MTH 301: Group Theory

Semester 1, 2018-2019

Dr. Prahlad Vaidyanathan

Contents

Symmetries of a Square

[Gallian, §2.1]

0.1. Definition of a symmetry of a square with vertices labelled $\{1, 2, 3, 4\}$: A transformation that maps the object to itself.

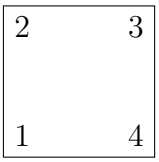
0.2. List of all such symmetries. Proof that there are exactly 8 such symmetries.

Proof. We list them down as

$$\{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

where

- R_θ is a rotation by θ degrees.
- H is the flip about the horizontal axis.
- V, D, D' are flips about the vertical axis, the leading diagonal, and the off diagonal axes respectively.



Each of these are distinct symmetries. There are 8 total because there are 4 possible spots for 1, and two possible spots for 2. Once those are fixed, 3 and 4 are automatically fixed as as well. □

0.3. Definition: D_4 is the set of all symmetries of a square. We can compose two elements of D_4 to obtain a third. We denote this by

$$\sigma \circ \tau$$

0.4. Properties of D_4 :

(i) Closure: Given $\sigma, \tau \in D_4, \sigma \circ \tau \in D_4$

(ii) Existence of Identity: $\delta = R_0$ has the property that $\sigma \circ \delta = \delta \circ \sigma = \sigma$ for all $\sigma \in D_4$.

(iii) Existence of Inverses: Given $\sigma \in D_4$, there is a $\sigma' \in D_4$ such that $\sigma \circ \sigma' = \delta = \sigma' \circ \sigma$.

I. Groups

1. Definition and Basic Properties

Definition 1.1. Let G be a set.

1.1. A binary operation on G is a function

$$f : G \times G \to G$$

1.2. A group is a set G, together with a binary operation $f : G \times G \to G$ such that the following axioms hold:

(i) Associativity: For any $a, b, c \in G$,

$$f(f(a, b), c) = f(a, f(b, c))$$

(ii) Identity: $\exists e \in G$ such that

$$f(a, e) = f(e, a) = a \quad \forall a \in G$$

(iii) Inverse: For any $a \in G, \exists a' \in G$ such that

$$f(a, a') = f(a', a) = e$$

Notation: Given a group (G, f) as above, we write

$$ab := f(a, b)$$

Hence the first axiom reads: $(ab)c = a(bc)$ for all $a, b, c \in G$. Note that the operation may not be multiplication in the usual sense.

Example 1.2. 1.1. $(\mathbb{Z}, +)$ is a group. $(\mathbb{Z}, -)$ is not a group. $(\mathbb{N}, +)$ is not a group.

1.2. $(\mathbb{Q}, \cdot)$ is not a group, but $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \cdot)$ is. Similarly, $\mathbb{R}^*$ and $\mathbb{C}^*$ are groups.

1.3. $(\mathbb{R}^n, +), (\mathbb{C}^n, +)$ are groups. More generally, any vector space is a group under addition.

1.4. The Dihedral groups D_n = the group of symmetries of a regular n-gon

Proposition 1.3. *Let $(G, *)$ be a group*

1.1. Uniqueness of Identity: Suppose $e_1, e_2 \in G$ are such that $ae_1 = ae_2 = a = e_1a = e_2a$, then $e_1 = e_2$

1.2. Cancellation laws: Suppose $a, b, c \in G$ such that $ab = ac$, then $b = c$. Similarly, if $ba = ca$, then $b = c$

1.3. Uniqueness of inverses: Given $a \in G$, suppose $b_1, b_2 \in G$ such that $ab_1 = ab_2 = e = b_1 a = b_2 a$, then $b_1 = b_2$

Proof. 1.1. By hypothesis, $e_1 = e_1 e_2 = e_2$.

1.2. If $ab = ac$, then choose $a' \in G$ such that $aa' = a'a = e$, so

$$a'(ab) = a'(ac)$$

By associativity,

$$(a'a)b = (a'a)c$$

But $a'a = e$ and $eb = b$. Similarly on the RHS, so $b = c$. The right cancellation law is similar.

1.3. Suppose $ab_1 = ab_2$, then by left cancellation, $b_1 = b_2$.

□

Definition 1.4. Let G be a group, $a \in G$

1.1. For $n \in \mathbb{Z}$, define

$$a^n := \underbrace{a \cdot a \cdot a \ldots a}_{n \text{ times}}$$

Note that by associativity, we may write this expression without any parentheses. Furthermore,

$$a^n a^m = a^{n+m}, \text{ and } (a^n)^m = a^{nm}$$

1.2. A group G is said to be cyclic if $\exists a \in G$ such that, for any $b \in G, \exists n \in \mathbb{Z}$ with $b = a^n$. Such an element a is called a generator of G (note that it may not be unique).

(End of Day 1)

Example 1.5. 1.1. $(\mathbb{Z}, +)$ is cyclic with generators 1 or -1

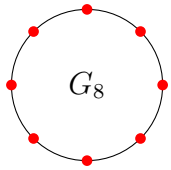
1.2. $(\mathbb{Z} \times \mathbb{Z}, +)$ is not cyclic

Proof. Suppose $a = (a_1, a_2)$ generated $\mathbb{Z} \times \mathbb{Z}$. Then $\exists n, m \in \mathbb{Z}$ such that

$$(1, 0) = n(a_1, a_2) \text{ and } (0, 1) = m(a_1, a_2)$$

But $n(a_1, a_2) = (na_1, na_2)$, so this would imply that $na_2 = 0$, whence $n = 0$ or $a_2 = 0$. But if $n = 0$ this equation cannot hold, so $a_2 = 0$. Similarly, from the other equation $a_1 = 0$, so $(a_1, a_2) = (0, 0)$. But this contradicts the first equation. □

1.3. For $k \in \mathbb{N}$, define $G_k = \{\xi \in \mathbb{C} : \xi^k = 1\}$. G_k is cyclic with generator $\xi_0 = e^{2\pi i/k}$



Note: Every cyclic group is either the same as $\mathbb{Z}$ or the same as G_k for some k (Proof later). Can represent G_k as a *cycle* in $\mathbb{C}$. Hence the term cyclic.

Definition 1.6. A group G is said to be abelian if

$$a * b = b * a$$

for all $a, b \in G$

Example 1.7. 1.1. $(\mathbb{Z}, +)$ is abelian. In general, any cyclic group is abelian.

1.2. $(\mathbb{Z} \times \mathbb{Z}, +)$ is abelian, but not cyclic.

1.3. Consider the water molecule: It has one rotational symmetry R_{180}, and two reflection symmetries V about the XZ-plane and H about the XY-plane. We write

$$V_4 := \{e, R_{180}, V, H\}$$

for the symmetries of this molecule. Note that

$$R_{180}^2 = V^2 = H^2 = e$$

Thus, this group is not cyclic. It is abelian, however (Check!).

