

MATH 110AH - FALL 2021

Pablo S. Ocal

based on "Lectures on Abstract Algebra"

by Richard S. Elman.

Section 2: Well-ordering and induction.

The well-ordering principle: Let $\emptyset \neq S \subseteq \mathbb{Z}^+$. Then S contains a least element: there exists $a \in S$ such that $a \leq x$ for all $x \in S$.

Proposition: Let $\emptyset \neq T \subseteq \mathbb{Z}$. Suppose that there is an $N \in \mathbb{Z}$ such

that $N \leq x$ for all $x \in T$ (i.e. T is bounded from below). Then

T contains a least element.

Similarly, if T is bounded from above, it contains a largest element.

Proposition: There is no integer N satisfying $0 < N < 1$.

Proof: Let $S = \{n \in \mathbb{Z} \mid 0 < n < 1\}$. If $\emptyset \neq S$ then there exists a least

element $N \in S$. Now $0 < N < 1$ implies $0 < N^2 < N < 1$ and

since $N \in \mathbb{Z}$ then $N^2 \in \mathbb{Z}$, so $N^2 \in S$ contradicting minimality. \square .

Proposition: Let $S \subseteq \mathbb{Z}^+$ and $1 \in S$. Suppose that if $n \in S$, then

$n+1 \in S$. Then $S = \mathbb{Z}^+$.

Proof: Let $T = \{n \in \mathbb{Z}^+ \mid n \notin S\}$. If $T = \emptyset$ then $S = \mathbb{Z}^+$. If

$T \neq \emptyset$ then there exists a least positive element $n \in T$. Then

$n \notin S$ and $n-1 \notin T$. Since $1 \notin T$ then $n > 1$ and $n-1 \in \mathbb{Z}^+$.

Then $n-1 \in S$, but by hypothesis $n \notin S$, contradiction.

□.

Theorem: (Induction) For each $n \in \mathbb{Z}^+$, let $P(n)$ be a true or false

statement. Suppose we know that $P(1)$ is true, and that if $P(u)$ is

true then $P(u+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Theorem: (Induction) For each $n \in \mathbb{Z}^+$, let $P(n)$ be a true or false

statement. Suppose that if $P(m)$ is true for all $m \leq n$ positive

integers, then $P(n)$ is true. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proposition: The product of any $n \geq 1$ consecutive positive integers is

divisible by $n!$, i.e. for all $m, n \in \mathbb{Z}^+$ we have: $\frac{m \cdot (m+1) \cdots (m+n-1)}{n \cdot (n-1) \cdots 2 \cdot 1} \in \mathbb{Z}^+$

Corollary: For every $n \in \mathbb{Z}^+$, there exist n consecutive composite positive

integers.

Corollary: Let $p > 1$ be a prime. Then p divides $\binom{p}{n}$ for all $1 \leq n \leq p-1$.

Section 3: The greatest integer function.

Another way of showing that the binomial coefficients are integers.

Definition: The greatest integer function: $[] : \mathbb{R} \longrightarrow \mathbb{Z}$

gives $[x]$ the greatest integer $[x] \leq x$ for $x \in \mathbb{R}$.

Proposition: For $x \in \mathbb{R}$ and $m, n \in \mathbb{Z}^+$, the following hold:

$$1) [x] \leq x < [x] + 1.$$

$$2) [x+m] = [x] + m.$$

$$3) \left[\frac{x}{m} \right] = \left[\frac{[x]}{m} \right].$$

$$4) [x] + [y] \leq [x+y] \leq [x] + [y] + 1.$$

5) $\left[\frac{n}{m} \right]$ is the number of integers among $1, \dots, n$ that are divisible by m .

Proof: (1), (2), (3), (4) are straightforward.

5) Let $m, 2m, \dots, jm$ all the positive integers below n and divisible

by m . Now $jm \leq n < (j+1)m$ so $j \leq \frac{n}{m} < j+1$ so $\left[\frac{n}{m} \right] = j$. \square .

Theorem: Let $n \in \mathbb{Z}^+$ and $p > 1$ a prime. Suppose that $p^e \mid n!$ but

$$e+1, 1 - \sum_{k=1}^{\infty} \lceil \frac{n}{p^k} \rceil$$

$$p \nmid u! \text{. Then: } e = \sum_{i=1}^r [p_i].$$

Corollary: Suppose that $a_1, \dots, a_r \in \mathbb{Z}^+$ with $a_1 + \dots + a_r = u$. Then

the multinomial coefficient $\frac{u!}{a_1! \cdots a_r!} \in \mathbb{Z}^+$.

Section 4: Division and the greatest common divisor.

Proposition: Let $r, u, m \in \mathbb{Z}$, the following hold:

1) If $r|m$ and $r|u$ then $r|au+bu$ for all $a, b \in \mathbb{Z}$.

2) If $r|u$ then $r|un$.

3) If $r|u$ and $u \neq 0$ then $|u| \geq |r| \geq r$.

4) If $m|u$ and $u|m$ then $u = \pm m$.

5) If $mn=0$ then $m=0$ or $n=0$.

6) If $m\tau = u\tau$ then $m=u$ or $\tau=0$.

Theorem: (Division Algorithm) Let $u \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then there exist

unique $q, r \in \mathbb{Z}$ satisfying $u = qm + r$ and $0 \leq r < m$.

Proof: We need to show existence and uniqueness.

Uniqueness: Let (q, r) and (q', r') satisfy the conclusion.

We have $qm+r=u=q'm+r'$ and $0 \leq r < m$, $0 \leq r' < m$.

WLOG suppose $r \leq r'$, then $0 \leq r' - r = (q - q')m$. If $q = q'$

then $r' - r = 0$ and we are done. If $q \neq q'$ then $r' - r > 0$

and $m \mid r' - r$. Thus $m \leq r' - r < m$, a contradiction.

Existence: If $n > 0$, let $S = \{s \in \mathbb{Z}^+ \mid sn > n\} \subseteq \mathbb{Z}^+$. Since

$n > 0$ we have $m \geq 1$ so $(n+1)m = mn + m \geq n + m > n$ so

$n+1 \in S \neq \emptyset$. There exists a least integer $q+1 \in S$, so $qn \leq n$.

Now $qn \leq n < (q+1)n$, choose $r = n - qn \geq 0$, we then have:

$$0 \leq r = n - qn < (q+1)n - qn = m.$$

If $n < 0$, there exist $q', r' \in \mathbb{Z}$ with $|n| = q'm + r'$ and

$0 \leq r' < m$. If $r' = 0$ then $q = -q'$ and $r = 0$ work. If $r' \neq 0$

then $q = -q'^{-1}$ and $r = m - r'$ work. \square .

