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 $n \in S$, 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 $P(n)$ is true then $P(n+1)$ 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 $m < n$ 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 $1, \ldots, n$ that are divisible by m.

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

5) Let $m, 2m, \ldots, jm$ 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

$$p^{e+1} \nmid n! \text{ then } e = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

$p \nmid n!$. Then: $e = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$.

Corollary: Suppose that $a_1, \dots, a_r \in \mathbb{Z}^+$ with $a_1 + \cdots + a_r = n$. Then the multinomial coefficient $\frac{n!}{a_1! \cdots a_r!} \in \mathbb{Z}^+$.

Section 4: Division and the greatest common divisor.

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

1) If $r \mid m$ and $r \mid n$ then $r \mid am + bn$ for all $a, b \in \mathbb{Z}$.

2) If $r \mid n$ then $r \mid mn$.

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

4) If $m \mid n$ and $n \mid m$ then $n = \pm m$.

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

6) If $mr = nr$ then $m = n$ or $r = 0$.

Theorem: (Division Algorithm) Let $n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then there exist unique $q, r \in \mathbb{Z}$ satisfying $n = qm + r$ 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 $qm + r = n = q'm + r'$ 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 $m \leq r' - r < r' < m$, a contradiction.

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

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

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

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. □.

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) $d \mid m$ and $d \mid n$,

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

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

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

Theorem: (Euclidean Algorithm) Let $a, b \in \mathbb{Z}^+$ with $b \nmid a$. Then there exists $k \in \mathbb{Z}^+$ and equations:

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

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

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

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 $p \mid a_1 \cdots a_r$ with $a_1, \cdots, a_r \in \mathbb{Z}$, 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 $n! \mid p(p-1)\cdots(p-n+1)$ 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 $n! \mid (p-1)\cdots(p-n+1)$.

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 $e_1, \ldots, e_r \in \mathbb{Z}$ such that $n = p_1^{e_1} \cdots p_r^{e_r}$.

Proof: We need to show existence and uniqueness.

Existence: Let $S = \{ n \in \mathbb{Z}^+ \mid n>1$ 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 $n_1, n_2 \in \mathbb{Z}^+$ such that $n = n_1 \cdot n_2$, $1 < n_1$, and $1 < n_2$. By minimality of n we have $n_1, n_2 \notin S$, so n_1 and n_2 are product of primes, so $n = n_1 \cdot n_2$ 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 $e_1, \ldots, e_r, f_1, \ldots, f_s \in \mathbb{Z}^+$. WLOG $p_1 \leq q_1$,

since $p_1 | n$ by Euclid's Lemma $p_1 | q_i$, but $p_1 \leq q_i$ and both are prime so $i=1$ and $p_1 = q_1$. Dividing by $p_1 = q_1$, we obtain $p_1^{e_1-1} \cdots p_r^{e_r} = n = q_1^{f_1-1} \cdots q_s^{f_s}$. Using induction, we are done. □.

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 $f: A \longrightarrow B$ 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:

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

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

This equivalence relation is called <u>similarity of matrices</u>.

6. Let R be a ring, set:

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

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

with $A = CBD$.

This equivalence relation is called <u>equivalence of matrices</u>.

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

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

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

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

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 $\bar{A} = A/\sim := \{ \bar{a} \mid a \in A \}$ the set of equivalence classes of $\sim$ on A. The map:

$$\begin{aligned} - : A &\longrightarrow \bar{A} \\ a &\longmapsto \bar{a} \end{aligned}$$

is called the natural or canonical surjection.

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:

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

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

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 $\bar{a}\cap\bar{b}=0$. 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 $a\in\bigcup_{\bar{a}\in A}\bar{a}$ 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 $\emptyset\neq\bar{a}\cap\bar{b}\ni c$. Then $a\sim c$ and $b\sim c$, so $c\sim b$, so $a\sim b$, so $a\in\bar{b}$. If $d\in\bar{a}$ then $a\sim d$ so $d\sim a$, so $d\sim b$, so $d\in\bar{b}$, whence $\bar{a}\subseteq\bar{b}$. Similarly $\bar{b}\subseteq\bar{a}$, so $\bar{a}=\bar{b}$. □.

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 $|A| < \infty$ then: $|A| = \sum_{x \in S} 1 \cdot x$. 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 $a \equiv b \bmod m$, if $m \mid a-b$ in $\mathbb{Z}$. The set:

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

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

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 $\mathbb{Z} = \bar{0} \vee \bar{1} \vee \cdots \vee \overline{m-1}$ and $\mathbb{Z}/\equiv \; = \mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$, so $|\mathbb{Z}/m\mathbb{Z}| = m$. Let $a, b, c, d \in \mathbb{Z}$ with $a \equiv b \bmod m$ and $c \equiv d \bmod m$.

Then $a + c \equiv b + d \bmod m$ and $a \cdot c \equiv b \cdot d \bmod m$. Define:

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

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

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

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

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

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

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

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

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

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

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

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

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

making $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}, +, \cdot\right)$ into a commutative ring. We call $\bar{0}$ the <u>zero</u> or <u>additive unity</u> and $\bar{1}$ the <u>one</u> or <u>multiplicative unity</u>.

<u>Remark</u>: Let $\sim$ be an equivalence relation on A. To show that an assignment $f: \bar{A} \longrightarrow B$ (for B a set) is <u>well defined</u>, 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:

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

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

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

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

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

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

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

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

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

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

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

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 $f: R \to S$ 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) $f(a +_R b) = f(a) +_S f(b)$

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

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

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

Example: The canonical surjection $\bar{\ }: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ 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 $\gcd(a_1 \cdots a_r, m) = 1$.

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

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

$$x \equiv c_1 \bmod m_1, \quad x \equiv c_2 \bmod m_2, \ldots, \quad x \equiv c_r \bmod m_r,$$

and it is unique modulo m (i.e. if $y \in \mathbb{Z}$ also satisfies $y \equiv c_i \bmod m$ for $i = 1, \ldots, r$ then $x \equiv y \bmod m$).

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

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

Set $b_i = e_i n_i$ for $i = 1, \ldots, r$, then $1 \equiv b_i \bmod m_i$, and if $i \neq j$ then $b_i = e_i n_i = e_i m_1 \cdots \widehat{m_j} \cdots m_r$ so $m_j \mid b_i$ so $0 \equiv b_i \bmod m_j$. Hence:

$$x := c_1 b_1 + \cdots + c_r b_r \equiv c_i b_i \equiv c_i \bmod m_i, \quad i = 1, \ldots, r.$$

Uniqueness: Suppose y also works. Then $x \equiv y \bmod m_i$ for $i = 1, \ldots, r$, so $m_i \mid x - y$ for $i = 1, \ldots, r$. Then by the Lemma $m \mid x - y$ so $x \equiv y \bmod m$. $\square$.

Definition: Let R be a ring, if $a \in R$ has a multiplicative inverse, i.e. there is $b \in R$ with $a \cdot b = 1 = b \cdot a$, 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 $\overline{xy}$ 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 $m = m_1 \cdots m_r$.

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

$\frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$, $[a]_m \longmapsto ([a]_{m_1}, \dots, [a]_{m_r})$ is also well defined. This map is a ring homomorphism, and by the Chinese Reminder Theorem it is bijective. The inverse is also a ring homomorphism, so the above is a ring isomorphism: $\frac{\mathbb{Z}}{m\mathbb{Z}} \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$. In particular if $n = p_1^{e_1} \cdots p_r^{e_r}$ is its prime factorization, then $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_r^{e_r}\mathbb{Z}}$.

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

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

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

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

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

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 $\cdot : G \times G \longrightarrow G$ a binary operation.

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

1. If G satisfies associativity and $a_1, \ldots, a_n \in G$, 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: $e = e e' = e'$.

3. If G is a monoid, then $a \in G$ has at most one inverse, denoted a^{-1}.

If b and c are inverses of a then:

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

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 $\cdot : R \times R \to R$ and $+ : R \times R \to R$. 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 $\mathbb{Z}/m\mathbb{Z}$, 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 $\Sigma(S) := \{f : S \to S \mid f \text{ bijection}\}$ is

a group under composition of functions. The unit is the identity map on S. A bijection $f: S \to S$ 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:

$$\begin{aligned} \Sigma(S) \times S &\longrightarrow S \\ (f, s) &\longmapsto f(s) \end{aligned}$$

If $S = \{1, \dots, n\}$ we call $S_n := \Sigma(S)$ 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:

$$\Sigma(S)_{x_0} = \{ f \in \Sigma(S) \mid f(x_0) = x_0 \}$$ is a subgroup of $\Sigma(S)$ called 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:

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

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

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 $m > 1$.

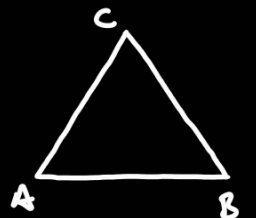
10. Let $T := \{z \in \mathbb{C} \mid |z| = 1\}$ where $|z| = \sqrt{z \cdot \bar{z}}$ and $\bar{z}$ the complex conjugate of z. This is an abelian group under multiplication, called the <u>circle group</u>. It is a subgroup of $\mathbb{C}^\times$. If $n \in \mathbb{Z}^+$ then:

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

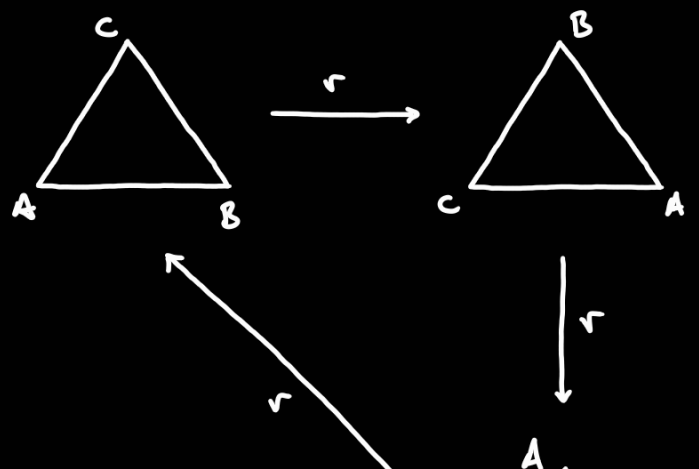
11. The symmetries of a geometric object (often) form a group.

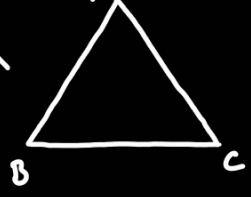


r: counterclockwise rotation of $\frac{2\pi}{3}$.

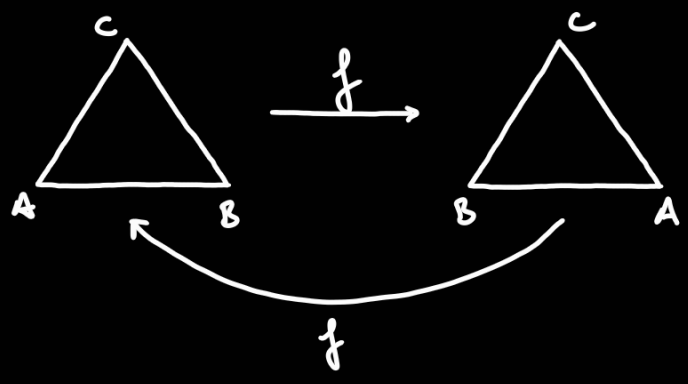
f: flip along the vertical axis.