1.4. D_4 is non-abelian (and hence not cyclic)

Proof. Check that

$$HR_{90} = D \text{ but } R_{90}H = D'$$

so it is non-abelian. □

1.5. For $n \in \mathbb{N}$, the general linear group is defined as

$$GL_n(\mathbb{R}) := \{A = (a_{i,j})_{n \times n} : \det(A) \neq 0\}$$

This is the collection of all invertible matrices, which is a group under multiplication. It is non-abelian and infinite.

Definition 1.8. The order of a group G is $|G|$, the cardinality of the underlying set.

Table of groups discussed thus far (Note that *Cyclic* $\Rightarrow$ *Abelian*)

Group	Finite	Cyclic	Abelian
G_k	Y	Y	Y
V_4	Y	N	Y
D_n	Y	N	N
$\mathbb{Z}$	N	Y	Y
$\mathbb{Z} \times \mathbb{Z}$	N	N	Y
$GL_n(\mathbb{R})$	N	N	N

2. The Integers

(See [Gallian, §0.1], and [Herstein, §1.3])

Axiom 2.1 (Well-Ordering Principle)*:* Every non-empty subset of positive integers contains a smallest member.

Definition 2.2. 2.1. For $a, b \in \mathbb{Z}, b \neq 0$, we say that b divides a (In symbols $b \mid a$) if $\exists q \in \mathbb{Z}$ such that $a = bq$.

Note: If $a \mid b$ and $b \mid a$, then $a = \pm b$.

2.2. A number $p \in \mathbb{Z}$ is said to be prime if, whenever $a \mid p$, then either $a = \pm 1$ or $a = \pm p$.

Theorem 2.3 (Euclidean Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then $\exists$ unique $q, r \in \mathbb{Z}$ with the property that*

$$a = bq + r \text{ and } 0 \leq r < b$$

Proof. We prove existence and uniqueness separately.

- Existence: Define

  $$S := \{a - bk : k \in \mathbb{Z}, \text{ and } a - bk \geq 0\}$$

  Note that S is non-empty because:

  - If $a \geq 0$, then $a - b \cdot 0 \in S$
  - If $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$ because $b > 0$

  If $0 \in S$, then $b \mid a$, so we may take $q = a/b$ and $r = 0$.

  Suppose $0 \notin S$, then S has a smallest member, say

  $$r = a - bq$$

  Then $a = bq + r$, so it remains to show that $0 \leq r < b$. We know that $r \geq 0$ by construction, so suppose $r \geq b$, then

  $$r - b = a - b(q + 1) \in S$$

  Since $b > 0$, this contradicts the fact that r is the smallest member in S.

- Uniqueness: Suppose r', q' are such that

$$a = bq' + r' \text{ and } 0 \leq r' < b$$

Then suppose $r' \geq r$ without loss of generality, so

$$r' - r + b(q' - q) = 0$$

Hence, $b \mid (r' - r)$, but $r' - r \leq r' < b$, so this is impossible unless $r' - r = 0$. Hence, $q' - q = 0$ because $b \neq 0$.

□

Theorem 2.4. *Given two non-zero integers $a, b \in \mathbb{Z}$, there exists $d \in \mathbb{Z}_+$ such that*

2.1. $d \mid a$ and $d \mid b$

2.2. If $c \mid a$ and $c \mid b$, then $c \mid d$

Furthermore, $\exists s, t \in \mathbb{Z}$ such that

$$d = sa + tb$$

Note that this number if unique and is called the greatest common divisor (GCD) of a and b, denoted by

$$gcd(a, b) = (a, b)$$

(proof later)

Definition 2.5. Given $a, b \in \mathbb{Z}$, we say that they are relatively prime if $gcd(a, b) = 1$

Lemma 2.6 (Euclid's Lemma)**.** *If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$. In particular, if p prime and $p \mid bc$, then either $p \mid b$ or $p \mid c$*

Proof. By the previous theorem, $\exists s, t \in \mathbb{Z}$ such that

$$sa + tb = 1$$

Hence,

$$sac + tbc = c$$

Since $a \mid sac$ and $a \mid tbc$, it follows that $a \mid c$. □

(End of Day 2)

Theorem 2.7 (Unique Factorization theorem)**.** *Given $a \in \mathbb{Z}$ with $a > 1$, then $\exists$ prime numbers $p_1, p_2, \ldots, p_k \in \mathbb{Z}$ such that*

$$a = p_1 p_2 \ldots p_k$$

Furthermore, these primes are unique upto re-arrangement. ie. If $q_1, q_2, \ldots, q_m \in \mathbb{Z}$ are primes such that

$$a = q_1 q_2 \ldots q_m$$

Then $m = k$ and, after rearrangement, $q_i = p_i$ for all $1 \leq i \leq m$.

Proof.

- Existence: Let $a \in \mathbb{Z}_+$ with $a > 1$. If $a = 2$, then there is nothing to prove, so suppose $a > 2$. By induction, assume that the theorem is true for all numbers $d < a$.

  Now fix a and note that if a is prime, there is nothing to prove. Suppose a is not prime, then $\exists b \in \mathbb{Z}_+$ such that $b \mid a$, but $b \neq \pm a$ and $b \neq \pm 1$. Hence, $a = bc$ where we may assume that $1 < b, c < a$. So by induction hypothesis, both b and c can be expressed as products of primes. Hence, a can be too.

- Uniqueness: Suppose a can be expressed in two ways as above. Then

  $$p_1 \mid a = q_1 q_2 \dots q_m$$

  By Euclid's lemma, $\exists 1 \leq j \leq m$ such that $p \mid q_j$. Assume without loss of generality that $p \mid q_1$. Since p is prime, $p \neq \pm 1$. Since q_1 is prime, it follows that $p = \pm q_1$. Hence,

  $$q_1 p_2 p_3 \dots p_k = q_1 q_2 \dots q_m$$

  Cancellation implies that

  $$p_2 p_3 \dots p_k = q_2 q_3 \dots q_m$$

  Now induction completes the proof (How?)

□

3. Subgroups and Cyclic Groups

3.1. Definition: Let $(G, *)$ be a group and $H \subset G$. H is called a subgroup of G if, $(H, *)$ is itself a group. If this happens, we write $H < G$.

3.2. Lemma: let G be a group and $H \subset G$. Then $H < G$ if and only if, for each $a, b \in H$, $ab^{-1} \in H$.

Proof. Suppose H is a subgroup, then for any $a, b \in H, b^{-1} \in H$, so $ab^{-1} \in H$.

Conversely, suppose this condition holds, then we wish to show that H is a subgroup.

- Identity: If $a \in H$, then $aa^{-1} = e \in H$
- Inverse: If $a \in H$, then $ea^{-1} = a^{-1} \in H$
- Closure: If $a, b \in H$, then $b^{-1} \in H$, so $b = (b^{-1})^{-1} \in H$. Hence, $ab = a(b^{-1})^{-1} \in H$.
- Associativity: holds trivially because it holds in G.

□

3.3. Examples :

(i) For fixed $n \in \mathbb{N}$, consider

$$n\mathbb{Z} := \{0, \pm n, \pm 2n, \dots\}$$

(ii) $\{R_0, R_{90}, R_{180}, R_{270}\} < D_4$

(iii) (See Example 1.5(iii)) $G_k < S^1$ where $S^1 := \{z \in \mathbb{C} : |z| = 1\}$.