Definition: Let $n, m \in \mathbb{Z}$ at least one non-zero. A $d \in \mathbb{Z}$ is called

a greatest common divisor if it satisfies the following:

i) $d > 0$,

ii) $d|m$ and $d|n$,

iii) If $e \in \mathbb{Z}$ satisfies $e|m$ and $e|n$, then $e|d$.

If $\gcd(u, v) = 1$ we say that they are relatively prime.

Theorem: Let $m, n \in \mathbb{Z}$ with $n \neq 0$. Then $\gcd(m, n)$ exists and is unique.

Theorem: (Euclidean Algorithm) Let $a, b \in \mathbb{Z}^+$ with $b \neq a$. Then

there exists $k \in \mathbb{Z}^+$ and equations:

$$a = bq_1 + r_1, \quad b = r_1 q_2 + r_2, \quad \dots, \quad r_{k-2} = r_{k-1} q_k + r_k, \quad r_{k-1} = r_k q_{k+1}$$

with: $0 < r_1 < b, \quad 0 < r_2 < r_1, \quad \dots, \quad 0 < r_k < r_{k-1}$

for $q_1, \dots, q_{k+1}, r_1, \dots, r_k \in \mathbb{Z}$.

Theorem: (General Euclid's Lemma) Let $a, b \in \mathbb{Z}$ relatively prime, $a \neq 0$.

If $a \mid bc$ for some $c \in \mathbb{Z}$, then $a \mid c$.

Corollary: If $p > 1$ prime satisfies $p \mid a_1 \dots a_r$ with $a_1, \dots, a_r \in \mathbb{Z}$, then

$p \mid a_i$ for some $1 \leq i \leq r$.

Corollary: Let $p > 1$ be a prime. Then p divides $\binom{p}{n}$ for all $1 \leq n \leq p-1$.

Proof: We know that $n! \mid p(p-1)\dots(p-n+1)$ since these are n

consecutive positive integers. If $1 < s < p$, then $\gcd(s, p) = 1$, so

$\gcd(n!, p) = 1$ so by Euclid's lemma $n! \mid (p-1)\dots(p-n+1)$.

Hence $p \cdot n! \mid p(p-1) \cdots (p-n+1)$, so $p \mid \frac{p(p-1) \cdots (p-n+1)}{n!}$. \square .

Proposition: Let $p \in \mathbb{Z}$, $|p| > 1$. Then p is prime if and only if whenever

$p \mid ab$ with $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Theorem: (Fundamental Theorem of Arithmetic) Let $n \in \mathbb{Z}$, $n > 1$.

Then there exist unique primes $1 < p_1 < \cdots < p_r$ and $e_1, \dots, e_r \in \mathbb{Z}$ such

that $n = p_1^{e_1} \cdots p_r^{e_r}$.

Proof: We need to show existence and uniqueness.

Existence: Let $S = \{n \in \mathbb{Z}^+ \mid n > 1 \text{ and it is not a product of primes}\}$.

If $S = \emptyset$, we are done. Suppose $S \neq \emptyset$, then there exists a minimal

$n \in S$. Since S does not contain any primes, n is not a prime.

Hence there exist $u_1, u_2 \in \mathbb{Z}^+$ such that $n = u_1 \cdot u_2$, $1 < u_1$, and

$1 < u_2$. By minimality of n we have $u_1, u_2 \notin S$, so u_1 and u_2 are

product of primes, so $n = u_1 \cdot u_2$ is a product of primes, contradiction.

Uniqueness: Suppose $p_1^{e_1} \cdots p_r^{e_r} = n = q_1^{f_1} \cdots q_s^{f_s}$ with $1 < p_1 < \cdots < p_r$ and

$1 < q_1 < \cdots < q_s$ primes and $e_1, \dots, e_r, f_1, \dots, f_s \in \mathbb{Z}^+$. WLOG $p_1 \leq q_1$,

since $q_1 \mid n$ by Euclid's Lemma $q_1 \mid q_i$, but $q_1 \leq q_i$ and both are

prime so $i=1$ and $q_1 = q_1$. Dividing by $q_1 = q_1$, we obtain

$q_1^{e_1-1} \cdots q_r^{e_r} = n = q_1^{f_1-1} \cdots q_s^{f_s}$. Using induction, we are done. \square .

Section 5: Equivalence relations.

Definition: A relation on two sets A and B is a subset $R \subseteq A \times B$.

We write aRb if $(a, b) \in R$.

Example: A function $f: A \rightarrow B$ gives a relation $R = \{(a, f(a)) \mid a \in A\}$.

Definition: A relation R on A is called an equivalence relation if :

1) Reflexivity : aRa

2) Symmetry : if aRb then bRa

3) Transitivity : if aRb and bRc then aRc for all $a, b, c \in A$.

We denote an equivalence relation by \sim .

Examples:

1. Any set A under equality: for $a, b \in A$ then $a \sim b$ if $a = b$.

2. Triangles in \mathbb{R}^2 under congruence (one can be transformed into the other by an isometry, i.e. a composition of translations, rotations,

and reflections).

3. $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ with $(a,b) \sim (c,d)$ if $ad = bc$ in \mathbb{Z} .

4. \mathbb{Z} under equivalence modulo 2: $m \sim n$ if $m-n$ is even.

5. Let $R \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, set:

$M_n(R) := \{n \times n \text{ matrices with entries in } R\}$.

$A \sim B$ if there is C invertible with $A = CBC^{-1}$.

This equivalence relation is called similarity of matrices.

6. Let R be a ring, set:

$R^{m \times n} := \{m \times n \text{ matrices with entries in } R\}$.

$A \sim B$ if there is $C \in M_n(R)$ and $D \in M_n(R)$ invertible

with $A = C B D$.

This equivalence relation is called equivalence of matrices.

7. Let R be a ring. On $M_n(R)$ set: (transpose)

$A \sim B$ if there is C invertible with $A = C B C^t$.

8. On $M_n(\mathbb{C})$ set: (adjoint)

$A \sim B$ if there is C invertible with $A = C B C^*$.