Graphically:



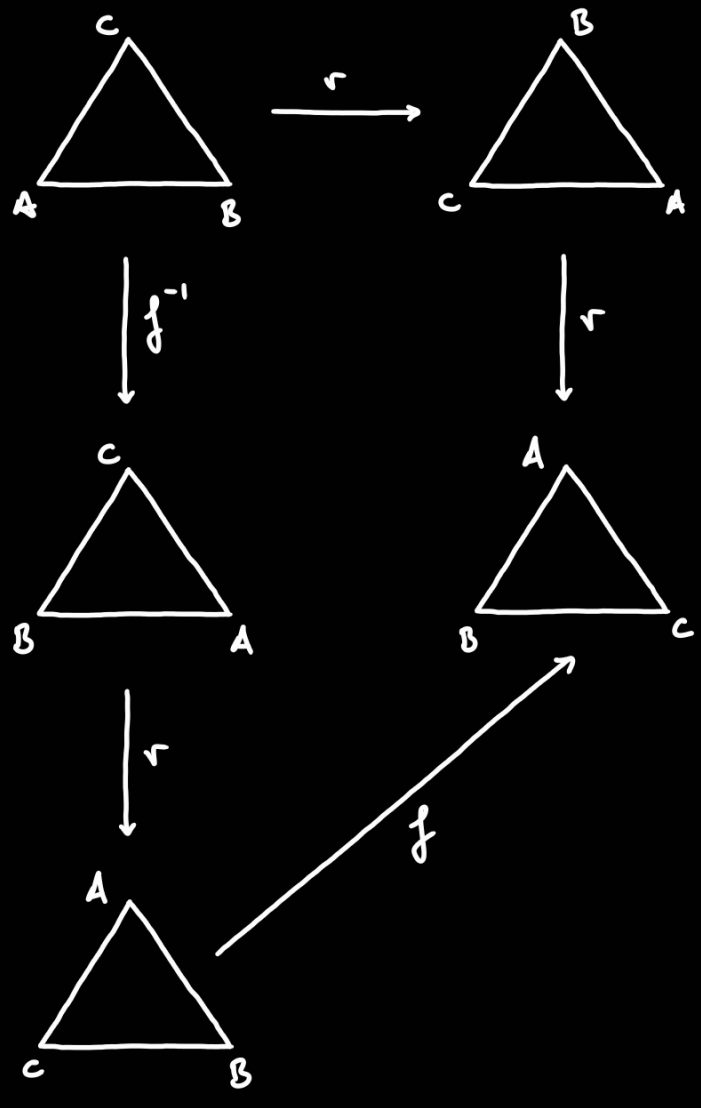


so $r^3 = 1$ and $|\langle r \rangle| = 3$.



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

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



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

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 "$\langle$generators | relations$\rangle$":

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

This group is called the <u>dihedral group of order six</u> 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 ~ 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 <u>dihedral group of order $2n$</u> 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 $Q=\{1,-1,i,-i,j,-j,k,-k\}$ with the relations $(-1)^2=1$, $k=ij=-ji$, and $i^2=j^2=-1$ is a non-abelian group called the <u>quaternion group</u>.

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:

$Aut_F(V) := \{ T : V \longrightarrow V \mid T \text{ is a linear isomorphism} \}$ 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:

$\underset{i \in I}{X} G_i := \left\{ f : I \longrightarrow \bigcup_{i \in I} G_i \;\middle|\; f(i) \in G_i \text{ for all } i \in I \right\}$. 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

$\prod_{i \in I} G_i$ 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 $f: G \to H$ 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:

$$e_H = f(e_G)^{-1} \cdot_H f(e_G) = f(e_G)^{-1} \cdot_H f(e_G \cdot_G e_G) = f(e_G)^{-1} \cdot_H f(e_G) \cdot_H f(e_G) =$$

$$= f(e_G).$$

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

Definition: Let $f: G \longrightarrow H$ 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 $f^{-1}: H \longrightarrow G$ is a group homomorphism we say it is a group isomorphism.

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

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

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

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

Proposition: Let $f: G \longrightarrow H$ 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

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

(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 $f: G \longrightarrow H$, $a \longmapsto e_H$ is called the trivial homomorphism.
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 $\det: GL_n(F) \longrightarrow F^\times$ is an epimorphism.

$A \longmapsto \det(A)$

Its kernel is $SL_n(F)$ the special linear group.

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

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

5. Let $m \in \mathbb{Z}^+$, the map $\begin{aligned} f : \frac{\mathbb{Z}}{m\mathbb{Z}} &\longrightarrow \mathbb{C}^\times \\ \bar{x} &\longmapsto e^{\frac{2\pi i}{m} \cdot x} \end{aligned}$ is a well defined group

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

6. Let G be a group, then $\begin{aligned} f : G &\longrightarrow G \\ x &\longmapsto x^{-1} \end{aligned}$ 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

$\begin{aligned} \theta : \mathbb{Z} &\longrightarrow G \\ m &\longmapsto a^m \end{aligned}$ is a group epimorphism. It is an isomorphism if and only

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 $\begin{aligned} \bar{\theta} : \frac{\mathbb{Z}}{n\mathbb{Z}} &\longrightarrow G \\ \bar{x} &\longmapsto a^x \end{aligned}$ 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 G is infinite. If G

(since Θ is surjective). Hence if Θ is injective then Θ is bijective. If G

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 <u>not</u> 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 $a^n = e_G$.

<u>Claim:</u> We have $a^i = a^j$ if and only if $i \equiv j \bmod n$.

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

Thus by the claim $|G| = n$ if and only if $a^m = e_G$ means $m = k \cdot n$ 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. $\square$.

<u>Theorem:</u> (Cyclic subgroup Theorem) Let $G = \langle a \rangle$ be a cyclic group and $H \leq G$ 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 $m \mid n$. If G is infinite then $|H| = 1$ or H is infinite.

2. If $|G| = n$ and $m \mid n$ then $\langle a^m \rangle$ is the unique subgroup of G of order $\frac{n}{m}$.

3. If $|G| = n$ and $m \nmid n$ 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

$a \equiv b \mod H$ 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 G/H for $G/\equiv$.

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

$a \longmapsto \bar{a} = aH$

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

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

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

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

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

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

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

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.

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:

$\lambda_a : H \longrightarrow aH$, $h \longmapsto ah$, we have seen above that λ_a is surjective. But if $ah = ah'$ for some $h, h' \in H$ then $h = h'$ and λ_a is injective. Now:

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

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.

Corollary: Let G be a finite group and $a \in G$. Then the order of a divides $|G|$.

Corollary: Let G be a finite group and H, K two finite subgroups with $\gcd(|H|,|K|)=1$.

Then $K \cap H = \{e\}$.

Corollary: Let G be a finite group of prime order p. Then $G \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$. In particular

the only subgroups of G are the trivial subgroup and G.

Corollary: Let G be a finite group and $a \in G$. Then $a^{|G|} = e$.

Proof: By Lagrange's Theorem $|\langle a \rangle|$ divides $|G|$, so $|G| = |\langle a \rangle| m$ for some $m \in \mathbb{Z}^+$.

Then: $a^{|G|} = a^{|\langle a \rangle| m} = \left(a^{|\langle a \rangle|}\right)^m = e^m = e$. $\square$.

Definition: The Euler phi function $\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ is defined by $\varphi(1) = 1$

and $\varphi(m) = \left|\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times\right|$ for $m > 1$.

Remark: The Euler phi function $\varphi(n)$ counts the number of positive integers smaller

than n and coprime to n. Moreover $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m,n)=1$.

Corollary: (Euler's Theorem) Let m, n be relatively prime integers, $m > 1$. Then:

$$n^{\varphi(m)} \equiv 1 \mod m.$$

Proof: Note that $\bar{n} \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times = \left\{\bar{a} \in \frac{\mathbb{Z}}{m\mathbb{Z}} \mid \gcd(a,m) = 1\right\}$, so:

$\bar{1} = \bar{n}^{|(\mathbb{Z}/m\mathbb{Z})^\times|} = \bar{n}^{\varphi(m)} = n^{\varphi(m)}$ in $\frac{\mathbb{Z}}{m\mathbb{Z}}$, namely $n^{\varphi(m)} \equiv 1 \bmod m$. $\square$.

Corollary: (Fermat's Little Theorem) Let $p \in \mathbb{Z}^+$ be prime. Then $n^p \equiv n \bmod p$ for all $n \in \mathbb{Z}$. If p does not divide n, then $n^{p-1} \equiv 1 \bmod p$.

Section 11: Homomorphisms.

Remark: Let $f: G \to H$ be a group homomorphism and $K \leq G$ a subgroup of G. Then $f(K)$ is a subgroup of H.

Definition: Let G be a group, $x \in G$. The map $\theta_x: G \to G$, $g \mapsto xgx^{-1}$ is called conjugation by x. For $H \leq G$ a subgroup, set:

$$xHx^{-1} := \theta_x(H) = \{xhx^{-1} \mid h \in H\}.$$

Lemma: Let G be a group, $x \in G$. Then $\theta_x: G \to G$ is an isomorphism. In particular for $H \leq G$ a subgroup then $\theta_x(H) \leq G$ is a subgroup and $H \cong xHx^{-1} = \theta_x(H)$. In particular $|H| = |xHx^{-1}|$.

Proof: The inverse of θ_x is $\theta_{x^{-1}}$ since for all $g \in G$:

$$\theta_x \theta_{x^{-1}}(g) = \theta_x(x^{-1}gx) = xx^{-1}gxx^{-1} = g$$

$$\theta_{x^{-1}} \theta_x(g) = \theta_{x^{-1}}(xgx^{-1}) = x^{-1}xgx^{-1}x = g.$$

Moreover Θ_x is a group homomorphism since for all $g_1, g_2 \in G$ we have:

$$\Theta_x(g_1 g_2) = x g_1 g_2 x^{-1} = x g_1 x^{-1} x g_2 x^{-1} = \Theta_x(g_1)\,\Theta_x(g_2).$$

Now $\Theta_x|_H : H \longrightarrow xHx^{-1}$ is surjective by definition, and injective because Θ_x is injective, so it is an isomorphism. $\square$.

<u>Remark:</u> If G is abelian then $\Theta_x : G \longrightarrow G$ is the identity. If G is <u>not</u> abelian there must be elements $x, y \in G$ satisfying $xy \neq yx$ so Θ_x is <u>not</u> the identity. In general for H a subgroup we have $xHx^{-1} \neq H$.

$g \longmapsto g$

<u>Definition:</u> Let G be a group and $H \leq G$ a subgroup. We say that H is <u>normal</u>, and write $H \trianglelefteq G$ whenever $xHx^{-1} = H$ for all $x \in G$.

<u>Example:</u> Consider $G = S_3$ and $H = \{e, (12)\}$. Then H is <u>not</u> normal.

<u>Remarks:</u> Let G be a group and $H \leq G$ a subgroup.