(iv) $(\mathbb{Q}, +) < (\mathbb{R}, +)$

(v) $SL_n(\mathbb{R}) < GL_n(\mathbb{R})$ where $SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$

3.4. Theorem: Every subgroup $H < \mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$

Proof. If $H < \mathbb{Z}$, then consider $S := \{h \in H : h > 0\}$, then S has a smallest member n by the well-ordering principle. We claim

$$H = n\mathbb{Z}$$

Since $n \in H$, so $n\mathbb{Z} \subset H$. So suppose $h \in H$, we WTS: $h \in n\mathbb{Z}$. Assume WLOG that $h > 0$, and use Division Algorithm to write

$$h = nq + r, \text{ where } 0 \leq r < n$$

Now, $nq \in H$ and $h \in H$, so $r \in H$. But then $r \in S$, and $0 \leq r < n$. If $r > 0$, then this would contradict the minimality of n, so $r = 0$. Hence,

$$h = nq \in n\mathbb{Z}$$

□

Proof of Theorem 2.4

Proof. Let $a, b \in \mathbb{Z}$. WTS: $\exists d \in \mathbb{Z}$ with the required properties. Consider

$$H := \{sa + tb : s, t \in \mathbb{Z}\}$$

Then (Check!) that $H < \mathbb{Z}$. Hence, $\exists d \in \mathbb{Z}_+$ such that $H = d\mathbb{Z}$. Now observe:

- $a = 1 \cdot a + 0 \cdot b \in H$, so $d \mid a$. Similarly, $d \mid b$
- $\exists s, t \in \mathbb{Z}$ such that $d = sa + tb$.
- If $c \mid a$ and $c \mid b$, then $c \mid sa + tb = d$.

Hence, $d = gcd(a, b)$. □

3.5. Remark : G a group, $a \in G$ fixed.

(i) Cyclic subgroup generated by a is the set

$$\{a^n : n \in \mathbb{Z}\}$$

and is denoted by $\langle a \rangle$

(ii) Order of a, denoted by $O(a)$, is $|\langle a \rangle|$. If $n = O(a) < \infty$, then

(a) $a^m = e \Leftrightarrow n \mid m$

(b) $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

3.6. Example :

(i) $G = \mathbb{Z}$, $a = n$, then a has infinite order

(ii) $G = D_4$, $a = R_{90}$, then $O(a) = 4$

(iii) $G = S^1, a = e^{2\pi i/k}$, then $O(a) = k$

3.7. Theorem: Every subgroup of a cyclic group is cyclic.

Proof. Suppose $G = \langle a \rangle$ is cyclic, and $H < G$, then consider

$$S := \{n \in \mathbb{Z} : a^n \in H\} \subset \mathbb{Z}$$

Since $e \in H, 0 \in S$. If $n, m \in S$, then $a^n, a^m \in H$, so

$$a^{n-m} = a^n(a^m)^{-1} \in H \Rightarrow n - m \in S$$

Hence, $S < \mathbb{Z}$ by Lemma 3.2. By Theorem 3.4, $\exists k \in \mathbb{Z}$ such that $S = k\mathbb{Z}$. Hence,

$$a^n \in H \Leftrightarrow k \mid n$$

In other words, $H = \langle a^k \rangle$. □

(End of Day 3)

4. Orthogonal Matrices and Rotations

(See [Artin, §5.1] (mostly taken from the 1st edition))

4.1. Definition :

(i) Real Orthogonal matrix is a matrix A such that $A^tA = AA^t = I$

(ii) $O_n(\mathbb{R})$ is the set of all orthogonal matrices.

$$SO_n(\mathbb{R}) := \{A \in O_n(\mathbb{R}) : \det(A) = 1\}$$

Note that $O_n(\mathbb{R})$ and $SO_n(\mathbb{R})$ are subgroups of $GL_n(\mathbb{R})$ [Check!]

4.2. Theorem : Let A be an $n \times n$ real matrix. Then TFAE :

(i) A is an orthogonal matrix

(ii) $\langle Ax, Ay \rangle = \langle x, y \rangle$ for all $x, y \in \mathbb{R}^n$

(iii) The columns of A form an orthonormal basis of $\mathbb{R}^n$

Proof. We prove each implication (i) ⇒ (ii) ⇒ (iii) ⇒ (i).

(i)⇒ (ii): If $AA^t = A^tA = I$, then fix $x, y \in \mathbb{R}^n$, then

$$\langle Ax, Ay \rangle = (Ay)^t(Ax) = (y^tA^t)(Ax) = y^t(A^tA)x = y^tx = \langle x, y \rangle$$

(ii)⇒ (iii): If $\langle Ax, Ay \rangle = \langle x, y \rangle$, then consider the standard basis $\{e_1, e_2, \ldots, e_n\}$ of $\mathbb{R}^n$. Then

$$\langle Ae_i, Ae_j \rangle = \langle e_i, e_j \rangle = \delta_{i,j}$$

But the columns of A are precisely the vectors $\{Ae_i : 1 \leq i \leq n\}$

(iii)$\Rightarrow$ (i): Suppose the columns of A form an orthonormal basis of $\mathbb{R}^n$. Then, for any $1 \leq i \leq n$,

$$\langle e_i, e_j \rangle = \delta_{i,j} = \langle Ae_i, Ae_j \rangle = \langle A^t Ae_i, e_j \rangle$$

This is true for all $1 \leq j \leq n$, so (Why?)

$$A^t Ae_i = e_i$$

Hence, $A^t A = I$ because the $\{e_i\}$ form a basis. Similarly, $AA^t = I$ as well.

□

4.3. Example :

(i) For $\theta \in \mathbb{R}$, $\rho_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \in SO_2(\mathbb{R})$

(ii) $r = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$

4.4. Lemma: $SO_2(\mathbb{R}) = \{\rho_\theta : \theta \in \mathbb{R}\}$. Hence, $SO_2(\mathbb{R})$ is called the 2×2 rotation group.

Proof. If

$$A = \begin{pmatrix} c & a \\ s & b \end{pmatrix}$$

is an orthogonal matrix, then $(c, s) \in \mathbb{R}^2$ is a unit vector. Hence, $\exists \theta \in \mathbb{R}$ such that $c = \cos(\theta)$ and $s = \sin(\theta)$. Now let

$$R := \begin{pmatrix} c & -s \\ s & c \end{pmatrix} = \rho_\theta$$

Then $R \in SO_2(\mathbb{R})$ and hence

$$P := R^t A = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in SO_2(\mathbb{R})$$

By the previous lemma, the second column of P is a unit vector perpendicular to $(0, 1)$. Hence,

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

Since $\det(P) = 1$, $P = I$, so $A = R = \rho_\theta$. □

4.5. Definition: A rotation of $\mathbb{R}^3$ about the origin is a linear operator ρ with the following properties:

(i) ρ fixes a unit vector $u \in \mathbb{R}^3$

(ii) ρ rotates the two dimensional subspace W orthogonal to u.