Definition: Let \sim be an equivalence relation on A . Let $a \in A$, the set:
 $\bar{a} = [a] = [a]_{\sim} := \{b \in A \mid a \sim b\}$ is called the equivalence class of
 a relative to \sim . We call $\bar{A} = \frac{A}{\sim} := \{\bar{a} \mid a \in A\}$ the set of
equivalence classes of \sim on A . The map:

$\bar{} : A \longrightarrow \bar{A}$ is called the natural or canonical surjection.
 $a \longmapsto \bar{a}$

Example:

1. $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ with $(a, b) \sim (c, d)$ if $ad = bc$ in \mathbb{Z} . Then:

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim \quad \text{and} \quad \overline{(a, b)} = \frac{a}{b}.$$

2. \mathbb{Z} under equivalence modulo 2: $m \sim n$ if $m - n$ is even. Then:

$$\bar{0} = \{ \text{all even integers} \} = \overline{2n} \quad \text{for all } n \in \mathbb{Z}.$$

$$\bar{1} = \{ \text{all odd integers} \} = \overline{2n+1} \quad \text{for all } n \in \mathbb{Z}.$$

We write $\overline{\mathbb{Z}} = \frac{\mathbb{Z}}{2\mathbb{Z}} = \{\bar{0}, \bar{1}\}$.

Definition: Let $A_i, i \in I$ be sets. Their union is the set:

$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I \text{ with } x \in A_i\}.$$

Their intersection is the set:

$$\bigcap_{i \in I} A_i := \{x \mid x \in A_i \text{ for all } i \in I\}.$$

We call I an indexing set. If $A_i \cap A_j = \emptyset$ for all $i, j \in I$, $i \neq j$, we call

this union disjoint and denote it $\bigvee_{i \in I} A_i$ or $\coprod_{i \in I} A_i$.

Proposition: Let \sim be an equivalence relation on A . Then $A = \bigvee_{\bar{a} \in \bar{A}} \bar{a}$. In

particular if $a, b \in A$ then either $\bar{a} = \bar{b}$ or $\bar{a} \cap \bar{b} = \emptyset$. Hence $\bar{a} = \bar{b}$ if and only if $a \sim b$.

Proof: Note that if $a \in A$ then $a \in \bar{a} \in \bar{A}$ so $a \in \bigcup_{\bar{a} \in \bar{A}} \bar{a}$ so $A \subseteq \bigcup_{\bar{a} \in \bar{A}} \bar{a}$.

If $b \in \bigcup_{\bar{a} \in \bar{A}} \bar{a}$ then $b \in \bar{a}$ for some $\bar{a} \in \bar{A}$, so $b \in A$ so $\bigcup_{\bar{a} \in \bar{A}} \bar{a} \subseteq A$.

Suppose $a, b \in A$ and $\not\exists c \in A$ such that $a \sim c$ and $b \sim c$. Then $a \sim b$, so $a \sim b$,

so $a \sim b$, so $a \sim b$. If $d \in \bar{a}$ then $d \sim a$, so $d \sim b$, so

$d \sim b$, whence $\bar{a} \subseteq \bar{b}$. Similarly $\bar{b} \subseteq \bar{a}$, so $\bar{a} = \bar{b}$. \square .

Definition: Let \sim be an equivalence relation on A . An element $x \in \bar{a}$, $a \in A$, is

called a representative of \bar{a} . A system of representatives for A relative to \sim is a set S containing exactly one element from each equivalence class.

Remark: If S is a system of representatives for A relative to \sim , then:

$$A = \bigvee \bar{x}.$$

$x \in S$

In particular, if $|S| < \infty$ then: $|S| = \sum_{x \in S} 1$. This is sometimes

called the Mantra of Equivalence Relations.

Section 6: Modular arithmetic.

Definition: Fix $m \in \mathbb{Z}$, $m > 1$. Let $a, b \in \mathbb{Z}$. We say that a is congruent to b

modulo m , and write $a \equiv b \pmod{m}$, if $m \mid a - b$ in \mathbb{Z} . The set:

$$\bar{a} = [a]_m := \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

$$= \{x \in \mathbb{Z} \mid x = a + km \text{ for some } k \in \mathbb{Z}\}$$

is a subset of \mathbb{Z} called the residue class of a modulo m . We denote it

by $a + m\mathbb{Z}$.

Proposition: Let $m \in \mathbb{Z}^+$. Then congruence modulo m is an equivalence relation.

Hence $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \dots \cup \overline{m-1}$ and $\overline{\mathbb{Z}} = \frac{\mathbb{Z}}{m\mathbb{Z}} = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$, so

$|\frac{\mathbb{Z}}{m\mathbb{Z}}| = m$. Let $a, b, c, d \in \mathbb{Z}$ with $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then $a+c \equiv b+d \pmod{m}$ and $a \cdot c \equiv b \cdot d \pmod{m}$. Define:

$$+ : \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}}$$
$$(\bar{a}, \bar{b}) \longmapsto \bar{a+b} =: \bar{a} + \bar{b}$$

$$\cdot : \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}}$$

$$(\bar{a}, \bar{b}) \mapsto \overline{\bar{a} \cdot \bar{b}} =: \bar{a} \cdot \bar{b}$$

Both + and · are well defined. Moreover for all $a, b, c \in \mathbb{Z}$:

$$(1) \quad (\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$$

$$(2) \quad \bar{0} + \bar{a} = \bar{a} = \bar{a} + \bar{0}$$

$$(3) \quad \bar{a} + (-\bar{a}) = \bar{0} = (-\bar{a}) + \bar{a}$$

$$(4) \quad \bar{a} + \bar{b} = \bar{b} + \bar{a}$$

$$(5) \quad (\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$

$$(6) \quad \bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1}$$

$$(7) \quad \bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$$

$$(8) \quad \bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

$$(9) \quad (\bar{b} + \bar{c}) \cdot \bar{a} = \bar{b} \cdot \bar{a} + \bar{c} \cdot \bar{a}$$

making $(\frac{\mathbb{Z}}{m\mathbb{Z}}, +, \cdot)$ into a commutative ring. We call $\bar{0}$ the zero

or additive unity and $\bar{1}$ the one or multiplicative unity.

Remark: Let \sim be an equivalence relation on \mathbb{A} . To show that an assignment

$f: \bar{\mathbb{A}} \rightarrow \mathcal{B}$ (for \mathcal{B} a set) is well defined, it must be independent of

the representative: if $\bar{a} = \bar{a}'$ we must have $f(\bar{a}) = f(\bar{a}')$.