1. If $H \trianglelefteq G$, that does <u>not</u> mean that $\Theta_x|_H : H \longrightarrow H$ is the identity for all $x \in G$. For example $\langle r \rangle \trianglelefteq D_3$ but $frf^{-1} = r^{-1}$.

2. Let $\mathrm{Aut}(G) := \{\sigma : G \longrightarrow G \mid \sigma \text{ is an automorphism}\}$. Then $\mathrm{Aut}(G)$ is a group under composition, and it is a subgroup of $\Sigma(G)$. A conjugation Θ_x is also called an <u>inner automorphism</u>. Set $\mathrm{Inn}(G) := \{\Theta_x \text{ conjugation} \mid x \in G\}$, this

is a subgroup of $\mathrm{Aut}(G)$, called the inner automorphism group of G.

The following are equivalent:

(i) $H \trianglelefteq G$.

(ii) $\theta(H) = H$ for all $\theta \in \mathrm{Inn}(G)$.

(iii) $\theta|_H \in \mathrm{Aut}(H)$ for all $\theta \in \mathrm{Inn}(G)$.

(iv) The restriction map $|_H : \mathrm{Inn}(G) \longrightarrow \mathrm{Aut}(H)$ is well defined.

3. $H \trianglelefteq G$ if and only if $xH = Hx$ for all $x \in G$.

4. $H \trianglelefteq G$ if and only if $xHx^{-1} \subseteq H$ for all $x \in G$.

Example: Let G be a group.

1. We always have $1 \trianglelefteq G$ and $G \trianglelefteq G$. Whenever G is non-trivial and these are the only normal subgroups of G we say that G is a simple group. We have seen that $\frac{\mathbb{Z}}{p\mathbb{Z}}$ is a simple group for all primes p.

2. If G is abelian, every subgroup is normal.

3. The center of G is $Z(G) := \{x \in G \mid xg = gx \text{ for all } g \in G\}$. Any subgroup of $Z(G)$ is a normal subgroup of G. G is abelian if and only if $Z(G) = G$.

4. Let $f: G \longrightarrow H$ be a group homomorphism. Then $\ker(f) \trianglelefteq G$.

5. $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

6. If $H \leq G$ is of index two, then $H \trianglelefteq G$: for $a \in G \setminus H$ we have

$G = H \sqcup aH = H \sqcup Ha$ so we must have $aH = Ha$.

<u>Recall:</u> For $T: V \longrightarrow W$ a linear transformation of vector spaces over a field F with bases $\mathcal{B}$ and $\mathcal{C}$ respectively, we denote by $[T]_{\mathcal{B},\mathcal{C}}$ the matrix representation of this linear transformation relative to these bases.

7. If $\sigma \in S_n$ we can write $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ where the top row is the elements of the domain and the bottom row is the corresponding values. Let $\mathcal{E}_n = \{e_1, \ldots, e_n\}$ be the standard basis for $V = \mathbb{R}^n$. For each $\sigma \in S_n$ define the linear transformation $T_\sigma: V \longrightarrow V$. This is a vector space isomorphism with inverse $T_{\sigma^{-1}}$. Define $\Theta: S_n \longrightarrow GL_n(\mathbb{R})$ which is a group homomorphism. Each T_σ is a permutation matrix, namely it has exactly one non-zero entry 1 in each row and each column. Hence it is just a permutation of the rows or columns of the identity matrix.

$$\sum_i \alpha_i e_i \mapsto \sum_i \alpha_i e_{\sigma(i)}$$

$$\sigma \longmapsto [T_\sigma]_{\mathcal{E}_n}$$

The set $\mathrm{Perm}_n(\mathbb{R})$ of permutation matrices is the image of Θ, so it is a group.

We have the isomorphism $\Theta : S_n \to \mathrm{Perm}_n(\mathbb{R})$, and that $\det(A) = \pm 1$ for all $A \in \mathrm{Perm}_n(\mathbb{R})$, so:

$$S_n \xrightarrow{\Theta} \mathrm{Perm}_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\} \text{ is a group homomorphism.}$$

For $n > 1$ we call $A_n := \ker(\det \circ \Theta)$ the alternating group on n letters.

The elements of A_n are called even permutations and the elements of $S_n \setminus A_n$ are called odd permutations. We have $A_n \trianglelefteq S_n$ and $[S_n : A_n] = 2$.

Remark:

1. The groups of prime order are the only abelian simple groups. The group A_5 is the non-abelian simple group of smallest order.

Theorem: (Abel's Theorem) The group A_n is simple for $n \geq 5$.

A_2 is trivial, A_3 is the cyclic group of order three (so simple), A_4 is not simple.

2. If K, H are subgroups of G with $K \subseteq H \subseteq G$, $K \trianglelefteq H$, $H \trianglelefteq G$, it is not necessarily true that $K \trianglelefteq G$.

$G = D_4$, $K = \langle f \rangle$, $H = \langle r^2, f \rangle$.

3. If K, H are subgroups of G with $K \subseteq H \subseteq G$ and $K \trianglelefteq G$, then $H \trianglelefteq G$.

Definition: Let G be a group. A subgroup H is a <u>characteristic group</u> of G if for every $\sigma \in \mathrm{Aut}(G)$ we have $\sigma|_H \in \mathrm{Aut}(H)$. We write $H \trianglelefteq\trianglelefteq G$.

Remark: If $H \trianglelefteq\trianglelefteq G$ then $H \trianglelefteq G$, and if $K \trianglelefteq\trianglelefteq H \trianglelefteq\trianglelefteq G$ then $K \trianglelefteq\trianglelefteq G$.

Section 12: The first isomorphism theorem.

Theorem: (First Isomorphism Theorem) Let $f: G \to H$ be a group homomorphism. Then there is a commutative diagram of groups and groups homomorphisms:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle\pi}\downarrow & \overset{\bar{f}}{\nearrow} & \uparrow{\scriptstyle\iota} \\ \dfrac{G}{\ker(f)} & \xrightarrow{\quad} & \mathrm{im}(f) \end{array}$$

with π the canonical group epimorphism, $\bar{f}$ a group isomorphism, and ι the canonical group monomorphism.

Proof: We first check that $\bar{f}: \dfrac{G}{\mathrm{im}(f)} \longrightarrow \mathrm{im}(f)$, $\bar{a} \longmapsto f(a)$ is a well defined group homomorphism.

Suppose that $\bar{a} = \bar{b}$ in $\dfrac{G}{\ker(f)}$ for some $a, b \in G$. Then $\bar{f}(\bar{a}) = f(a) = f(b) = \bar{f}(\bar{b})$ so $\bar{f}$ is well defined. This map is surjective since if $x \in \mathrm{im}(f)$ then there is $a \in G$ with $f(a) = x$, and now $\bar{f}(\bar{a}) = x$ so $x \in \mathrm{im}(\bar{f})$. This map is also injective, since if $\bar{f}(\bar{a}) = \bar{f}(\bar{b})$ for some $a, b \in G$, then $f(a) = f(b)$, so $f(ab^{-1}) = 1$ so $ab^{-1} \in \ker(f)$ so $\bar{a} = \bar{b}$. This map is a group homomorphism since for any $a, b \in G$ we have

$\bar{f}(\bar{a}\bar{b}) = \bar{f}(\overline{ab}) = f(ab) = f(a)f(b) = \bar{f}(\bar{a})\bar{f}(\bar{b})$. Moreover the diagram commutes:

$$\iota \bar{f} \pi(a) = \iota \bar{f}(\bar{a}) = \iota f(a) = f(a) \quad \text{for all } a \in G. \qquad \square.$$

Example: Let G be a group, the map $\Theta : G \longrightarrow Aut(G)$, $x \longmapsto \Theta_x$ is a group homomorphism.

We have that the unit in $Aut(G)$ is $1_G = \Theta_e$, so $\ker(\Theta) = Z(G)$ the center of G. By the First Isomorphism Theorem $\bar{\Theta} : \frac{G}{Z(G)} \longrightarrow Inn(G)$ is an isomorphism.

Remark: Let G be a group and $H \leq G$ a subgroup. Then G/H is a group under $\cdot : G/H \times G/H \longrightarrow G/H$, $(\bar{a}, \bar{b}) \longmapsto \overline{ab}$ if and only if $H \trianglelefteq G$ is a normal subgroup.

Corollary: (Cayley's Theorem) Let G be a group. Then the map: $\lambda : G \longrightarrow \Sigma(G)$, $x \longmapsto \begin{pmatrix} \lambda_x : G \to G \\ g \mapsto xg \end{pmatrix}$ is a group monomorphism. In particular if $|G| = n$ then there exists a monomorphism $G \hookrightarrow S_n$.

Corollary: Let G be a finite group, p the smallest positive prime dividing $|G|$, and suppose that there is H a subgroup of G of index p. Then $H \trianglelefteq G$.

Section 13: The correspondence principle.

Theorem: (Correspondence Principle) Let $f : G \to H$ be a group epimorphism. Then:

1) If A is a (normal) subgroup of G, then $f(A)$ is a (normal) subgroup of H.

2) If A is a subgroup of G containing $\ker(f)$ then $f^{-1}(f(A)) = A$.

3) If B is a (normal) subgroup of H then $f^{-1}(B)$ is a (normal) subgroup of A containing $\ker(f)$ and $B = f(f^{-1}(B))$.

In particular:

$$\{A \mid A \subseteq G \text{ subgroup containing } \ker(f)\} \rightleftharpoons \{B \mid B \subseteq H \text{ subgroup}\}$$
$$A \longmapsto f(A)$$
$$f^{-1}(B) \longmapsto B$$

is a bijection of sets preserving inclusions and restricting to a bijection on normal subgroups.

Theorem: (Third Isomorphism Theorem) Let G be a group with normal subgroups K and H with $K \subseteq H$. Then $f: G/K \to G/H$ is a group epimorphism with kernel H/K, $xK \longmapsto xH$ inducing an isomorphism $\overline{f}: (G/K)/(H/K) \to G/H$.

Proof: Since $H, K \trianglelefteq G$, we know that G/K and G/H are groups. Now f is well defined since if $xK = yK$ then $y^{-1}x \in K \subseteq H$ so $xH = yH$, and surjective since given $xH \in G/H$ we have $f(xK) = xH$. Moreover f is a group homomorphism since: $f(xKyK) = f(xyK) = xyH = xHyH = f(xK)f(yK)$. Now $\ker(f) = H/K$:

$\subseteq$) If $xk \in \ker(f)$ then $xH = f(xk) = eH$ so $x \in H$ so $xK \in H/K$.

$\supseteq$) If $x \in H$ then $f(xk) = xH = eH$ so $xk \in \ker(f)$.

The result follows from the First Isomorphism Theorem. $\square$.

<u>Theorem:</u> (Second Isomorphism Theorem) Let G be a group and $H, N \leq G$ subgroups with N normal. Then:

1) $H \cap N \trianglelefteq H$.

2) $HN = NH$ is a subgroup of G.

3) $N \trianglelefteq HN$.

4) $H/(H \cap N) \cong HN/N$.

<u>Proof:</u> 1), 2), 3) do <u>not</u> require fancy machinery.