The matrix associated to a rotation is called a rotation matrix, and the axis of rotation is the line spanned by u.

4.6. Example/Remark:

(i) The identity matrix is a rotation, although its axis is indeterminate.

(ii) The matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

is a rotation matrix with axis $\operatorname{span}(e_1)$.

(iii) If ρ is a rotation that is not the identity, then let u be a unit vector in its axis of rotation. Let $W := \{u\}^\perp$ denote the subspace orthogonal to u. Then $W \cong \mathbb{R}^2$, and

$$\rho|_W \colon W \to W$$

is a rotation. Hence, we may think of $\rho|_W \in SO_2(\mathbb{R})$. The angle of rotation (computed by the Right Hand Rule) is denoted by θ, and we write $\rho = \rho_{(u,\theta)}$. The pair (u, θ) is called the spin of the rotation ρ.

4.7. Lemma: If $A \in SO_3(\mathbb{R}), \exists v \in \mathbb{R}^3$ such that $Av = v$.

Proof. We show that 1 is an eigen-value of A. To see this, note that

$$\det(A - I) = (-1)\det(I - A) \text{ and } \det(A - I) = \det((A - I)^t)$$

by the properties of the determinant. Since $\det(A) = 1$, we have

$$\det(A - I) = det((A - I)^t) = \det(A)\det(A^t - I) = \det(AA^t - A) = det(I - A)$$

Hence, $\det(A - I) = 0$ as required. □

(End of Day 4)

4.8. Euler's Theorem: The elements of $SO_3(\mathbb{R})$ are precisely all the rotation matrices. ie.

$$SO_3(\mathbb{R}) = \{\rho_{u,\theta} : u \in \mathbb{R}^3 \text{ unit vector}, \theta \in \mathbb{R}\}$$

Proof. (i) Let $\rho = \rho_{u,\theta}$. Since u is a unit vector, there is an orthonormal basis $\mathcal{B}$ of $\mathbb{R}^3$ containing u. Let P denote the change of basis matrix associated to $\mathcal{B}$. Then $P \in SO_3(\mathbb{R})$ because its columns are orthogonal (by Lemma 4.2). Furthermore,

$$B := PAP^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Hence, $B \in SO_3(\mathbb{R})$. Since $P \in SO_3(\mathbb{R})$, it follows that $\rho \in SO_3(\mathbb{R})$.

(ii) Conversely, suppose $A \in SO_3(\mathbb{R})$, then choose a unit vector $v \in \mathbb{R}^3$ such that $Av = v$. Consider an orthonormal basis $\mathcal{B}$ of $\mathbb{R}^3$ containing v, then with P as above,

$$B := PAP^{-1} \in SO_3(\mathbb{R})$$

Let $W := \{e_1\}^\perp$, then $B(e_1) = e_1$ and $B(W) \subset W$. Hence, B has the form

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

Let $C := \begin{pmatrix} a & b \\ c & b \end{pmatrix}$, then $\det(C) = \det(B) = 1$, and the columns of C are orthogonal vectors. Hence by Lemma 4.2, $C \in SO_2(\mathbb{R})$. Hence, $\exists \theta \in \mathbb{R}$ such that

$$C = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Hence, $B = \rho_{e_1,\theta}$, so $A = \rho_{v,\theta}$.

□

4.9. Corollary: Composition of rotations about any two axes is a rotation about some other axis.

5. Homomorphisms

5.1. Definition: Let $(G, *)$ and $(G', \cdot)$ be two groups. A function $\varphi : G \to G'$ is called a group homomorphism if

$$\varphi(g_1 * g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

for all $g_1, g_2 \in G$.

5.2. Examples :

(i) $n \mapsto 2n$ from $\mathbb{Z}$ to $\mathbb{Z}$

(ii) $x \mapsto e^x$ from $(\mathbb{R}, +)$ to $(\mathbb{R}^*, \times)$

(iii) $det : GL_n(\mathbb{R}) \to \mathbb{R}^*$

(iv) $\theta \mapsto \rho_\theta$ from $(\mathbb{R}, +)$ to $SO_2(\mathbb{R})$

5.3. Lemma : Let $\varphi : G \to G'$ be a group homomorphism, then

(i) $\varphi(e) = e'$ where e, e' are the identity elements of G and G' respectively

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$

Proof. (i) Note that

$$e' \cdot \varphi(e) = \varphi(e) = \varphi(e * e) = \varphi(e) * \varphi(e)$$

By cancellation, $\varphi(e) = e'$

(ii) For $g \in G$,

$$\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e) = e' = \varphi(g) \cdot \varphi(g)^{-1}$$

By cancellation $\varphi(g^{-1}) = \varphi(g)^{-1}$.

□

5.4. Definition : $\varphi : G \to G'$ a homomorphism

(i) $\ker(\varphi) := \{g \in G : \varphi(g) = e'\}$. Note that $\ker(\varphi) < G$

(ii) $\text{Image}(\varphi) := \{\varphi(g) : g \in G\}$. Note that $\text{Image}(\varphi) < G'$.

5.5. Examples :

(i) $\varphi : \mathbb{Z} \to \mathbb{Z}$ is $\varphi(n) = 2n$, then $\ker(\varphi) = \{0\}$, $\text{Image}(\varphi) = 2\mathbb{Z}$

(ii) $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is $\varphi(A) = det(A)$, then $\ker(\varphi) = SL_n(\mathbb{R})$, $\text{Image}(\varphi) = \mathbb{R}^*$

(iii) $\varphi : \mathbb{R} \to SO_2(\mathbb{R})$ is $\varphi(\theta) = \rho_\theta$, then $\ker(\varphi) = 2\pi\mathbb{Z}$, $\text{Image}(\varphi) = SO_2(\mathbb{R})$ by Lemma 4.4

(iv) $\varphi : \mathbb{C}^* \to \mathbb{R}^*$ is $\varphi(z) = |z|$, then $\ker(\varphi) = S^1$, $\text{Image}(\varphi) = \mathbb{R}^*$

5.6. Definition : Let $\varphi : G \to G'$ be a group homomorphism

(i) φ is said to be injective (or one-to-one) if, for any $g_1, g_2 \in G$,

$$\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$$

(ii) φ is said to be surjective (or onto) if, for any $g' \in G', \exists g \in G$ such that $\varphi(g) = g'$.

(iii) φ is said to be bijective if it is both injective and surjective. Note, if φ is bijective, then

$$\varphi^{-1} : G' \to G$$

is also a group homomorphism. If such a homomorphism exists, then we say that φ is an isomorphism, and we write

$$G \cong G'$$

5.7. Theorem : $\varphi : G \to G'$ is injective iff $\ker(\varphi) = \{e\}$. In that case, $\varphi : G \xrightarrow{\sim} \text{Image}(G)$.

Proof. (i) If φ is injective, and $g \in \ker(\varphi)$, then $\varphi(g) = e' = \varphi(e)$. Hence, $g = e$, whence $\ker(\varphi) = \{e\}$.