Definition: A commutative ring is a set R together with two maps:

$+ : R \times R \rightarrow R$ and $\cdot : R \times R \rightarrow R$ called addition and multiplication

respectively, satisfying for all $a, b, c \in R$:

$$(1) \quad (a+b)+c = a+(b+c)$$

$$(2) \quad \text{There exists an element } 0 \in R \text{ with } 0+a = a = a+0$$

$$(3) \quad \text{There exists an element } -a \in R \text{ with } a+(-a) = 0 = (-a)+a$$

$$(4) \quad a+b = b+a$$

$$(5) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

$$(6) \quad \text{There exists an element } 1 \in R \text{ with } 1 \cdot a = a = a \cdot 1$$

$$(7) \quad a \cdot b = b \cdot a$$

$$(8) \quad a \cdot (b+c) = a \cdot b + a \cdot c$$

$$(9) \quad (b+c) \cdot a = b \cdot a + c \cdot a$$

If R does not satisfy (7), we call it a ring.

Examples:

1. Any field F is a commutative ring.

2. The sets \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , $\frac{\mathbb{Z}}{m\mathbb{Z}}$ are commutative rings.

3. If R is a ring, then $M_n(R)$ under the usual addition and multiplication of matrices is a ring.

3. If R is a ring, then $R[t]$ under the usual addition and multiplication of polynomials is a ring.

Definition: A map $f: R \rightarrow S$ between rings is called a ring homomorphism if

it preserves addition, multiplication, and units. Namely if $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ are rings with units $1_R, 1_S$ respectively, then for all $a, b \in R$:

$$(1) \quad f(a +_R b) = f(a) +_S f(b)$$

$$(2) \quad f(a \cdot_R b) = f(a) \cdot_S f(b)$$

$$(3) \quad f(1_R) = f(1_S)$$

A surjective or injective ring homomorphism is also called epimorphism or monomorphism, respectively.

Example: The canonical surjection $\bar{\ }: \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}}$ is an epimorphism.

Lemma: Let $m, n, a_1, \dots, a_r \in \mathbb{Z}$.

(1) If $\gcd(a_i, m) = 1$ for $i=1, \dots, r$ then $\gcd(a_1 \dots a_r, m) = 1$.

(2) If $\gcd(a_i, a_j) = 1$ for $i \neq j$ and $a_i \mid n$ for $i, j = 1, \dots, r$ then $a_1 \cdots a_r \mid n$.

Theorem: (Chinese Remainder Theorem) Let $m_1, \dots, m_r \in \mathbb{Z}$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$, $i, j = 1, \dots, r$. Let $c_1, \dots, c_r \in \mathbb{Z}$ and $m = m_1 \cdots m_r$. Then there

exists an $x \in \mathbb{Z}$ such that:

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \dots, \quad x \equiv c_r \pmod{m_r},$$

and it is unique modulo m (i.e. if $y \in \mathbb{Z}$ also satisfies $y \equiv c_i \pmod{m_i}$

for $i = 1, \dots, r$ then $x \equiv y \pmod{m}$).

Proof: We need to prove existence and uniqueness.

Existence: Let $n_i = \frac{m}{m_i} = m_1 \cdots \widehat{m_i} \cdots m_r$. We have $\gcd(m_i, n_i) = 1$ for

$i = 1, \dots, r$, so there exist equations (see Properties 4.9.(1)):

$$1 = d_i m_i + e_i n_i \text{ for some } d_i, e_i \in \mathbb{Z}, \quad i = 1, \dots, r.$$

Set $b_i = e_i n_i$ for $i = 1, \dots, r$, then $1 \equiv b_i \pmod{m_i}$, and if $i \neq j$ then

$b_i = e_i n_i = e_i m_1 \cdots \widehat{m_i} \cdots m_r$ so $m_j \mid b_i$ so $0 \equiv b_i \pmod{m_j}$. Hence:

$$x := c_1 b_1 + \cdots + c_r b_r \equiv c_i b_i \equiv c_i \pmod{m_i}, \quad i = 1, \dots, r.$$

Uniqueness: Suppose y also works. Then $x \equiv y \pmod{m_i}$ for $i = 1, \dots, r$, so

$m_i \mid x - y$ for $i = 1, \dots, r$. Then by the Lemma $m \mid x - y$ so $x \equiv y \pmod{m}$. \square .

Definition: Let R be a ring, if $a \in R$ has a multiplicative inverse, i.e. there is $b \in R$ with $a \cdot b = b \cdot a = 1$, it is called a unit. The set of units of R is denoted R^\times .

Corollary: Let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then \bar{a} is a unit in $\frac{\mathbb{Z}}{m\mathbb{Z}}$ if and only if

$$\gcd(a, m) = 1.$$

In particular, the set of units of $\frac{\mathbb{Z}}{m\mathbb{Z}}$ is closed under multiplication: let $x, y \in \mathbb{Z}$,

then \bar{x}, \bar{y} are units in $\frac{\mathbb{Z}}{m\mathbb{Z}}$ if and only if \bar{xy} is a unit in $\frac{\mathbb{Z}}{m\mathbb{Z}}$.

Remark: Let $m_1, \dots, m_r \in \mathbb{Z}$ with $\gcd(m_i, m_j) = 1$ if $i \neq j$, set $m = m_1 \dots m_r$.

Then the map: $\frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m_j\mathbb{Z}}$ is well defined, and thus:
 $[a]_m \longmapsto [a]_{m_j}$

$\frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ is also well defined. This map is
 $[a]_m \longmapsto ([a]_{m_1}, \dots, [a]_{m_r})$

a ring homomorphism, and by the Chinese Remainder Theorem it is

bijective. The inverse is also a ring homomorphism, so the above is a

ring isomorphism: $\frac{\mathbb{Z}}{m\mathbb{Z}} \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$. In particular if

$n = p_1^{e_1} \dots p_r^{e_r}$ is its prime factorization, then $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p_r^{e_r}\mathbb{Z}}$.

Furthermore: $(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times \longrightarrow (\frac{\mathbb{Z}}{m_1\mathbb{Z}})^\times \times \dots \times (\frac{\mathbb{Z}}{m_r\mathbb{Z}})^\times$ is also bijective.
 $[a]_m \longmapsto ([a]_{m_1}, \dots, [a]_{m_r})$

Section 8: Definitions and Examples (of a Group).

Definition: Let G be a set with a binary operation $\cdot: G \times G \rightarrow G$. We call

(G, \cdot) a group if it satisfies:

Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.

Unity: there is $e \in G$ such that $a \cdot e = a = e \cdot a$ for all $a \in G$.