4) Define $f: H \longrightarrow HN/N$, $x \longmapsto xN$. This is a group homomorphism:

$f(xy) = xyN = xNyN = f(x)f(y)$ for all $x, y \in H$. Moreover $\ker(f) = H \cap K$:

$\subseteq$) If $x \in \ker(f) \leq H$ then $xN = f(x) = eN$ so $x \in N$, so $x \in H \cap N$.

$\supseteq$) If $x \in H \cap N$ then $f(x) = xN = eN$ so $x \in \ker(f)$.

Finally, f is surjective since:

$HN/N = \{hnN \mid h \in H, n \in N\} = \{hN \mid h \in H\}$.

The result follows from the First Isomorphism Theorem. $\square$.

Section 14: Finite abelian groups.

Lemma: Let G be an abelian group, H_1, H_2 finite subgroups of relatively prime order. Then H_1H_2 is a group. If $H_1 \cap H_2 = 1$ then $|H_1H_2| = |H_1||H_2|$. If H_1 and H_2 are both cyclic, then H_1H_2 is cyclic.

Proposition: Let G be a finite abelian group and p a prime dividing $|G|$. Then there exists an element of order order p in G.

Proof: We prove this by induction on G. The case $|G| = 1$ does not apply. If $|G| = p$ a prime, then $G \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$ and we are done. If $|G|$ is not a prime, then G has a subgroup $1 < H < G$. If $p \mid |H|$, since $|H| < |G|$, we are done by induction, so we may assume that $p \nmid |H|$. Thus there exists a prime q different from p with $q \mid |H|$. By induction hypothesis, there exists an element $y \in H$ of order q. Since G is abelian then $\bar{G} = \frac{G}{\langle y \rangle}$ is a group. By Lagrange's Theorem $|\bar{G}| = \frac{|G|}{|\langle y \rangle|}$ and since $p \mid |G|$ and $p \neq q$ we have $p \mid |\bar{G}|$. Denoting by $^- : G \to \bar{G}$ the canonical epimorphism, since $|\bar{G}| < |G|$, by induction hypothesis there is an $x \in G$ with $\bar{x} \in \bar{G}$ having order p in $\bar{G}$.

Now $\overline{z^p} = \bar{z}^p = \bar{1}$ in $\bar{G}$, so $z^p \in \langle y \rangle$ so $z^p = y^i$ for some $i \in \mathbb{Z}^+$. Now z^t has order q in G: $(z^t)^q = (z^p)^t = (y^i)^t = (y^t)^i = 1$ since y has order q. □.

Theorem: Let G be a finite abelian group and p a prime dividing G, say $|G| = p^n m$ with $\gcd(p, m) = 1$. Then: $G(p) := \{x \in G \mid x^{p^r} = e \text{ for some } r \in \mathbb{Z}^+\}$ is normal in G and $|G(p)| = p^n$. Moreover, $G(p)$ is the unique subgroup of G of order p^n.

Corollary: Let G be a finite abelian group of order $n = p_1^{m_1} \cdots p_r^{m_r}$ with positive primes $p_1 < \cdots < p_r$ and positive integers $m_1, \ldots, m_r$. Then $G = G(p_1) \cdots G(p_r)$ and $G \cong G(p_1) \times \cdots \times G(p_r)$.

We have reduced the study of finite abelian groups to the study of groups having order a power of a prime.

Definition: Let $p \in \mathbb{Z}^+$ be a prime. A non-trivial group of order a power of p is called ~~p-group~~ a p-group.

Lemma: Let G be a finite additive p-group with $x \in G$ an element of maximal order. Then there exists a subgroup H of G such that $G = \langle x \rangle \oplus H$.

Corollary: Let G be a finite abelian p-group. Then G is a product of cyclic groups.

Proposition: Every finite abelian group is a product of cyclic groups.

Theorem: (Fundamental Theorem of Finite Abelian Groups) Let G be a finite additive group and for each prime $p \in \mathbb{Z}^+$ dividing G let $G(p)$ be the unique p-subgroup of G of maximal

order. Then: $G = \bigoplus_{p \mid |G|} G(p)$. If $p \mid |G|$ then $G(p) \cong \bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{p^{u_i}\mathbb{Z}}$ with $r \in \mathbb{Z}^+$ unique and $1 \leq u_1 \leq \cdots \leq u_r$ unique up to reordering. In particular, any finite abelian group is a product of cyclic p-groups for various primes $p \in \mathbb{Z}^+$.

Proof: By the above Corollary and Proposition, it suffices to show $G(p) \cong \bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{p^{u_i}\mathbb{Z}}$ and uniquely up to isomorphism. Since every abelian p-group is isomorphic to a product of cyclic p-groups by the Lemma above, and every cyclic p-group must be isomorphic to $\frac{\mathbb{Z}}{p^u\mathbb{Z}}$ for some $u \in \mathbb{Z}^+$, we only need to show that if $\bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{p^{u_i}\mathbb{Z}} \cong \bigoplus_{j=1}^{s} \frac{\mathbb{Z}}{p^{m_j}\mathbb{Z}}$ with $u_1 \geq \cdots \geq u_r$ and $m_1 \geq \cdots \geq m_s$, then $r = s$ and $u_i = m_i$ for all i. We prove this by induction on $|G(p)|$.

Suppose $\bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{p^{u_i}\mathbb{Z}} \cong \bigoplus_{j=1}^{s} \frac{\mathbb{Z}}{p^{m_j}\mathbb{Z}}$. Since $p\left(\frac{\mathbb{Z}}{p^k\mathbb{Z}}\right) \cong \frac{\mathbb{Z}}{p^{k-1}\mathbb{Z}}$ for all $k \in \mathbb{Z}^+$, multiplying by p gives $\bigoplus_{i=N+1}^{r} \frac{\mathbb{Z}}{p^{u_i-1}\mathbb{Z}} \cong \bigoplus_{i=M+1}^{s} \frac{\mathbb{Z}}{p^{m_j-1}\mathbb{Z}}$. Without loss of generality, assume that $N \leq M$. By induction $u_i - 1 = m_j - 1$ for all $i > N$ and $r - N + 1 = s - N + 1$. Notice that $u_i = 1$ for $i \leq N$ and $m_j = 1$ for $j \leq M$. Since $\prod_{i=1}^{r} p^{u_i} = |G(p)| = \prod_{j=1}^{s} p^{m_j}$ then $\prod_{i=1}^{N} p = \prod_{j=1}^{M} p$ so $N = M$. Thus $r = s$ and $u_i = m_i$ for all i. □.

Section 16: Finitely generated groups.

If G is an arbitrary group and H a subgroup of finite index n in G, then the General Cayley Theorem gives a group homomorphism $\lambda : G \to \Sigma\left(\frac{G}{H}\right) \cong S_n$. The First

$$x \longmapsto \left(\lambda_x : G/H \to G/H,\ gH \mapsto xgH\right)$$

Isomorphism Theorem gives a group

monomorphism $\bar{\lambda}: G/\ker(\lambda) \longrightarrow S_n$. Since S_n is finite, $G/\ker(\lambda)$ is finite, and thus G contains a normal subgroup of finite index. We study this context for G finitely generated.

Proposition: Let G be a finitely generated group and $n \in \mathbb{Z}^+$. Then there exist finitely many subgroups of G of index n.

Proof: Let $G = \langle a_1, \dots, a_r \rangle$ and $\varphi: G \longrightarrow S_n$ a group homomorphism. Then φ is completely determined by $\varphi(a_1), \dots, \varphi(a_r) \in S_n$. Since we have finitely many choices, there are only finitely many possible group homomorphisms φ. For each such φ we have one normal subgroup $\ker(\varphi)$, so we have finitely many normal subgroups.

Fix $H < G$, $[G:H] = n$, then we can define $\varphi: G \longrightarrow \Sigma(G/H) \cong S_n$ a group homomorphism. There can only be finitely many

$$x \longmapsto \left(\lambda_x : G/H \to G/H,\ gH \mapsto xgH\right)$$

of these. Fix one such φ, notice that if H and K are two different subgroups of index n giving this same φ, then $\ker(\varphi) \subseteq H$ and $\ker(\varphi) \subseteq K$ (if $x \in \ker(\varphi)$ then $\varphi(x) = id_{\Sigma(G/H)}$ so $xhH = \lambda_x(hH) = \varphi(x)(hH) = id_{\Sigma(G/H)}(hH) = hH$ for any $h \in H$, so $x \in H$). Now $\varphi: G \longrightarrow \mathrm{im}(\varphi)$ is surjective, and since S_n is finite,

$\text{im}(\Psi)$ is also finite, and it has finitely many subgroups. By the Correspondence Principle, there will be finitely many subgroups L of G satisfying $\text{Ker}(\Psi) \subseteq L \subseteq G$, which are the ones with $[G:L] = n$. Since there are finitely many Ψ, we are done. $\square$.

Corollary: Let G be a finitely generated group. Suppose G contains a subgroup H of finite index. Then there exists a characteristic subgroup K of H of finite index in G.

Proof: By the Proposition, there exist finitely many subgroups $H, H_2, \ldots, H_m$ of finite index $[G:H]$. Given an automorphism Ψ of G, it sends subgroups to subgroups, so $\Psi(H) = H_i$ for some i. Let $K = H \cap H_2 \cap \cdots \cap H_m$, we have $\Psi(K) = K$ so K is a characteristic subgroup of H. Since K is the finite intersection of subgroups of finite index, K has finite index. $\square$.

Theorem: Let G be a finitely generated group and H be a subgroup of finite index. Then H is a finitely generated group.

Proof: Let $G = \langle a_1, \ldots, a_s \rangle$ and $y_1, \ldots, y_n$ a system of representatives for the cosets of H in G with $y_1 = e$. Let $\lambda : G \longrightarrow \Sigma(G/H)$, since λ_x is a bijection (with inverse $\lambda_{x^{-1}}$) it permutes the

$$a \longmapsto \begin{pmatrix} \lambda_a : \frac{G}{H} \to \frac{G}{H} \\ xH \mapsto axH \end{pmatrix}$$

cosets $y_1 H, \ldots, y_n H$. Fix $i = 1, \ldots, r$, then for each $j = 1, \ldots, n$ there exists a $k = k(i,j)$

with $k \in \{1,\dots,n\}$ satisfying $a_i y_j H = y_k H$. Hence there are $h_{ij} \in H$ satisfying

$y_k = a_i y_j h_{ij}$ for all $i = 1,\dots,r$ and $j = 1,\dots,n$. Let $H_0 := \langle h_{ij} \rangle_{i=1,\dots,r}^{j=1,\dots,n} \leq G$ a finitely generated subgroup of G contained in H. To prove that H is finitely generated, it suffices to prove that $H \leq H_0$. Set $W = \bigcup_{j=1}^{n} y_j H_0$, now for each $i = 1,\dots,r$ we have:

$a_i W = \bigcup_{j=1}^{n} a_i y_j H_0 = \bigcup_{j=1}^{n} a_i y_j h_{ij} H_0 = \bigcup_{k=1}^{n} y_k H_0 = W$. Since $G = \langle a_1,\dots,a_r \rangle$ we have $GW = W$ and since $e \in W$ we have $G = W = \bigcup_{j=1}^{n} y_j H_0$. In particular

$H \leq G = \bigcup_{j=1}^{n} y_j H_0$, and $H = eH = y_1 H$ is disjoint from $\bigcup_{j=2}^{n} y_j H$, so H is disjoint from $\bigcup_{j=2}^{n} y_j H_0$, so $H \leq y_1 H_0 = e H_0 = H_0$. □.