(ii) Conversely, if $\ker(\varphi) = \{e\}$, and suppose $g_1, g_2 \in G$ such that $\varphi(g_1) = \varphi(g_2)$, then

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e'$$

Hence, $g_1 g_2^{-1} \in \ker(\varphi)$, so $g_1 g_2^{-1} = e$, whence $g_1 = g_2$. Thus, φ is injective.

The second half of the argument follows from the fact that $\varphi : G \to \text{Image}(\varphi)$ is surjective. □

(End of Day 5)

5.8. Examples :

(i) $\varphi : \mathbb{Z} \to \mathbb{Z}$ is $\varphi(n) = 2n$, then φ is injective, but not surjective

(ii) $\varphi : (\mathbb{R}, +) \to SO_2(\mathbb{R})$ is $\varphi(\theta) = \rho_\theta$, then f is surjective, but not injective, because $\rho_0 = \rho_{2\pi}$.

(iii) If G is a finite cyclic group with $|G| = k$, then $G \cong G_k$

Proof. Let $G = \langle a \rangle$ with $|a| = k$. Define a map $\varphi : G \to G^k$ by

$$a^n \mapsto \zeta^n$$

where $\zeta = e^{2\pi i/k}$. Then (Check!) that φ is an isomorphism. □

(iv) $G_4 \ncong V_4$

Proof. Suppose there were an isomorphism $\varphi : G_4 \to V_4$, then consider $b := \varphi(\zeta)$, where $\zeta = e^{2\pi i/4}$. Since $|\zeta| = 4$, it follows that $|b| = 4$ (Why?). But V_4 has no elements of order 4, so this is impossible. □

6. The Symmetric Group

6.1. Definition : Let X be a set

(i) A permutation of X is a bijective function $\sigma : X \to X$

(ii) Let S_X denote the set of all permutations of X. Given two elements $\sigma, \tau \in S_X$, the product $\sigma \circ \tau \in S_X$ is given by composition. Since composition of functions is associative, this operation makes S_X a group, called the symmetric group on X.

6.2. Lemma : If $|X| = |Y|$, then $S_X \cong S_Y$

Proof. If $|X| = |Y|$, there is a bijective function $f : X \to Y$. Define $\Theta : S_X \to S_Y$ by

$$\Theta(\sigma) := f \circ \sigma \circ f^{-1}$$

Then

(i) Θ is a group homomorphism:

$$\Theta(\sigma \circ \tau) = f \circ \sigma \circ \tau \circ f^{-1} = f \circ \sigma \circ f^{-1} \circ f \circ \tau \circ f^{-} = \Theta(\sigma) \circ \Theta(\tau)$$

(ii) Θ is injective: If $\sigma \in \ker(\Theta)$, then $f \circ \sigma \circ f^{-1} = \mathrm{id}_Y$. For each $y \in Y$,

$$f(\sigma(f^{-1}(y)) = y \Rightarrow \sigma(f^{-1}(y)) = f^{-1}(y) \quad \forall y \in Y$$

Since f^{-1} is surjective, this implies

$$\sigma(x) = x \quad \forall x \in X$$

So $\sigma = \mathrm{id}_X$.

(iii) Θ is surjective: Given $\tau \in S_Y$, define $\sigma := f^{-1} \circ \tau \circ f$, then $\sigma \in S_X$ and $\Theta(\sigma) = \tau$.

□

6.3. Definition : If $X = \{1, 2, \ldots, n\}$, then S_X is denoted by S_n, and is called the symmetric group on n letters. By the previous lemma, if Y is any set such that $|Y| = n$, then $S_Y \cong S_n$

6.4. Remark :

(i) $O(S_n) = n!$

Proof. Let $\sigma \in S_n$, then $\sigma(1) \in \{1, 2, \ldots, n\}$ has n choices. Now $\sigma(2)$ has $(n-1)$ choices, and so on. The total number of possible such σ's is $n \times (n-1) \times \ldots \times 1 = n!$. □

(ii) If $\sigma \in S_n$, we represent σ by

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

(iii) For $\sigma \in S_n$, define $P_\sigma \in GL_n(\mathbb{R})$ by $P_\sigma(e_i) = e_{\sigma(i)}$. Since the columns of P_σ are orthogonal, $P_\sigma \in O_n(\mathbb{R})$

6.5. Theorem : The function $\varphi : S_n \to O_n(\mathbb{R})$ by $\sigma \mapsto P_\sigma$ is a homomorphism.

Proof. Given $\sigma, \tau \in S_n$, consider

$$P_{\sigma\circ\tau}(e_i) = e_{\sigma\circ\tau(i)} = e_{\sigma(\tau(i))} = P_\sigma(e_{\tau(i)}) = P_\sigma P_\tau(e_i)$$

This is true for each i, so $P_{\sigma\circ\tau} = P_\sigma P_\tau$. □

6.6. Definition :

(i) Note that $\det : O_n(\mathbb{R}) \to \{\pm 1\}$ is a group homomorphism. Define the sign function

$$sgn : S_n \to \{\pm 1\}$$

as the composition $\sigma \mapsto P_\sigma \mapsto \det(P_\sigma)$

(ii) The alternating group on n letters is

$$A_n := \{\sigma \in S_n : sgn(\sigma) = 1\}$$

6.7. Remark/Example :

(i) In S_3, consider

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto -1$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \mapsto 1$$

Hence,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in A_3 \text{ but } \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \notin A_3$$

(ii) $S_n = A_n \sqcup B_n$ where $B_n = \{\sigma \in S_n : sgn(\sigma) = -1\}$ [Not a subgroup of S_n]

(iii) Let $\sigma_0 \in S_n$ denote the permutation

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}$$

For any $\sigma \in A_n, \sigma_0\sigma \in B_n$ and conversely. Hence the map

$$f : A_n \to B_n \text{ given by } \sigma \mapsto \sigma_0\sigma$$

is a bijection (not a group homomorphism though). Hence,

$$S_n = A_n \sqcup B_n$$

and

$$|A_n| = |B_n| = \frac{n!}{2}$$

(End of Day 6)

II. Quotient Groups

1. Modular Arithmetic

1.1. Definition : Let X be a set. An equivalence relation on a set X is a subset $R \subset X \times X$ such that

(i) $(x, x) \in R$ for all $x \in X$ [Reflexivity]

(ii) If $(x, y) \in R$, then $(y, x) \in R$ [Symmetry]

(iii) If $(x, y), (y, z) \in R$, then $(x, z) \in R$ [Transitivity]

We write $x \sim y$ if $(x, y) \in R$.

1.2. Examples :

(i) X any set, $x \sim y \Leftrightarrow x = y$

(ii) $X = \mathbb{R}^2$, $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow y_1 - y_2 = x_1 - x_2$

(iii) $X = \mathbb{C}$, $z \sim w \Leftrightarrow |z| = |w|$

(iv) $X = \mathbb{Z}$, $a \sim b \Leftrightarrow n \mid (b - a)$. Denote this by $a \equiv b \pmod{n}$

Proof. (a) Reflexivity: Obvious

(b) Symmetry: If $a \sim b$, then $b - a = nk$ for some $k \in \mathbb{Z}$, so $a - b = n(-k)$, whence $n \mid (a - b)$, so $b \sim a$.