Inverses: for every $a \in G$ there is $y \in G$ with $x \cdot y = e = y \cdot x$.

A group is called abelian if it satisfies:

Commutativity: $a \cdot b = b \cdot a$ for all $a, b \in G$.

Remarks: Let G be a set and $\cdot: G \times G \rightarrow G$ a binary operation.

0. If (G, \cdot) satisfies Associativity and Unity it is called a monoid.

1. If G satisfies associativity and $a_1, \dots, a_n \in G$, then $a_1 \cdots a_n$ is

independent of parenthesis. If G is a monoid, we set $a^0 = e$ for all

$a \in G$.

2. If G satisfies Unity, then the unit is unique. If e' is another

unit then: $e = e \cdot e' = e'$.

3. If G is a monoid, then $a \in G$ has at most one inverse denoted \bar{a} .

If b and c are inverses of a then:

$$b = b \cdot c = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c.$$

4. If G is a monoid and $a, b \in G$ have inverses, then ab has inverse

$$(ab)^{-1} = b^{-1}a^{-1}.$$

5. If G is a group then the cancellation laws hold: for all $a, b \in G$

if $ab = ac$ then $b = c$, and if $ba = ca$ then $b = c$.

6. If $(G, +)$ is a group, it will be an abelian group. We call G an additive group, write 0 for the unit and $-a$ for the inverse of $a \in G$.

Definition: Let R be a set with two binary operations $\cdot : R \times R \rightarrow R$ and

$+ : R \times R \rightarrow R$. We say that R is a ring under addition $+$ and

multiplication \cdot if $(R, +)$ is an additive group, (R, \cdot) is a monoid,

and they satisfy the distributive laws for all $a, b, c \in R$:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

We say that R is a commutative ring if (R, \cdot) is a commutative monoid.

Whenever $1 = 0$ we have $R = \{0\}$ the trivial ring. A non-trivial ring

is called a division ring if $(R \setminus \{0\}, \cdot)$ is a group. A commutative division ring is called a field.

Examples:

1. A trivial group is a group consisting of a single element.
2. Any ring, say \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , or $\frac{\mathbb{Z}}{m\mathbb{Z}}$, is an additive group under $+$.
3. The set \mathbb{R}^+ of positive real numbers is an abelian group under \cdot , but \mathbb{Z}^+ is only an abelian monoid under multiplication, and not a group.
4. If F is a field, say $F = \mathbb{Q}$, \mathbb{R} , or \mathbb{C} , then $F^\times = F \setminus \{0\}$ is an abelian group under multiplication. If R is any ring then its set of units R^\times is a group under \cdot , and it is abelian if R is commutative, called the group of units of R .
5. Let V be a vector space over a field. Then $(V, +)$ is an additive group.
6. Let S be a non-empty set, then $\Sigma(S) := \{f: S \rightarrow S \mid f \text{ bijection}\}$ is

a group under composition of functions. The unit is the identity map on S . A bijection $f: S \rightarrow S$ is called a permutation, and we call $\Sigma(S)$ the group of all permutations of S . It is a transitive group on S because for all $x, y \in S$ there is a permutation $f \in \Sigma(S)$ such that $f(x) = y$. The group $\Sigma(S)$ acts on S via :

$$\Sigma(S) \times S \longrightarrow S . \quad \text{If } S = \{1, \dots, n\} \text{ we call } S_n := \Sigma(S)$$

$$(f, s) \longmapsto f(s)$$

the symmetric group on n letters, note $|S_n| = n!$.

Definition: Let G be a group. A subset $H \subseteq G$ is called a subgroup of G if it becomes a group under the restriction of the binary operation, i.e. H is closed so $\cdot|_{H \times H}: H \times H \longrightarrow H$ makes sense.

Remark: A subgroup has the same unit as the original group.

Examples:

7. Let S be a non-empty set and $x_0 \in S$. The set :

$$\Sigma(S)_{x_0} = \{f \in \Sigma(S) \mid f(x_0) = x_0\}$$

the stabilizer of x_0 in $\Sigma(S)$. We say that the elements of $\Sigma(S)_{x_0}$

fix x_0 . In particular x_0 is a fixed point of the action of $\Sigma(S)_{x_0}$

on S . Note that $(S_n)_n$ looks like S_{n-1} algebraically. Let

$x_0, \dots, x_n \in S$, then

$$\Sigma(S)_{x_0} \cap \dots \cap \Sigma(S)_{x_n} = \{f \in \Sigma(S) \mid f(x_i) = x_i \text{ for } i=1, \dots, n\}$$

is a subgroup of $\Sigma(S)$ and of $\Sigma(S)_{x_i}$ for all $i=1, \dots, n$ stabilizing

x_1, \dots, x_n .

8. Let G be a group and $H_i, i \in I$, be subgroups of G . Then $\bigcap_{i \in I} H_i$ is a

subgroup of G . In general, $\bigcup_{i \in I} H_i$ is not a subgroup of G .

9. Let G be a group and $W \subseteq G$ a subset. Set:

$$W = \{H \subseteq G \mid H \text{ is a subgroup of } G \text{ with } W \subseteq H\}.$$

Now $W \neq \emptyset$ since $G \in W$, set: $\langle W \rangle := \bigcap_{H \in W} H = \bigcap_{\substack{W \subseteq H \subseteq G \\ H \text{ subgroup of } G}} H$.

This is the unique smallest subgroup of G containing W . We say that

W generates $\langle W \rangle$ and that W is a set of generators for $\langle W \rangle$, but such

a set is not unique. We say that G is finitely generated if there is

a finite set W with $G = \langle W \rangle$, and cyclic if there is an $a \in G$ with

$G = \langle a \rangle$. If this is the case then $G = \{a^n \mid n \in \mathbb{Z}\}$ and is abelian.

Namely $(\mathbb{Z}, +) = \langle 1 \rangle$ and $(\mathbb{Z}/m\mathbb{Z}, +) = \langle \bar{1} \rangle$ for $m > 1$.

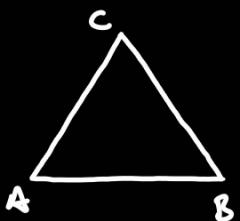
10. Let $T := \{z \in \mathbb{C} \mid |z| = 1\}$ where $|z| = \sqrt{z \cdot \bar{z}}$ and \bar{z} the complex conjugate of z . This is an abelian group under multiplication, called the circle group. It is a subgroup of \mathbb{C}^\times . If $n \in \mathbb{Z}^+$ then :

$\mu_n := \{z \in T \mid z^n = 1\} = \langle e^{2\pi i/n} \rangle$ is a cyclic subgroup of T called the group of n -th roots of unity. Another subgroup of T is:

$$\bigcup_{n \in \mathbb{Z}^+} \mu_n = \{z \in T \mid z \in \mu_n \text{ for some } n \in \mathbb{Z}^+\}.$$

Note that a subgroup of an abelian group is abelian.