Section 19: The orbit decomposition theorem

Groups act on objects: the symmetric group acts on finite sets, the dyhedral group acts on regular polygons, and matrices act on vectors. These actions induce equivalence relations on the set, which will be useful to compute cardinalities.

Definition: Let G be a group, S a non-empty set. We say that S is a <u>left G-set</u> under the action $* : G \times S \to S$ whenever for all $g_1, g_2 \in G$ and $s \in S$ we have:

$(g, s) \mapsto g * s$

(i) $(g_1 g_2) * s = g_1 * (g_2 * s)$.

(ii) $e * s = s$.

We say that $*$ is a G-action on S.

Remark: Let S be a G-set, H a subgroup of G. Then S is an H-set with H-action

$$*|_{H\times S} : H\times S \longrightarrow S.$$
$$(h,s) \longmapsto h*s$$

Definition: Let S be a G-set under $*: G\times S \to S$. For $s_1, s_2 \in S$ we denote $s_1 \sim_G s_2$ whenever there exists a $g\in G$ with $s_1 = g*s_2$.

Lemma: Let S be a G-set under $*: G\times S \to S$. Then $\sim_G$ is an equivalence relation.

Proof: Reflexivity: we have $e*s=s$ for all $s\in S$, so $s\sim_G s$.

Symmetry: let $s_1\sim_G s_2$, then there is $g\in G$ with $s_1 = g*s_2$. Now:

$$g^{-1}*s_1 = g^{-1}*(g*s_2) = (gg^{-1})*s_2 = e*s_2 = s_2, \text{ so } s_2 \sim_G s_1.$$

Transitivity: let $s_1\sim_G s_2$ and $s_2\sim_G s_3$, then there are $g,h\in G$ with $s_1 = g*s_2$ and $s_2 = h*s_3$. Then: $s_1 = g*s_2 = g*(h*s_3) = (gh)*s_3$ so $s_1\sim_G s_3$. □.

Definition: Let S be a G-set under $*: G\times S \to S$. The equivalence class of $s\in S$ is called the orbit of s under $*$, we denote it by $G*s$.

$$G*s := \overline{s} = [s]_{\sim_G} = \{ s'\in S \mid \exists g\in G \text{ with } s' = g*s\} = \{g*s \mid g\in G\}.$$

We will denote by $\mathcal{O}$ a system of representatives for the equivalence classes of $\sim_G$.

We will denote the set of orbits of $\sim_G$ as $G\backslash S := \frac{S}{\sim_G} = \{G*s \mid s \in \mathcal{O}\}$.

Remark: Let S be a G-set under $*: G \times S \to S$ and $\mathcal{O}$ a system of representatives for the equivalence class $\sim_G$, then:

$$S = \bigvee_{s \in \mathcal{O}} G*s \quad \text{so if } S \text{ is finite } |S| = \sum_{s \in \mathcal{O}} |G*s|.$$

We now want to find a way of computing the size of an orbit.

Definition: Let S be a G-set under $*: G \times S \to S$, and $s \in S$. The stabilizer or isotropy subgroup of s is: $G_s := \{x \in S \mid x*s = s\}$.

Lemma: Let S be a G-set under $*: G \times S \to S$. Then G_s is a subgroup of G.

Proof: Since $e \in G_s$ because $e*s = s$, we have $G_s \neq \emptyset$. For $x, y \in G_s$ we have $xy \in G_s$ because $(xy)*s = x*(y*s) = x*s = s$, and $x^{-1} \in G_s$ because $x^{-1}*s = x^{-1}*(x*s) = (x^{-1}x)*s = s$. □.

Proposition: Let S be a G-set under $*: G \times S \to S$. The function $f_s: \frac{G}{G_s} \to G*s$, $xG_s \mapsto x*s$ is a well-defined bijection. In particular if $[G : G_s]$ is finite then $|G*s| = [G : G_s]$ and $|G*s|$ divides $|G|$.

Proof: For $x, y \in G$, note that:

$$f_s(x) = x*s = y*s = f_s(y) \iff y^{-1}*(x*s) = y^{-1}*(y*s) = s$$

$\Leftrightarrow (y^{-1}x) * s = s \Leftrightarrow y^{-1}x \in G_s \Leftrightarrow xG_s = yG_s.$

The forward implication proves that f_s is injective. The backward implication proves that f_s is well defined. Moreover since given $x \in G$ we have $x * s = f_s(xG_s)$, then f_s is well defined. $\square$.

Example: Let S be the faces of a cube and G the group of rotations of the faces of a cube. Now G acts on S, and given any two faces $s_1, s_2 \in S$, there is an element $g \in G$ taking s_1 to s_2. Hence there is one single orbit under this action. Moreover if $s \in S$ is a face, the isotropy group G_s of s is the cyclic group $\frac{\mathbb{Z}}{4\mathbb{Z}}$ of rotations of the face about its center. Thus by the Proposition:

$$|G| = [G : G_s] \cdot |G_s| = |G * s| \, |G_s| = 6 \cdot 4 = 24.$$

More generally, let S be the faces of the regular solid with n-faces, and let each face have k edges. Let G be the group of all rotations of S. Then by an analogous argument $|G| = nk$. There are only five regular solids: tetrahedron ($n=4, k=3$), cube ($n=6, k=4$), octahedron ($n=8, k=3$), dodecahedron ($n=12, k=5$), icosahedron ($n=20, k=3$).

Definition: Let S be a G-set under $*: G \times S \to S$, let $s_1, s_2 \in S$. If there is some $g \in G$ such that $s_1 = g * s_2$, we say that the action is transitive.

Definition: Let S be a G-set under $*: G \times S \to S$, let $s \in S$. We say that $G * s$ is a one point orbit of S, and s is a fixed point under the action of G, if $G * s = \{s\}$.

We define $F_G(S) := \{ s \in S \mid |G * s| = 1 \}$ the set of fixed points of S under the action of G.

Lemma: Let S be a G-set under $*: G \times S \to S$, let $s \in S$. The following are equivalent:

(i) $s \in F_G(S)$.

(ii) $G_s = G$.

(iii) $G * s = \{s\}$.

In particular, if $\mathcal{O}$ is a system of representatives of the action, then $F_G(S) \subseteq \mathcal{O}$.

Remark: For $\mathcal{O}$ a system of representatives of a G-set S, we denote $\mathcal{O}^* = \mathcal{O} \setminus F_G(S)$.

Hence if $s \in \mathcal{O}^*$ then $[G : G_s] = |G * s| > 1$ so $G_s \leq G$ is a strict subgroup of G.

Theorem: (Orbit Decomposition Theorem) Let S be a G-set under $*: G \times S \to S$, then:

$$S = F_G(S) \vee \bigvee_{s \in \mathcal{O}^*} G * s \quad \text{so if } S \text{ is finite } \quad |S| = |F_G(S)| + \sum_{s \in \mathcal{O}^*} |G * s|.$$

Section 21: Examples of group actions

Conjugation on elements: Let G be a group, $S = G$. Consider the left action $*: G \times G \to G$, $(g, s) \mapsto gsg^{-1}$ called **conjugation** by G. The orbit of an element $a \in G$ is also called the **conjugacy class** of a:

$C(a) := G * a = \{xax^{-1} \mid x \in G\}$. The stabilizer of a is:

$Z_G(a) := G_a = \{x \in G \mid xax^{-1} = a\} = \{x \in G \mid xa = ax\}$, which is also called the **centralizer** of a since it consists of the elements of G commuting with a. The fixed points of this action are:

$F_G(S) = \{a \in S \mid xax^{-1} = a \text{ for all } x \in G\} = \{a \in G \mid xa = ax \text{ for all } x \in G\} = Z(G)$ the **center** of G. Let $\mathcal{C}$ be a system of representatives for the conjugation action of G on itself. Then $\mathcal{C}^* = \mathcal{C} \setminus Z(G)$ and thus:

$$G = Z(G) \vee \bigvee_{a \in \mathcal{C}^*} C(a) \quad \text{so if } G \text{ is finite} \quad |G| = |Z(G)| + \sum_{a \in \mathcal{C}^*} [G : Z_G(a)].$$

This is called the **class equation.**

Recall: A group G with $|G| = p^n$ for some $p, n \in \mathbb{Z}^+$, p prime, is called a ~~p-group~~. In particular, a subgroup of a p-group is either trivial or a p-group by Lagrange's Theorem.

Example: Let $G = D_3 = \{e, r, r^2, f, fr, rf\}$. Now $|G| = 6$, $r^3 = e = f^2$, $frf^{-1} = r^{-1} = r^2$.

Since $fr = r^2 f$ and $rf = fr^2$ then the orbits are:

$C(e) = \{e\}$ with $1 \mid 6$, $C(r) = \{r, r^2\}$ with $2 \mid 6$, $C(f) = \{f, fr, rf\}$ with $3 \mid 6$.

The centralizers are:

$Z_G(e) = G$ with $|C(e)| = 1$,

$Z_G(r) = \{e, r, r^2\}$ with $|C(r)| = 2$,

$Z_G(f) = \{e, f\}$ with $|C(f)| = 3$.

The fixed points are:

$F_G(s) = Z(G) = \{e\}$.

So the class equation states:

$|G| = |Z(G)| + |C(r)| + |C(f)|$, namely $6 = 1 + 2 + 3$. (recall $[G : G_s] = |G * s|$)

Proposition: Let G be a p-group, then $|Z(G)| > 1$. Since $Z(G) \trianglelefteq G$, if $|G| = p^n$ with $n > 1$, then G is not simple.

Proof: Let $a \in \mathcal{C}^*$, then $a \notin Z(G)$, so there is some $g \in G$ with $ga \neq ag$. Thus $Z_G(a)$ is not all G, and since $|G| = [G : Z_G(a)]\,|Z_G(a)|$ we have $p \mid [G : Z_G(a)]$. Now:

$$|G| \equiv |Z(G)| + \sum_{a \in \mathcal{C}^*} [G : Z_G(a)] \mod p, \text{ so } 0 \equiv |Z(G)| \mod p.$$

Since $e \in Z(G)$ we have $|Z(G)| \geq 1$, and since $p \mid |Z(G)|$ we have $|Z(G)| \geq p$.

If G is not abelian then $Z(G) \neq G$ so G is not simple. If G is abelian,

then there is an element $a \in G$ of order p, and since $|G| > p$ then $\langle a \rangle \subsetneq G$. $\square$.

Theorem: Let G be a group of order p^2 with $p \in \mathbb{Z}^+$ prime. Then G is abelian.

Proposition: Let G be a p-group and N a non-trivial normal subgroup of G. Then there is a non-identity element $x \in N$ with $x \in Z(G)$.