(c) Transitivity: If $a \sim b$ and $b \sim c$, then $\exists k, \ell \in \mathbb{Z}$ such that

$$b - a = nk \text{ and } c - b = n\ell$$

Hence

$$c - a = c - b + b - a = n(\ell + k) \Rightarrow n \mid (c - a) \Rightarrow a \sim c$$

□

1.3. Definition: Let X be a set, and $\sim$ an equivalence relation on X. For $x \in X$, the equivalence class of x is the set

$$[x] := \{y \in X : y \sim x\}$$

Note that $x \in [x]$, so it is a non-empty set.

1.4. Theorem : Equivalence classes partition the set

Proof. Since $x \in [x]$ for all $x \in X$, we have that

$$X = \bigcup_{x \in X} [x]$$

WTS: Any two equivalence classes are either disjoint or equal. So fix two classes $[x], [y]$ and suppose

$$z \in [x] \cap [y]$$

WTS: $[x] = [y]$ So choose $w \in [x]$, then

$$w \sim x \sim z \sim y \Rightarrow w \in [y]$$

Hence, $[x] \subset [y]$. Similarly, $[y] \subset [x]$ □

1.5. Examples : (See Example 1.2)

(i) $[x] = \{x\}$

(ii) $[(x_1, y_1)] =$ the line parallel to the line $y = x$ passing through (x_1, y_1)

(iii) $[z] =$ the circle of radius $|z|$

(iv) $[a] = \{b \in Z : \exists q \in \mathbb{Z}$ such that $b = a + nq\}$

1.6. Lemma : Consider $\mathbb{Z}$ with $\equiv \pmod{n}$

(i) There are exactly n equivalence classes $\{[0], [1], \ldots, [n-1]\}$

(ii) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a + b \equiv (a' + b') \pmod{n}$

Proof. (i) Firstly note that if $0 \leq i, j \leq n-1$, then $i \nsim j$. Hence, there are at least $n-1$ equivalence classes as listed above. To see that there are exactly n equivalence classes, note that if $a \in \mathbb{Z}$, then by the Division Algorithm, $\exists q, r \in \mathbb{Z}$ such that

$$a = nq + r, \text{ and } 0 \leq r < n$$

Hence, $[a] = [r]$ as required.

(ii) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $\exists k, \ell \in \mathbb{Z}$ such that

$$a = a' + kn \text{ and } b = b' + \ell n$$

Hence,

$$a + b = a' + b' + n(k + \ell)$$

so $(a + b) = (a' + b') \pmod{n}$ as required.

□

1.7. Definition: Consider the set of all equivalence classes

$$\mathbb{Z}_n := \{[0], [1], [2], \ldots, [n-1]\}$$

We define the sum of two classes as

$$[a] + [b] := [a + b]$$

This is well-defined by the previous lemma.

1.8. Theorem: $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$ is a cyclic group of order n with generator $[1]$

Proof. (i) Associativity: Because $+$ on $\mathbb{Z}$ is associative.

(ii) Identity: $[0]$ is the identity element.

(iii) Inverse: Given $[a] \in \mathbb{Z}_n$, assume without loss of generality that $0 \leq a < n$, then $b := n - a$ has the property that

$$[a] + [b] = [a + b] = [n] = [0]$$

(iv) Cyclic: For any $a \in \mathbb{Z}$

$$[a] = a[1]$$

so $\mathbb{Z}_n$ is cyclic with generator $[1]$.

□

2. Lagrange's Theorem

Recall: In constructing $\mathbb{Z}_n$, we had 4 steps :

(i) Define an equivalence relation $\equiv \pmod{n}$ on $\mathbb{Z}$

(ii) Collecting the equivalence classes together : $\mathbb{Z}_n$

(iii) Counting that there are n of them

(iv) Defining a group structure on the equivalence classes, and showing that it is well-defined.

We now do the same thing for a general group.

2.1. Definition/Lemma : G a group, $H < G$. We say that two elements $a, b \in G$ are equivalent iff

$$a^{-1}b \in H$$

This is an equivalence relation, and we write $a \equiv b \pmod{H}$ if this happens.

Proof. (i) Reflexivity: If $a \in G$, then

$$a^{-1}a = e \in H$$

Hence, $a \equiv a \pmod{H}$.

(ii) Symmetry: If $a, b \in G$ and $a \equiv b \pmod{H}$, then $a^{-1}b \in H$. Since H is a subgroup

$$b^{-1}a = (a^{-1}b)^{-1} \in H$$

So $b \equiv a \pmod{H}$

(iii) Transitivity: If $a, b, c \in G$ and $a \equiv b \pmod{H}, b \equiv c \pmod{H}$, then

$$a^{-1}b, b^{-1}c \in H \Rightarrow a^{-1}c \in H$$

so $a \equiv c \pmod{H}$.

□

2.2. Definition :

(i) The equivalence class $[a]$ is called a left coset of H in G. Note that

$$[a] = \{ah : h \in H\} =: aH$$

Note that a coset aH is not a group unless $aH = H$.

(ii) The number of cosets of H in G is called the index of H in G and is denoted by $[G : H]$

(End of Day 7)

2.3. Examples :

(i) $G = \mathbb{Z}$, $H = n\mathbb{Z}$, then

(a) $a \equiv b \pmod{H}$ iff $a \equiv b \pmod{n}$

(b) $[\mathbb{Z} : n\mathbb{Z}] = n$ (Lemma 1.6)

(ii) $G = S_n, H = A_n$, then

(a) $\sigma = \tau \pmod{H}$ iff $sgn(\sigma) = sgn(\tau)$

(b) $[G : H] = 2$ (Remark I.6.7)

(iii) $G = \mathbb{C}^*, H = S^1$, then

(a) $z \equiv w \pmod{H}$ iff $|z| = |w|$

(b) $[G : H] = |(0, \infty)| = +\infty$

(iv) $G = \mathbb{R}^2$, $H = \{(x, x) : x \in \mathbb{R}\}$, then

(a) $(x_1, y_1) \equiv (x_2, y_2) \pmod{H}$ iff $y_1 - y_2 = x_1 - x_2$ iff (x_1, y_1) and (x_2, y_2) lie on the same line parallel to the line $y = x$.

(b) $[G : H] = |\mathbb{R}| = +\infty$

2.4. Lemma : $|aH| = |bH|$ for any $a, b \in G$

Proof. Define $f : aH \to bH$ by $ah \mapsto bh$. This map is

(i) Well-defined: If $ah_1 = ah_2$, then $h_1 = h_2$ by cancellation, so $bh_1 = bh_2$.

(ii) Injective: If $bh_1 = bh_2$, then $h_1 = h_2$ by cancellation, so $ah_1 = ah_2$

(iii) Surjective: Obvious.