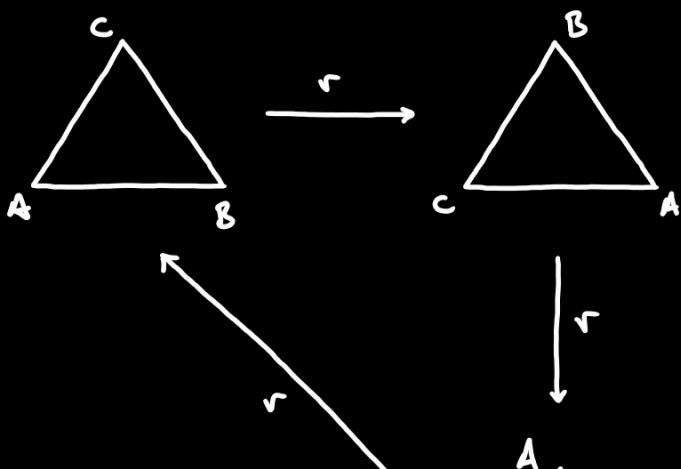
11. The symmetries of a geometric object (often) form a group.

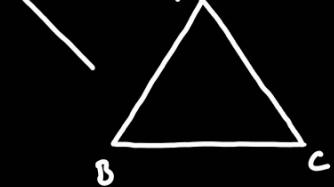


r : counterclockwise rotation of $\frac{2\pi}{3}$.

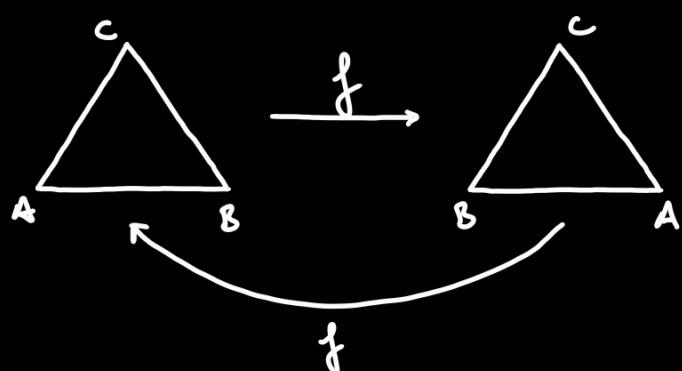
f : flip along the vertical axis.

Graphically :



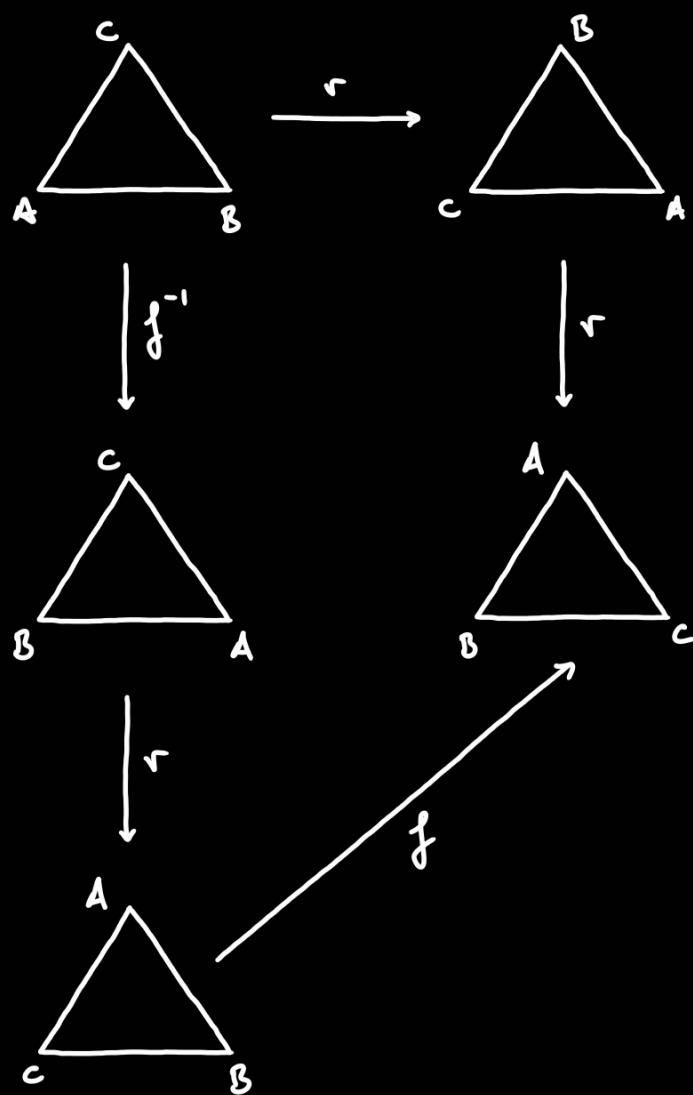


so $r^3 = 1$ and $|\langle r \rangle| = 3$.



so $f^2 = 1$ and $|\langle f \rangle| = 2$.

And similarly we obtain the relations $f^{-1}rf = r^2 = r^{-1}$:



Hence we obtain a non-abelian group with six elements $\{1, r, r^2, f, fr, r\bar{f}\}$.

We say that r and f generate this group subject to the relations $r^3 = 1$,

$f^2=1$, and $f^{-1}rf=r^{-1}$; and write this as " $\langle \text{generators} | \text{relations} \rangle$:

$$\langle r, f \mid r^3=1, f^2=1, f^{-1}rf=r^{-1} \rangle.$$

This group is called the dihedral group of order six D_3 , or the symmetries of an equilateral triangle.

In general, consider a regular n -gon for $n \geq 3$ with r a counterclockwise rotation of $\frac{2\pi}{n}$ and f a flip along the perpendicular at the bisection point of the base. Then under composition we get a non-abelian group

with $2n$ elements, which is defined by two generators satisfying three

relations: $r^n=1$, $f^2=1$, $f^{-1}rf=r^{-1}=r^{n-1}$. It is called the dihedral

group of order $2n$ D_n , or the symmetries of the regular n -gon.

$$D_n = \langle r, f \mid r^n=1, f^2=1, f^{-1}rf=r^{-1} \rangle.$$

Note that for $n > 3$, then $|D_n| \neq |S_n|$.

