starting the cycle in the middle of the loop gives another name for the same element of S_n. For example, $(4\ 5\ 1\ 7) = (5\ 1\ 7\ 4) = (1\ 7\ 4\ 5) = (7\ 4\ 5\ 1) \in S_7$.

Convention. Write the *smallest* number in a cycle first, *e.g.*, $(1\ 7\ 4\ 5)$.

For any $\sigma \in S_n$, apply σ repeatedly to a number i. Define $a_0 = i, a_1 = \sigma(i), a_2 = \sigma^2(i), \ldots, a_m = \sigma^m(i)$. Let m be the *smallest* positive integer such that $a_m = a_j$ for some $j < m$.

We claim that we must have $j = 0$.

Proof. If $0 < j < m$ then $\sigma^j(i) = \sigma^m(i)$, so $\sigma(\sigma^{j-1}(i)) = \sigma(\sigma^{m-1}(i))$. But σ is bijective, so $\sigma^{j-1}(i) = \sigma^{m-1}(i)$, contradicting the definition of m. So we must have $j = 0$.

So "what σ does to the element i" is the cycle $(a_0\ a_1\ \cdots\ a_{m-1})$ wich $a_m = a_0$. □

Conclusion. Every element of S_n is a product of disjoint cycles.

Example 8.10. The elements of S_3 are $1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$. That is all since $|S_3| = 6!$.

Example 8.11. The elements of S_4 are $1, (a\ b), (a\ b\ c), (a\ b\ c\ d), (a\ b)(c\ d)$ such as $(1\ 2)(3\ 4)$ or $(1\ 4)(2\ 3)$ or $(1\ 3)(2\ 4)$.