Hence f is a bijection. □

2.5. Lagrange's theorem : Let G be a finite group, then $|G| = [G : H]|H|$. In particular, $|H| \mid |G|$

Proof. Since the equivalence relation partitions G, G is a disjoint union of cosets. We enumerate the disjoint cosets by $\{a_1H, a_2H, \ldots, a_kH\}$, where $k = [G : H]$, so that

$$G = \bigsqcup_{i=1}^{k} a_iH$$

By Lemma 2.4, $|a_iH| = |H|$ for all i, so

$$|H| = \sum_{i=1}^{k} |a_iH| = \sum_{i=1}^{k} |H| = [G : H]|H|$$

□

2.6. Corollary: If $|G| = p$, a prime, then G is cyclic.

Proof. Let $x \in G$ be a non-identity element, then $H := \langle x \rangle$ is a subgroup of G. In particular,

$$|H| \mid p \Rightarrow |H| \in \{1, p\}$$

But $|H| \neq 1$, so $|H| = p$ whence $H = G$. □

2.7. Corollary: If $a \in G$, then $O(a) \mid |G|$, and hence $a^{|G|} = e$

Proof. Note that $O(a) = |\langle a \rangle|$, so $O(a) \mid |G|$ by Lagrange's theorem. Furthermore, if $k \in \mathbb{Z}$ such that $kO(a) = |G|$, then

$$a^{|G|} = (a^{O(a)})^k = e^k = e$$

□

3. Normal Subgroups

3.1. Definition : Let G be a group and $H < G$. Define

$$G/H := \{aH : a \in G\}$$

to be the set of all cosets of H in G. Note that $[G : H] = |G/H|$.

Important: G/H is not, in general, a group.

3.2. Examples :

(i) $G = \mathbb{Z}, H = n\mathbb{Z}$, then $G/H = \mathbb{Z}_n$

(ii) $G = \mathbb{C}^*, H = S^1$, then $G/H = \{\text{circles with varying radii around } 0\}$

(iii) $G = \mathbb{R}^2, H = \{(a, a) : x \in \mathbb{R}\}$, then $G/H = \{\text{lines parallel to } y = x\}$

(iv) $G = S_n, H = A_n$, then $G/H = \{A_n, B_n\}$ where $B_n = \{\sigma \in S_n : sgn(\sigma) = -1\}$

3.3. Remark : We want to define a group operation on G/H by

$$[a] * [b] = [ab]$$

Recall proof of Lemma 1.6(ii). Note: We only used the fact that $G = \mathbb{Z}$ is abelian.

3.4. Lemma : If G is abelian, and $H < G$, then $(G/H, *)$ is a group.

Proof. (i) Well-definedness of $*$: If $a_1 \equiv a_2 \pmod{H}$ and $b_1 \equiv b_2 \pmod{H}$, then WTS:

$$a_1 b_1 \equiv a_2 b_2 \pmod{H}$$

To see this, note that $a_1^{-1} a_2 \in H$ and $b_1^{-1} b_2 \in H$, so

$$(a_1 b_1)^{-1}(a_2 b_2) = b_1^{-1} a_1^{-1} a_2 b_2 = a_1^{-1} a_2 b_1^{-1} b_2 \in H$$

since G is abelian.

(ii) Now it is clear that $*$ is a binary operation that is associative since multiplication in G is associative.

(iii) Identity: $[e] \in G/H$ has the property that $[a] * [e] = [ae] = [a] = [e] * [a]$ for all $[a] \in G/H$

(iv) Inverse: Given $[a] \in G/H, a \in G$, so $a^{-1} \in G$, and

$$[a] * [a^{-1}] = [e] = [a^{-1}] * [a]$$

□

3.5. Remark: To show that $*$ is well-defined, we needed that: If $a_1^{-1} a_2 \in H$ and $b_1^{-1} b_2 \in H$, then

$$(a_1 b_1)^{-1}(a_2 b_2) \in H$$

Expanding out, this requires

$$b_1^{-1} a_1^{-1} a_2 b_2 \in H$$

We don't necessarily need G to be abelian.

3.6. Definition : Let G be a group and $H < G$. We say that H is a normal subgroup if, for each $h \in H$ and $g \in G$, we have

$$ghg^{-1} \in H$$

If this happens, we write $H \lhd G$.

(End of Day 8)

3.7. Theorem : If $H \lhd G$, then $(G/H, *)$ is a group under the operation

$$[a] * [b] := [ab]$$

Proof. We only need to prove well-definedness of $*$. The rest of the argument is as in Lemma 3.4. As before, we have $a_1, a_2, b_1, b_2 \in G$ such that $a_1^{-1} a_2 \in H$ and $b_1^{-1} b_2 \in H$. We WTS:

$$(a_1 b_1)^{-1} a_2 b_2 = b_1^{-1} a_1^{-1} a_2 b_2 \in H$$

Note that since $H \lhd G$

$$h := b_1^{-1}(a_1^{-1} a_2) b_1 \in H$$

Hence, $h b_1^{-1} = b_1^{-1} a_1^{-1} a_2$, so

$$b_1^{-1} a_1^{-1} a_2 b_2 = h b_1^{-1} b_2 \in H$$

□

3.8. Examples :

(i) $G = \mathbb{Z}, H = n\mathbb{Z}$, then $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

(ii) $G = \mathbb{C}^*, H = S^1$, then $*$ is the same as multiplying radii. $G/H \cong ((0,\infty), \times)$

Proof. Define $\varphi : G/H \to (0,\infty)$ by

$$\varphi([z]) := |z|$$

Then φ is well-defined and injective because

$$|z| = |w| \Leftrightarrow [z] = [w]$$

φ is clearly surjective, so it is suffices to show that it is a group homomorphism. But this follows from

$$\varphi([z] * [w]) = \varphi([zw]) = |zw| = |z||w| = \varphi([z])\varphi([w])$$

□

(iii) $G = \mathbb{R}^2, H = \{(a,a) : a \in \mathbb{R}\}$, then $*$ is the same as adding Y-intercepts. $G/H \cong (\mathbb{R}, +)$

Proof. Recall that any coset of H is of the form

$$y + H := \{(a, a+y) : a \in \mathbb{R}\}$$

and is a line parallel to the line $y = x$ with Y-intercept y. Define $\varphi : G/H \to \mathbb{R}$ by

$$\varphi(y + H) := y$$

This map is well-defined (Check!) and a group homomorphism. It is also injective because

$$y_1 + H = y_2 + H \Leftrightarrow y_1 = y_2$$

and is clearly surjective, so it is an isomorphism. □

(iv) $G = S_n, H = A_n$. $H \lhd G$ and $G/H \cong (\{\pm 1\}, \times)$

Proof. Define $\varphi : G/H \to \{\pm 1\}$ by

$$\varphi([\sigma]) = sgn(\sigma)$$

Then (Check!) φ is an isomorphism. □

3.9. Proposition: If G abelian, then every subgroup is normal.

Proof. Trivial, because $ghg^{-1} = h$ for all $g, h \in G$. □

3.10. Proposition: If $\varphi : G \to G'$ is a group homomorphism, then $\ker(\varphi) \lhd G$. In particular, $G/\ker(\varphi)$ is a group.