12. Let $\mathbb{Q} = \{1, -1, i, -i, j, -j, k, -k\}$ with the relations $(-1)^2=1$,

$k=ij=-ji$, and $i^2=j^2=-1$ is a non-abelian group called the

quaternion group.

13. Let F be $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, or any field. Then:

$GL_n(F) := \{ A \in M_n(F) \mid \det(A) \neq 0 \}$ is a group under matrix multiplication, called the general linear group of degree n . If $n=1$

then $GL_1(F) = F^\times$, but if $n > 1$ then $GL_n(F)$ is not abelian.

For a ring R the set of units $(M_n(R))^\times$ is also a group under

matrix multiplication, and if R is commutative taking

determinants is well defined and $A \in (M_n(R))^\times$ if and only if

$\det(A) \in R^\times$, so the general linear group of degree n is

$$GL_n(R) := (M_n(R))^\times.$$

14. Let V be a vector space over a field F . Then:

$\text{Aut}_F(V) := \{ T: V \rightarrow V \mid T \text{ is a linear isomorphism} \}$ is a group under composition, called the automorphism group of V , because an isomorphism of a vector space to itself is called an automorphism.

15. Let $G_i, i \in I$, be groups and set:

$$\bigtimes_{i \in I} G_i := \left\{ f: I \rightarrow \bigcup_{i \in I} G_i \mid f(i) \in G_i \text{ for all } i \in I \right\}. \text{ This is a}$$

group under component-wise operation, and it is called the external

direct product of $G_i, i \in I$. If G_i is abelian for all $i \in I$, then

$\bigtimes_{i \in I} G_i$ is also abelian.

16. Let $a, b \in \mathbb{Z}^+$ with $d = \gcd(a, b)$. Then $\langle a, b \rangle = \langle d \rangle$.

Section 9: First properties.

Proposition: Let G be a group and $H \subseteq G$ a non-empty subset. Then H is a subgroup of G if and only if :

(i) If $a, b \in H$ then $ab \in H$, and

(ii) If $a \in H$ then $a^{-1} \in H$.

Equivalently, if $a, b \in H$ then $ab^{-1} \in H$.

Corollary: Let G be a group and $H \subseteq G$ a non-empty finite subset. Then H is a subgroup of G if and only if H is closed under the operation.

Definition: Let G be a group. We say that $|G|$ is the order of G . Let $a \in G$,

we say that $|\langle a \rangle|$ is the order of a .

Definition: A map $f: G \rightarrow H$ between groups is called a group homomorphism if

it preserves the group operations. Namely if (G, \cdot_G) and (H, \cdot_H) are groups then $f(a \cdot_G b) = f(a) \cdot_H f(b)$ for all $a, b \in G$.

Remark: A group homomorphism preserves units: if (G, \cdot_G) and (H, \cdot_H) are groups with units e_G, e_H respectively, then:

$$\begin{aligned} e_H &= f(e_G)^{-1} \cdot_H f(e_G) = f(e_G)^{-1} \cdot_H f(e_G \cdot_G e_G) = f(e_G)^{-1} \cdot_H f(e_G) \cdot_H f(e_G) = \\ &= f(e_G). \end{aligned}$$

Similarly, $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

Definition: Let $f: G \rightarrow H$ be a group homomorphism. If it is injective we say it is a group monomorphism or monic. If it is surjective we say it is a group epimorphism or epic. If it is bijective and $f^{-1}: H \rightarrow G$ is a group homomorphism we say it is a group isomorphism.

Definition: Let $f: G \rightarrow H$ be a group homomorphism. Set:

$\ker(f) := \{a \in G \mid f(a) = e_H\}$ the kernel of f ,

$\text{im}(f) := \{f(a) \in H \mid a \in G\}$ the image of f .

Remark: If there is an isomorphism $f: G \rightarrow H$ between two groups, we say that G and H are isomorphic, and write $G \cong H$.

Proposition: Let $f: G \rightarrow H$ be a group homomorphism.

(1) $\ker(f)$ is a subgroup of G .

(2) $\text{im}(f)$ is a subgroup of H .

(3) f is monic if and only if $\ker(f) = \{e_G\}$.

(4) f is epic if and only if $\text{im}(f) = H$.

Proof:

(1) Let $a, b \in \ker(f)$. Then $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$ so $ab^{-1} \in \ker(f)$.

(2) Let $f(a), f(b) \in \text{im}(f)$. Then $f(a)f(b)^{-1} = f(ab^{-1}) \in \text{im}(f)$.

(3) \Rightarrow) Let f be monic and $a \in \ker(f)$. Then $f(a) = e_H = f(e_G)$ so $a = e_G$.

\Leftarrow) Let $\ker(f) = \{e_G\}$ and $a, b \in G$ with $f(a) = f(b)$. Then

$f(ab^{-1}) = f(a)f(b)^{-1} = f(b)f(b)^{-1} = e_H$ so $ab^{-1} \in \ker(f)$ so $a = b$.

(4) \Rightarrow) Let f be epic and $b \in H$. Then there is $a \in G$ with $b = f(a) \in \text{im}(f)$.

\Leftarrow) Let $\text{im}(f) = H$ and $b \in H$. Then there is $a \in G$ with $f(a) = b$. \square .

Example:

1. The group homomorphism $f: G \rightarrow H$ is called the trivial homomorphism.
 $a \mapsto e_H$

2. Let H be a subgroup of G , the inclusion of H in G is a group homomorphism.

3. Let F be a field. The map $\det: GL_n(F) \rightarrow F^\times$ is an epimorphism.

$$A \longmapsto \det(A)$$

Its kernel is $\text{SL}_n(F)$ the special linear group.

4. Let $m \in \mathbb{Z}^+$, the map $\bar{-}: \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}}$ is an epimorphism with kernel

$$x \longmapsto \bar{x}$$

$m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\}$ the multiples of m .

5. Let $m \in \mathbb{Z}^+$, the map $f: \frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \mathbb{C}^\times$ is a well defined group

homomorphism. It is monic with $\text{im}(f) = \mu_m$.