Definition: Let H be a subgroup of G, the **normalizer** of H in G is:

$$N_G(H) = \{ x \in G \mid xHx^{-1} = H \}.$$

Proposition: Let H be a subgroup of G, then:

1. $N_G(H)$ is a subgroup of G.
2. $H \trianglelefteq N_G(H)$.
3. If $H \trianglelefteq K$ with $K \leq G$ then $K \subseteq N_G(H)$.
4. $N_G(H)$ is the unique largest subgroup of G containing H as a normal subgroup.

Example: Let R be a ring, $G = GL_n(R)$, $S = M_n(R)$. Then S is a G-set under conjugation: $* : G \times S \longrightarrow S$, $(A, B) \longmapsto ABA^{-1}$. Finding a nice system of representatives for this action is an important question. If R is an algebraically closed field (namely a field R where every non-constant polynomial with coefficients in R has a root in R), such a system of representatives is called the set of Jordan canonical forms. If R is any field, such a

system of representatives is called the set of rational canonical forms. Similar questions can be

asked about the action: $*: G \times S \longrightarrow S$.
$$(A, B) \longmapsto ABA^t$$

Translation: Let G be a group, $S = \mathcal{P}(G)$ the power set of G. Consider the left action

$*: G \times \mathcal{P}(G) \longrightarrow \mathcal{P}(G)$ called translation by G. We can also act by translation on certain
$$(g, T) \longmapsto gT = \{gx \mid x \in T\}$$
subsets of $\mathcal{P}(G)$ such as $T_n = \{A \mid A \subseteq G \text{ with } |A| = n\}$. We can also act by translation on the

cosets G/H determined by some $H \leq G$: $*: G \times G/H \longrightarrow G/H$. The stabilizer of aH in G/H
$$(x, aH) \longmapsto xaH$$
under translation by G is:

$$G_{aH} = \{x \in G \mid xaH = aH\} = \{x \in G \mid a^{-1}xaH = H\} = \{x \in G \mid a^{-1}xa \in H\} = \{x \in G \mid x \in aHa^{-1}\} = aHa^{-1}$$

and if $H \leq G$ then the set of fixed points is empty: $F_G(G/H) = \emptyset$, since if $aH \in F_G(G/H)$ then

$G = G_{aH}$ so $G = aHa^{-1}$, but $|G| > |H| = |aHa^{-1}|$.

Proposition: Let G be a finite group, $H \leq G$. Suppose that H is a p-group and $p \mid [G:H]$. Then

$$p \mid [N_G(H) : H].$$

In fact, cosets arise naturally when considering actions by translation. Let G be a group and $H \leq G$,

consider G as a right H-set via the right H-action of translation: $*: G \times H \longrightarrow G$ and the orbits
$$(g, h) \longmapsto gh$$
$g * H = \{g *^h \mid h \in H\} = \{gh \mid h \in H\} = gH$ give the cosets in G/H. Let G be finite, then the

Orbit Decomposition Theorem gives $|G| = \sum_{g \in \mathcal{O}} |g*H| = \sum_{g \in \mathcal{O}} |gH|$. Since $|gH| = |H|$ for all $g \in G$

then $|G| = |H| \cdot \sum_{g \in \mathcal{O}} 1 = |H| \cdot |\mathcal{O}| = |H| \cdot [G:H]$ by the definition of index of a subgroup. This is

Lagrange's Theorem.

Shift: Understanding this action is the first step toward showing that if G is a finite group

with $|G| = p_1^{n_1} \cdots p_r^{n_r}$, then for each p_i and j_i with $1 \leq i \leq r$ and $1 \leq j_i \leq n_i$ there is $H \leq G$ with

$|H| = p_i^{j_i}$. Let G be a finite group, $p \in \mathbb{Z}^+$ a prime dividing $|G|$. Set:

$$S = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = e\} \subseteq G^p = \underbrace{G \times \cdots \times G}_{p}.$$

Since $(e, \ldots, e) \in S$ then $S \neq \emptyset$, and if $(g_1, \ldots, g_p) \in G$ then $g_p^{-1} = g_1 \cdots g_{p-1}$, or equivalently

$g_p = (g_1 \cdots g_{p-1})^{-1}$. Thus for every ordered choice $g_1, \ldots, g_{p-1}$ of $p-1$ elements of G we have a unique

$g_p \in G$ such that $(g_1, \ldots, g_p) \in S$. Hence $|S| = |G^{p-1}| = |G|^{p-1}$ so $p \mid |S|$.

For $y \in \mathbb{Z}$, we denote by $\tilde{y}$ the smallest positive integer such that $y \equiv \tilde{y} \bmod p$. Now for $x \in \mathbb{Z}$

we have that $\widetilde{1+x}, \ldots, \widetilde{p+x}$ is a cyclic permutation of $1, \ldots, p$. Consider the action of $\frac{\mathbb{Z}}{p\mathbb{Z}}$ on S

by: $* : \frac{\mathbb{Z}}{p\mathbb{Z}} \times S \longrightarrow S$. Note that if $(g_1, \ldots, g_p) \in S$ then any cyclic permutation

$(\bar{x}, (g_1, \ldots, g_p)) \mapsto (g_{\widetilde{1+x}}, \ldots, g_{\widetilde{p+x}})$

$(g_{i+1}, \ldots, g_p, g_1, \ldots, g_i) \in S$ for $1 \leq i \leq p$ since:

$$g_{i+1} \cdots g_p g_1 \cdots g_i = (g_i^{-1} \cdots g_1^{-1})(g_1 \cdots g_p)(g_1 \cdots g_i) = (g_1 \cdots g_i)^{-1} e (g_1 \cdots g_i) = e.$$

Theorem: (Cauchy's Theorem) Let $p \in \mathbb{Z}^+$ be a prime dividing the order of G a finite group. Then

G has an element of order p.

Proof: Apply the Orbit Decomposition Theorem to the shift action:

$$|S| = |F_{\frac{\mathbb{Z}}{p\mathbb{Z}}}(S)| + \sum_{x \in \mathcal{O}^*} \left[\frac{\mathbb{Z}}{p\mathbb{Z}} : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)_x\right].$$

For $x \in \mathcal{O}^*$ we have $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)_x \leq \frac{\mathbb{Z}}{p\mathbb{Z}}$ and $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)_x \neq \frac{\mathbb{Z}}{p\mathbb{Z}}$, since otherwise $x \in F_{\frac{\mathbb{Z}}{p\mathbb{Z}}}(S)$.

Now $\frac{\mathbb{Z}}{p\mathbb{Z}}$ only has $\{0\}$ and $\frac{\mathbb{Z}}{p\mathbb{Z}}$ as subgroups, so $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)_x = \{0\}$ and $\left[\frac{\mathbb{Z}}{p\mathbb{Z}} : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)_x\right] = p$.

Hence: $0 \equiv |S| \equiv |F_{\frac{\mathbb{Z}}{p\mathbb{Z}}}(S)| \mod p$. Since $(e,\dots,e) \in F_{\frac{\mathbb{Z}}{p\mathbb{Z}}}(S)$ we have

$|F_{\frac{\mathbb{Z}}{p\mathbb{Z}}}(S)| \geq 1$, so we must have $|F_{\frac{\mathbb{Z}}{p\mathbb{Z}}}(S)| \geq p$. Then there is $(g_1,\dots,g_p) \in F_{\frac{\mathbb{Z}}{p\mathbb{Z}}}(S)$

with $(g_1,\dots,g_p) \neq (e,\dots,e)$. Since it is fixed by the action:

$$(g_1,\dots,g_p) = (g_2,\dots,g_p,g_1) = \cdots = (g_{i+1},\dots,g_p,g_1,\dots,g_i) = \cdots = (g_p,g_1,\dots,g_{p-1})$$

and thus $g_1 = g_2 = \cdots = g_i = \cdots = g_p$, so renaming $g_i = g \in G$ we have $g \neq e$ and $(g,\dots,g) \in S$,

namely $g^p = g \cdots g = e$, so g has order p. $\square$.

Section 22: Sylow Theorems

Definition: Let G be a finite group, $|G| = p^r m$ with $\gcd(p,m) = 1$ and p prime, $p,m,r \in \mathbb{Z}^+$. A subgroup H of G is called a Sylow p-subgroup of G if $|H| = p^r$. We denote:

$$Syl_p(G) = \{H \mid H \text{ is a Sylow } p\text{-subgroup}\}.$$

Theorem: (First Sylow Theorem) Let $p \in \mathbb{Z}^+$ be a prime, G a finite group with $p \mid |G|$. Then

$Syl_p(G)$ is not empty, namely there exists a Sylow p-subgroup.

Theorem: (Generalized First Sylow Theorem) Let $p \in \mathbb{Z}^+$ be a prime, $s \in \mathbb{Z}^+$, and G a finite group with $p^s \mid |G|$. Then there exists a subgroup of G of order p^s.

Proof: We will use induction on the order of G. If $|G| \leq p$, then G is the subgroup we want.

We make the following induction hypothesis: if T is any finite group with $|T| < |G|$ and $p^r \mid |T|$, then T contains a subgroup of order p^r. We now prove the induction step. Let $H < G$ a subgroup with $p \nmid [G:H]$. Since $|G| = [G:H]\,|H|$ and $p^s \mid |G|$, then $p^s \mid |H|$, and since $|H| < |G|$, by the induction hypothesis H contains a subgroup of order p^s, so G contains a subgroup of order p^s. Hence without loss of generality we may assume that whenever $H < G$ is a subgroup then $p \mid [G:H]$. Applying now the class equation we have:

$$|G| = |Z(G)| + \sum_{a \in \mathcal{C}^*} [G : Z_G(a)]$$

and for each $a \in \mathcal{C}^* = \mathcal{C} \setminus Z(G)$ we have $\{e\} \neq Z_G(a) < G$, so $p \mid [G : Z_G(a)]$ and thus:

$0 \equiv |G| \equiv |Z(G)| \mod p$, so $p \mid |Z(G)|$. Then by Cauchy's Theorem there exists an element $a \in Z(G)$ of order p. Let $H = \langle a \rangle$, a subgroup of G of order p. Since $a \in Z(G)$ we have $xa^i x^{-1} = a^i$ for all $x \in G$ and $i \in \mathbb{Z}$, whence $H \trianglelefteq G$. Now $\frac{G}{H}$ is a group of order

$\left|\frac{G}{H}\right| = [G:H] = \frac{|G|}{|H|} = \frac{|G|}{p}$, so $p^{s-1} \mid \left|\frac{G}{H}\right|$ and

$|H| \cdot [G:H] = \frac{|G|}{|H|} = \frac{|G|}{p} < |G|$. Moreover since $p^s \mid |G|$ we have $p^{s-1} \mid \frac{|G|}{|H|}$, so by the induction hypothesis there is a subgroup $T < \frac{G}{H}$ of order p^{s-1}. Consider the canonical epimorphism $^- : G \longrightarrow \frac{G}{H}$, by the Correspondence Principle there is a subgroup $\tilde{T}$ of G containing H and satisfying $T = \frac{\tilde{T}}{H}$. Hence $|\tilde{T}| = |T| \cdot |H| = p^s$, as desired. □.

<u>Lemma:</u> Let H, K be subgroups of a finite group G. Then $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

<u>Lemma:</u> Let G be a finite group, P a Sylow p-subgroup, and H a subgroup of G that is also a p-group. If $H < N_G(P)$ then H is a subgroup of P, and if H is also a Sylow p-subgroup then $H = P$.

<u>Proof:</u> Since $P \trianglelefteq N_G(P)$ and $H < N_G(P)$, by the Second Isomorphism Theorem HP is a subgroup of $N_G(P)$ with $P \trianglelefteq HP$ and $(H \cap P) \trianglelefteq H$, and moreover $\frac{HP}{P} \cong \frac{H}{H \cap P}$. Hence by the previous Lemma $|HP| = \frac{|P||H|}{|H \cap P|}$. Since P and H are both p-groups, and $H \cap P < H$ is also a p-group, then HP is a p-subgroup with $P \subseteq HP \subseteq G$. Thus $|P| = |HP|$ so $P = HP$, so $H < P$. If we had $|H| = |P|$ then $H < P$ implies $H = P$. □.

<u>Notation:</u> For a group G and the set $S = \mathcal{P}(G)$, consider the action $* : G \times S \longrightarrow S$. We set $(x, A) \mapsto xAx^{-1}$ $C(A) = G * A = \{xAx^{-1} \mid x \in G\}$, now for $H < G$ we have that the action restricts to an action by conjugation $*|_{G \times C(H)} : G \times C(H) \longrightarrow C(H)$, making $C(H)$ into a G-set.

We can translate the Lemma above to the language of group actions.

Lemma: Let G be a finite group, P a Sylow p-subgroup, and $H < G$ a p-group. Then:

1. $C(P)$ consists of Sylow p-subgroups of G.

2. The conjugacy class $C(P)$ is an H-set by conjugation.

3. If T is a fixed point under the H-action, namely:

   $T \in F_H(C(P)) = \{ W \in C(P) \mid xWx^{-1} = W \text{ for all } x \in H \}$, then $H \subseteq T$.

4. If H is a Sylow p-subgroup then under the H-action, H is the only possible fixed point,

   namely $F_H(C(P)) \subseteq \{H\}$.

Remark: Let G be a finite group, P a Sylow p-subgroup, and $H < G$ a p-group. Then the isotropy subgroup of P is $H_P = N_G(P) \cap H$. Since P is a Sylow p-subgroup of $N_G(P)$, the proof of the Lemma above by restricting the action to H_P we have $N_G(P) \cap H \subseteq P$.

Theorem: (Second Sylow Theorem) Let G be a finite group, $p \in \mathbb{Z}^+$ a prime dividing $|G|$.

Then all Sylow p-subgroups are conjugate, namely if $P \in Syl_p(G)$ then $C(P) = Syl_p(G)$.

Theorem: (Third Sylow Theorem) Let G be a finite group, $p \in \mathbb{Z}^+$ a prime dividing $|G|$.

Let P be a Sylow p-subgroup of G, then the following are true:

(i) $|Syl_p(G)| = [G : N_G(P)]$.

(ii) $|\mathrm{Syl}_p(G)|$ divides $|G|$.

(iii) $|\mathrm{Syl}_p(G)| \equiv 1 \bmod p$.

(iv) $|\mathrm{Syl}_p(G)|$ divides $[G:P]$, namely if $|G| = p^n m$ with $p \nmid m$, then $|\mathrm{Syl}_p(G)|$ divides m.

Theorem: (Fourth Sylow Theorem) Let G be a finite group, $p \in \mathbb{Z}^+$ a prime dividing $|G|$.

Let $H < G$ be a p-group. Then H lies in some Sylow p-subgroup of G.

Proof: (of the Second, Third, and Fourth Sylow Theorems) Let H be a subgroup of G that is a p-group and P a Sylow p-subgroup of G. By the Lemma above, $C(P) \subseteq \mathrm{Syl}_p(G)$ is an H-set under conjugation. By the Orbit Decomposition Theorem we have:

$$|C(P)| = |F_H(C(P))| + \sum_{T \in \mathcal{O}^*} [H : H_T].$$

If $T \in \mathcal{O}^*$ then $H_T \subsetneq H$ so p divides $[H : H_T]$, so $|C(P)| \equiv |F_H(C(P))| \bmod p$.

If $H = P$, by the Lemma above we have $F_P(C(P)) \subseteq \{P\}$. Since $xPx^{-1} = P$ for all $x \in P$ we have $F_P(C(P)) = \{P\}$. Now using the congruence above: $|C(P)| \equiv |F_P(C(P))| \equiv 1 \bmod p$.

If H is a Sylow p-subgroup of G, not necessarily P, then:

$$|F_H(C(P))| \equiv |C(P)| \equiv |F_P(C(P))| \equiv 1 \bmod p.$$

Hence $F_H(C(P))$ is not empty, so $F_H(C(P)) = \{H\}$ by the Lemma above. In particular $H \in F_H(C(P)) \subseteq C(P)$. Since H is any Sylow p-subgroup, then $\mathrm{Syl}_p(G) \subseteq C(P)$, whence

$\mathrm{Syl}_p(G) = C(P)$, proving the Second Sylow Theorem. Hence: $|\mathrm{Syl}_p(G)| \equiv |C(P)| \equiv 1 \bmod p$,

and $|\mathrm{Syl}_p(G)| = |C(P)| = [G : N_G(P)]$, and $|G| = [G : N_G(P)]\,|N_G(P)| = |\mathrm{Syl}_p(G)| \cdot |N_G(P)|$

so $|\mathrm{Syl}_p(G)|$ divides $|G|$. Moreover since $P \subseteq N_G(P)$ we have:

$[G : P] = [G : N_G(P)][N_G(P) : P] = |\mathrm{Syl}_p(G)| \cdot [N_G(P) : P]$ so $|\mathrm{Syl}_p(G)|$ divides $[G : P]$,

proving the Third Sylow Theorem.

If H is a p-subgroup of G, <u>not</u> necessarily a Sylow p-subgroup, we still have

$$|F_H(C(P))| \equiv |C(P)| \equiv |F_P(C(P))| \equiv 1 \bmod p.$$

Thus there exists a $T \in F_H(C(P)) \subseteq C(P) = \mathrm{Syl}_p(G)$, and by the Lemma above $H \subseteq T$.

Hence H is contained in a Sylow p-subgroup, proving the Fourth Sylow Theorem. □.

<u>Corollary:</u> Let G be a finite group, $p \in \mathbb{Z}^+$ prime dividing $|G|$, and P a Sylow p-subgroup. Then

$N_G(P) = N_G(N_G(P))$.

<u>Examples:</u> Let G be a finite group, $p \in \mathbb{Z}^+$ prime dividing $|G|$. We denote by P_p an arbitrary

Sylow p-subgroup of G, and we denote by n_p the number of Sylow p-subgroups. By the Third

Sylow Theorem there exists an integer k, which depends on p, such that $n_p = 1 + pk$. By the

Second Sylow Theorem, P_p is normal if and only if $k = 0$.

1. Let $|G|=15$, then $n_3=1$, $n_5=1$, $|P_3|=3$, $|P_5|=5$, so $P_3=\frac{\mathbb{Z}}{3\mathbb{Z}}$ and $P_5=\frac{\mathbb{Z}}{5\mathbb{Z}}$. Then

$G=P_3\cdot P_5=\frac{\mathbb{Z}}{15\mathbb{Z}}$, so cyclic.

Let $|G|=45$, then $n_3=1$, $n_5=1$, $|P_3|=9$, $|P_5|=5$, so $P_3\in\{\frac{\mathbb{Z}}{3\mathbb{Z}}\times\frac{\mathbb{Z}}{3\mathbb{Z}},\frac{\mathbb{Z}}{9\mathbb{Z}}\}$ and

$P_5=\frac{\mathbb{Z}}{5\mathbb{Z}}$. Then $G=P_3\cdot P_5\in\{\frac{\mathbb{Z}}{15\mathbb{Z}}\times\frac{\mathbb{Z}}{3\mathbb{Z}},\frac{\mathbb{Z}}{45\mathbb{Z}}\}$, so abelian.

2. Let $|G|=p^r\cdot q$ for $p,q,r\in\mathbb{Z}^+$, p and q prime, $p>q$. Then $n_p=1$ so P_p is normal.

3. Let $|G|=315=3^2\cdot5\cdot7$, then G is <u>not</u> simple. Suppose for contradiction that G is simple,

then it has <u>no</u> normal subgroups, so $n_3>1$ and $n_5>1$. Moreover $n_3=1+3k=[G:N_G(P_3)]$

divides $5\cdot7$ and $n_5=1+5k=[G:N_G(P_5)]$ divides $3^2\cdot7$. Thus $n_3=7=[G:N_G(P_3)]$ and

$n_5=21=[G:N_G(P_5)]$. Thus by Lagrange's Theorem:

$|N_G(P_3)|=\frac{|G|}{[G:N_G(P_3)]}=45$ and $|N_G(P_5)|=\frac{|G|}{[G:N_G(P_5)]}=15$. We have seen that both must

be abelian. If $T\in Syl_5(N_G(P_3))$ then $|T|=5$ and $T<N_G(P_3)<G$, so $T\in Syl_5(G)$ and thus

$|N_G(T)|=15$. Also since $N_G(P_3)$ is abelian, we have $T\trianglelefteq N_G(P_3)$. Thus $N_G(P_3)\leq N_G(T)$, so

by Lagrange's Theorem: $15=|N_G(T)|=[N_G(T):N_G(P_3)]\cdot|N_G(P_3)|=[N_G(T):N_G(P_3)]\cdot45$,

a contradiction.

4. Let $|G|=525=3\cdot5^2\cdot7$, then G is <u>not</u> simple. Suppose for contradiction that G is simple,

then it has <u>no</u> normal subgroups, so $n_5>1$. Let P and Q be distinct Sylow 5-subgroups, set

$I = P \cap Q$. Then $|I| \in \{1, 5\}$, and $|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = \frac{|P| \cdot |Q|}{|I|}$. If $|I| = 1$ then $|PQ| = 5^4 > |G|$, a contradiction. If $|I| = 5$ then $|PQ| = 5^3$. Since $|P| = 5^2 = |Q|$ and groups of order p^2 are abelian, P and Q are abelian, so $I \trianglelefteq P$ and $I \trianglelefteq Q$, so $P \subseteq N_G(I)$ and $Q \subseteq N_G(I)$. Thus $PQ \subseteq N_G(I)$ hence $|N_G(I)| \geq |PQ| = 5^3$. Since by Lagrange's Theorem $|N_G(I)|$ divides $|G|$, we have $|N_G(I)| \in \{3 \cdot 5^2 \cdot 7, 5^2 \cdot 7\}$. If $|N_G(I)| = 3 \cdot 5^2 \cdot 7$ then $N_G(I) = G$ and $I \trianglelefteq G$, contradicting that G is simple. If $|N_G(I)| = 5^2 \cdot 7$ then by Lagrange's Theorem $[G : N_G(I)] = \frac{|G|}{|N_G(I)|} = 3$, and since 3 is the smallest prime dividing $|G|$, we have $N_G(I) \trianglelefteq G$, contradicting that G is simple.