6. Let G be a group, then $f: G \longrightarrow G$ is a group homomorphism if and only if G is abelian.

Theorem: (Classification of cyclic groups) Let $G = \langle a \rangle$ be a cyclic group. The map

$\theta: \mathbb{Z} \longrightarrow G$ is a group epimorphism. It is an isomorphism if and only if a

$$m \longmapsto a^m$$

if G is infinite. If G is finite then $|G|=n$ if and only if $\ker(\theta) = n\mathbb{Z}$.

In that case the map $\bar{\theta}: \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow G$ is a group isomorphism.

Proof: Since $\theta(i+j) = a^{i+j} = a^i a^j = \theta(i) \cdot \theta(j)$ for all $i, j \in \mathbb{Z}$, this is a group

homomorphism. Since $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, it is an epimorphism.

Now θ is injective if and only if $a^i \neq a^j$ for all $i \neq j$ integers, if and only if $a^k \neq e_G$ for all $k \neq 0$ integer, if and only if θ is an isomorphism

(since θ is surjective). Hence if θ is injective then $\langle a \rangle$ is infinite. If $\langle a \rangle$

is infinite then $a^k \neq e_G$ for all $k \neq 0$ integer, so Θ is injective.

Suppose G is finite, so Θ is not injective, so there is $N \in \mathbb{Z}^+$ with $a^N = e_G$.

By the well-ordering principle there exists a least $n \in \mathbb{Z}^+$ with $a^n = e_G$.

Claim: We have $a^i = a^j$ if and only if $i \equiv j \pmod{n}$.

If $i=j$, we are done. Suppose $i \neq j$. WLOG suppose $j > i$ and using the

division algorithm write $j-i = kn+r$ with $0 \leq r < n$ and $r, k \in \mathbb{Z}$. Now

$$e_G = a^{j-i} = a^{kn+r} = (a^n)^k \cdot a^r = a^r \text{ so } r=0 \text{ by the minimality of } n, \text{ whence}$$

$$n \mid j-i \text{ so } i \equiv j \pmod{n}.$$

Thus by the claim $|G|=n$ if and only if $a^n = e_G$ means $n = k \cdot n$ for some $k \in \mathbb{Z}$, if and only if $\ker(\Theta) = n\mathbb{Z}$.

Now $\bar{\Theta}$ is a bijection by the claim, and since it is a group homomorphism, it is

a group isomorphism. □.

Theorem: (Cyclic subgroup Theorem) Let $G = \langle a \rangle$ be a cyclic group and $H \subseteq G$

a subgroup. Then :

1. $H = \{e_G\}$ or $H = \langle a^m \rangle$ with $m \in \mathbb{Z}^+$ the least positive integer such that

$a^m \in H$. If $|G|=n$ then $m|n$. If G is infinite then $|H|=1$ or H is infinite.

2. If $|G|=n$ and $m|n$ then $\langle a^m \rangle$ is the unique subgroup of G of order $\frac{n}{m}$.
3. If $|G|=n$ and n prime then G has no subgroup of order m .
4. If $|G|=n$ the number of subgroups of G is equal to the number of positive divisors of n .
5. If $|G|$ is a prime then $\{e\}$ and G are the only subgroups of G .

Section 10: Cosets

We extend the equivalence relation of congruence to any group and subgroup.

Definition: Let G be a group and H a subgroup. For $a, b \in G$ we write

$$a \equiv b \pmod{H} \text{ whenever } b^{-1}a \in H.$$

Remark: This is an equivalence relation.

The equivalence class \bar{a} of $a \in G$ is called the left coset of a relative to H .

We may write aH for \bar{a} and $\underline{G/H}$ for $\underline{\underline{G}} \equiv$.

Remark: We have the natural surjection: $\bar{_}: G \longrightarrow \underline{G/H}$.

$$a \mapsto a = ah$$

However, $\frac{G}{H}$ is not a group in general, so this surjection is not a group homomorphism: consider $G = S_3$ and $H = \{\text{id}, (12)\}$.

Remark: Let G be a group and H a subgroup. Now for any $a \in G$ we have:

$aH = cH$ if and only if $a = \bar{c}^{-1}a \in H$, namely $\bar{a} = \bar{c}$ if and only if

$c \in \bar{a}$ if and only if $a \in \bar{c}$. In fact, the notation $\bar{a} = aH$ is justified:

$$\bar{a} = \{b \in G \mid b \equiv a \pmod{H}\} = \{b \in G \mid \bar{a}^{-1}b \in H\} =$$

$$= \{b \in G \mid \bar{a}^{-1}b = h \text{ for some } h \in H\} = \{b \in G \mid b = ah \text{ for some } h \in H\} =$$

$$= \{ah \mid h \in H\} = aH.$$

Definition: Let G be a group, H a subgroup, and \mathcal{H} a system of representatives

for the equivalence modulo H . We call $|\mathcal{H}|$ the index of H in G and

denote it $[G : H]$.

Remark: Let G be a group, H a subgroup, and \mathcal{H} a system of representatives

for the equivalence modulo H . Then:

$$G = \bigvee_{a \in \mathcal{H}} aH \quad \text{so if } G \text{ is finite} \quad |G| = \sum_{a \in \mathcal{H}} |aH|.$$

Theorem: (Lagrange's Theorem) Let G be a finite group and H a subgroup.

$$\text{Then: } |G| = [G : H] |H|.$$

In particular $|H|$ divides $|G|$ and $[G:H]$ divides $|G|$.

Proof: We first note that for any group G and any subgroup H , then for all

$a \in G$ we have $|aH| = |H|$. To see this, define:

$\lambda_a : H \longrightarrow aH$, we have seen above that λ_a is surjective. But
 $h \mapsto ah$

if $ah = ah'$ for some $h, h' \in H$ then $h = h'$ and λ_a is injective. Now:

$$|G| = \sum_{a \in H} |aH| = \sum_{a \in H} |H| = |H| |H| = [G:H] |H|.$$

□.

Remark: There is an analogous result for right cosets, but if G is finite

and H is a subgroup then $\frac{|G|}{|H|}$ is both the left and right index of H

in G . Namely the number of right cosets of H in G is the same as

the number of left cosets of H in G , so $[G:H]$ makes sense without

prescribing right or left cosets. However, for $a \in G$ we have $aH \neq Ha$ in

general, when they are equal the subgroup will be called normal.

Remark: The converse to Lagrange's Theorem is false: if G is a finite group

and $m \in \mathbb{Z}^+$ with m dividing $|G|$, there may not be a subgroup H of G

such that $|H| = m$: consider A_4 the group of even permutations on four

elements.