5. Let $|G| = 945 = 3^3 \cdot 5 \cdot 7$, then G is <u>not</u> simple. Suppose for contradiction that G is simple, then it has <u>no</u> normal subgroups, so $n_3 > 1$. Moreover $n_3 = 1 + 3k = [G : N_G(P_3)]$ divides $5 \cdot 7$ so we have $n_3 = 7 = [G : N_G(P_3)]$. Since $|G|$ does <u>not</u> divide $7! = [G : N_G(P_3)]!$, then $N_G(P_3)$ contains a nontrivial normal subgroup of G.

<u>Recall:</u> Let G be a finite group, $H < G$ a subgroup with $|G|$ <u>not</u> dividing $[G : H]!$, then there is a non-trivial $N \trianglelefteq G$ such that $N \subseteq H$.

6. Let $|G| = p \cdot m$ with $p, m \in \mathbb{Z}^+$, p a prime <u>not</u> dividing m. Then G contains $n_p(p-1)$ distinct elements of order p, so $|G| \geq n_p(p-1) + 1$ once we include the identity.

Let $|G| = p \cdot q \cdot m$ with $p, q, m \in \mathbb{Z}^+$, p and q distinct primes not dividing m. Then G contains $n_p(p-1)$ distinct elements of order p and $n_q(q-1)$ distinct elements of order q, so $|G| \geq n_p(p-1) + n_q(q-1) + 1$. Note that if $p = q$ this is not true because two distinct Sylow p-subgroups can intersect non-trivially, and it is hard to count the number of elements in the union of all the Sylow p-subgroups.

Theorem: Let G be a finite group, $|G| = p^s q$ with $p, q, s \in \mathbb{Z}^+$, p and q prime. Then G is not simple.

Definition: Let G be a group. We say that a subgroup M of G is maximal if $M \subsetneq G$ and if $M \subsetneq H \subseteq G$ for any other subgroup H of G, then $H = G$. We say that G is an internal direct product of the normal subgroups $N_1, \ldots, N_r$ whenever $G = N_1 \cdots N_r$ and $N_i \cap N_1 \cdots N_{i-1} N_{i+1} \cdots N_r = \{e\}$ for all $i = 1, \ldots, r$.

Theorem: Let G be a finite group. Then the following are equivalent:

(i) Every Sylow subgroup of G is normal in G.

(ii) G is isomorphic to an internal direct product of its Sylow subgroups.

(iii) Every maximal subgroup of G is normal in G.

Definition: A finite group G is called nilpotent if all of its Sylow subgroups are normal.

Corollary: Let G be a finite nilpotent group. Then G is solvable.

Section 24: The symmetric and alternating groups.

Recall: The symmetric group on n letters, denoted by S_n, is the group of all permutations of the set $\{1,\dots,n\}$.

Notation: For $\sigma \in S_n$ we write $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ with the domain of σ in the top row, and the corresponding values of the domain in the bottom row.

Example: For $\sigma, \tau \in S_4$ with $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ then $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ and $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$.

Definition: A permutation $\alpha \in S_n$ is called a cycle of length r, $r \leq n$, if there exist distinct $a_1,\dots,a_r \in \{1,\dots,n\}$ satisfying:

(1) $\alpha(a_i) = a_{i+1}$ for $i = 1,\dots,r-1$,

(2) $\alpha(a_r) = a_1$,

(3) $\alpha(a) = a$ for all $a \in \{1,\dots,n\} \setminus \{a_1,\dots,a_n\}$.

We denote such an r-cycle by $(a_1,\dots,a_r)$. We say that α is nontrivial whenever $r > 1$.

We say that two cycles $\alpha = (a_1,\dots,a_r)$ and $\beta = (b_1,\dots,b_s)$ are disjoint when $\{a_1,\dots,a_r\} \cap \{b_1,\dots,b_s\} = \emptyset$.

Example:

1. $(a_1) = 1_{S_n} = 1$ is the identity on $\{1, \dots, n\}$.

2. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (23)$.

3. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (34)(12) = (12)(34)$.

4. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1342)$

Proposition: Let $\alpha = (a_1, \dots, a_r) \in S_n$ with $n \geq 2$. Then:

(1) $\alpha = (a_i \cdots a_r a_1 \cdots a_{i-1})$ for all $1 \leq i \leq r$.

(2) α has order r.

(3) $\alpha^{-1} = (a_r, \dots, a_1)$

(4) If $\sigma \in S_n$ we have $\sigma \alpha \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_r))$.

Lemma: Let $\alpha, \beta \in S_n$ be disjoint cycles, then $\alpha\beta = \beta\alpha$.

Remark: We can decompose any permutation $\gamma \in S_n$ into a multiplication of disjoint cycles.

To see this, let $S = \{1, \dots, n\}$ and $\gamma \in S_n$ with $n > 1$. Let $\Gamma = \langle \gamma \rangle < S_n$. Now S is a Γ-set

via the evaluation: $* : \Gamma \times S \longrightarrow S$. The orbit of $a \in S$ is $\Gamma * a = \{\gamma^j(a) \mid j \in \mathbb{Z}\}$.
$(\gamma^j, a) \mapsto \gamma^j(a)$

Since $|\Gamma| \leq |S_n| = n!$, there exists a least positive integer $m = m(a)$ depending on a satisfying

$\gamma^m(a) = a$. Thus the orbit of $a \in S$ is $\Gamma * a = \{a, \gamma(a), \dots, \gamma^{m-1}(a)\} \subseteq S$. To this orbit we

associate the n-cycle $\gamma_a := (a, \gamma(a), \dots, \gamma^{m-1}(a)) \in S_n$. Let $\mathcal{O}$ be a system of representatives for the equivalence relation $\sim_\Gamma$ given by the Γ-action on S, let $b \in \{1, \dots, n\}$. Then there is an $a \in \mathcal{O}$ with $b \in \Gamma * a$, namely $\gamma(b) = \gamma_a(b)$, so since S is the disjoint union of the orbits, we have $S = \bigvee_{a \in \mathcal{O}} \Gamma * a$. Since disjoint cycles commute, we have $\gamma = \prod_{a \in \mathcal{O}} \gamma_a$ namely a product of disjoint cycles that is unique up to the order in which we multiply them.

Definition: Let $\gamma \in S_n$, we call $\prod_{a \in \mathcal{O}} \gamma_a$ the full cycle decomposition of γ.

Example: We have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix} = (135)(2)(4)(6)$ and $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 4 & 6 \end{pmatrix} = (12)(354)(6)$.

Remark: Note that a 1-cycle, say (a) for some $a \in \{1, \dots, n\} = S$, is the identity $1_S : S \to S$.

For $\gamma \in S_n$, the fixed points of the Γ-action, that is the elements $a \in S$ with $\gamma(a) = a$, are precisely the elements of S appearing in the 1-cycles of the full cycle decomposition of γ. By convention, we usually do not write the 1-cycles in the cycle decomposition of γ.

Definition: Let $\gamma \in S_n$, by removing the 1-cycles from the full cycle decomposition of γ we obtain the cycle decomposition of γ.

Definition: A permutation $\tau \in S_n$ is called a transposition if τ is a 2-cycle.

Proposition: Let $n \in \mathbb{Z}^+$, $n > 1$, then every element in S_n is a product of the transpositions $(1i)$ for $i = 2, \dots, n$. In particular if $\sigma = (a_1 \dots a_r)$ for $a_1, \dots, a_r \in \{1, \dots, n\}$ distinct,

then $\sigma = (a_{r-1}\ a_r)(a_{r-2}\ a_r)\cdots(a_2\ a_r)(a_1 a_r) = (a_1 a_2)(a_2 a_3)\cdots(a_{r-2}\ a_{r-1})(a_{r-1}\ a_r)$.

Remark: The decomposition of a permutation into a product of transpositions is not unique.

Recall that we have group homomorphisms: $S_n \xrightarrow{\Theta} \mathrm{Perm}_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\}$ where

$\sigma \longmapsto [T_\sigma]_{\mathcal{E}_n} \longmapsto \det([T_\sigma]_{\mathcal{E}_n})$

$\mathcal{E}_n$ is the standard basis for $\mathbb{R}^n$, and $\mathrm{Perm}_n(\mathbb{R})$ are the permutation matrices. We define $A_n := \ker(\det \circ \Theta) \trianglelefteq S_n$, we have $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ and $[S_n : A_n] = 2$.

For a transposition $\tau \in S_n$, since τ permutes two columns of the identity matrix, we have $\det([T_\tau]_{\mathcal{E}_n}) = -1$. Hence if $\sigma \in S_n$ is a product of r transpositions and a product of s transpositions for some $r, s \in \mathbb{Z}^+$, then $(-1)^r = (-1)^s$ so $r \equiv s \bmod 2$. Thus by the Proposition above, for σ an r-cycle, we have $\sigma \in A_n$ for r odd and $\sigma \in S_n \setminus A_n$ for r even. We conclude:

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is a product of an even number of transpositions}\},$$

$$S_n \setminus A_n = \{\sigma \in S_n \mid \sigma \text{ is a product of an odd number of transpositions}\}.$$

Definition: An element in A_n is called an even permutation. An element in $S_n \setminus A_n$ is called an odd permutation.

Definition: Let $\sigma \in S_n$, suppose that $\sigma = \sigma_1 \cdots \sigma_r$ is the full cycle decomposition of σ. We

define the signum of σ as: $\operatorname{sgn}(\sigma) = (-1)^{n-r}$.

Remark: Since the full cycle decomposition of σ is unique, this defines a function

$$\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}.$$

Proposition: The function $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$ is a group homomorphism.

Corollary: The group homomorphisms $\det \circ \theta: S_n \longrightarrow \{\pm 1\}$ and $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$ coincide.

Corollary: The alternating group A_n is equal to the kernel of the signum $\ker(\operatorname{sgn})$.

Proposition: Let $n \in \mathbb{Z}^+$, $n \geq 3$. Then the alternating group A_n is generated by the 3-cycles $(12i)$ for

$i = 3, \ldots, n$.

Lemma: Let K be a normal subgroup of A_n. If K contains a 3-cycle, then $K = A_n$.

Theorem: (Abel's Theorem) Let $n \in \mathbb{Z}^+$, $n \neq 4$. Then the alternating group A_n is simple.

Remark: Recall that a subgroup of a solvable group is solvable, and that a non-abelian simple group cannot be solvable, so a group containing a non-abelian simple group cannot be solvable.

Hence S_n is not solvable for $n \geq 5$.

Proposition: Let $n \in \mathbb{Z}^+$, $n \geq 5$. Then A_n is the only subgroup of S_n of index two.

Theorem: The alternating group A_5 is, up to isomorphism, the only simple group of order 60.

Proposition: Let $n \in \mathbb{Z}^+$, $n \geq 5$, and H a normal subgroup of S_n. Then $H = \{1\}$ or $H = A_n$ or $H = S_n$.

Proposition: Let G be a finite group of order $2n$, n odd. Then G contains a normal subgroup of index two. In particular, if $n>1$ then G is <u>not</u> simple.

Theorem: Let G be a finite group of order $2^r m$ with m odd. If G contains a cyclic Sylow 2-subgroup, then there exists a normal subgroup of G of index 2^r. In particular, if $m>1$ or $r>1$, then G is <u>not</u> simple.