Proof. If $H = \ker(\varphi)$, then $H < G$ (by I.5.4). If $h \in H$, then for any $g \in G$,

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)e'\varphi(g)^{-1} = e'$$

so $ghg^{-1} \in H$. □

4. The Isomorphism Theorems

4.1. Proposition : Let $H \lhd G$, then the map $\pi : G \to G/H$ given by $\pi(a) = aH$ is a surjective homomorphism and $\ker(\pi) = H$

Proof. (i) π is surjective: Obvious because every element in G/H is of the form aH

(ii) π is a homomorphism: Because of the way multiplication is defined in G/H

$$(aH) * (bH) = abH$$

(iii) $\ker(\pi) = H$: If $h \in H$, then $hH = H$ which is the identity in G/H. Hence,

$$H \subset \ker(\pi)$$

Conversely, if $a \in \ker(\pi)$, then $aH = H$. But $a \in aH$, so $a \in H$ as required.

□

4.2. First Isomorphism theorem : Let $\varphi : G \to G'$ be a group homomorphism, then

$$G/\ker(\varphi) \cong \text{Image}(\varphi)$$

In particular, if φ is surjective, then $G/\ker(\varphi) \cong G'$

Proof. Define $H := \ker(\varphi)$ and $\widehat{\varphi} : G/H \to G'$ by

$$\widehat{\varphi}(aH) := \varphi(a)$$

Then

(i) $\widehat{\varphi}$ is well-defined: Suppose $aH = bH$, then $a^{-1}b \in H$, so

$$\varphi(a^{-1}b) = e' \Rightarrow \varphi(a)^{-1}\varphi(b) = e' \Rightarrow \varphi(a) = \varphi(b)$$

(ii) $\widehat{\varphi}$ is a homomorphism: If $aH, bH \in G/H$, then

$$\widehat{\varphi}(aH * bH) = \widehat{\varphi}(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \widehat{\varphi}(aH)\widehat{\varphi}(bH)$$

(iii) $\widehat{\varphi}$ is injective: If $\widehat{\varphi}(aH) = e'$, then $\varphi(a) = e'$, so $a \in \ker(\varphi) = H$, so $aH = H$, which is the identity element in G/H. Hence,

$$\ker(\widehat{\varphi}) = \{H\}$$

so it is injective by I.5.7.

(iv) $\text{Im}(\widehat{\varphi}) = \text{Im}(\varphi)$: Obvious.

Hence,

$$\widehat{\varphi} : G/\ker(\varphi) \to \text{Im}(\varphi)$$

is a bijective homomorphism, hence an isomorphism. □

(End of Day 9)

4.3. Examples :

(i) Any cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$ for some $n \in \mathbb{N}$

Proof. Let G be a cyclic group with generator a. Define $\varphi : \mathbb{Z} \to G$ by

$$\varphi(n) := a^n$$

Then φ is a surjective homomorphism. Hence,

$$\mathbb{Z}/\ker(\varphi) \cong G$$

by the First isomorphism theorem. But $\ker(\varphi) < \mathbb{Z}$, so is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Hence,

$$G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

If $n = 0$, then $G \cong \mathbb{Z}$ □

(ii) $G = \mathbb{R}^2$, and $H = \{(a, a) : a \in \mathbb{R}\}$, then $G/H \cong \mathbb{R}$

Proof. Define $\varphi : G \to \mathbb{R}$ by $(x, y) \mapsto y - x$. Then $H = \ker(\varphi)$, and φ is clearly surjective. Hence $G/H \cong \mathbb{R}$ □

(iii) $G = \mathbb{C}^*, H = S^1$, then $G/H \cong ((0, \infty), \times)$

Proof. Let $\varphi : G \to (0, \infty)$ be $z \mapsto |z|$ □

(iv) $S_n/A_n \cong \{\pm 1\}$

Proof. Define $\varphi : S_n \to \{\pm 1\}$ be given by $\sigma \mapsto sgn(\sigma)$ □

(v) $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$

Proof. Define $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ by $A \mapsto \det(A)$ □

4.4. Proposition : Let $\varphi : G \to G'$ be a homomorphism.

(i) If $H' < G'$, then $\varphi^{-1}(H') < G$

(ii) If $H < G$, then $\varphi(H) < G'$

Proof. (i) If $x, y \in \varphi^{-1}(H')$, then $\varphi(x), \varphi(y) \in H'$, so

$$\varphi(xy^{-1}) \in H' \Rightarrow xy^{-1} \in \varphi^{-1}(H')$$

So $\varphi^{-1}(H') < G$

(ii) Similar.

□

4.5. Remark : If $H \lhd G$ and $\pi : G \to G/H$ the natural projection, then if $K' < G/H$, then $K = \pi^{-1}(K') < G$ contains H.

4.6. The Second Isomorphism Theorem : If $H \lhd G$ and $\pi : G \to G/H$ the natural projection, then there is a one-to-one correspondence

$$\{K' < G/H\} \leftrightarrow \{K < G \text{ such that } H \subset K\}$$

Proof. Let $S := \{K' < G/H\}$ and $T := \{K < G : H \subset K\}$, and define $f : S \to T$ by

$$f(K') := \pi^{-1}(K')$$

This is a well-defined function by 4.4 and 4.5.

(i) f is injective: If $f(K_1') = f(K_2')$, then $\pi^{-1}(K_1') = \pi^{-1}(K_2')$. WTS: $K_1' = K_2'$. By symmetry, it suffices to show that $K_1' \subset K_2'$, so let $xH \in K_1'$, then $x \in \pi^{-1}(K_1') = \pi^{-1}(K_2')$, so $xH = \pi(x) \in K_2'$. Thus, $K_1' \subset K_2'$.

(ii) f is surjective: If $K < G$ such that $H \subset K$, consider $K' := \pi(K) < G/H$ by 4.4. We claim that: $\pi^{-1}(\pi(K)) = K$. Fix $x \in K$, then $xH \in \pi(K)$, so $x \in \pi^{-1}(\pi(K))$. Hence,

$$K \subset \pi^{-1}(\pi(K))$$

Conversely, if $x \in \pi^{-1}(\pi(K))$, then $xH = \pi(x) \in \pi(K)$. Hence, $\exists y \in K$ such that

$$xH = yH$$

But then $xy^{-1} \in H \subset K$. Hence, $x \in K$ as required.

□

4.7. Example : For $n \in \mathbb{N}$ fixed

$$\{\text{subgroups of } \mathbb{Z}_n\} \leftrightarrow \{\text{divisors of } n\}$$

Proof. We know that

$$\{\text{subgroups of } \mathbb{Z}_n\} \leftrightarrow \{\text{subgroups of } \mathbb{Z} \text{ containing } n\mathbb{Z}\}$$

But if $H < \mathbb{Z}$ such that $nZ \subset H$, then $H = d\mathbb{Z}$ for some $d \in \mathbb{Z}$ and $n \in d\mathbb{Z}$, whence $d \mid n$. Conversely, if $d \mid n$, then $n \in d\mathbb{Z}$ whence $n\mathbb{Z} \subset d\mathbb{Z}$. Hence the result.

□

(End of Day 10)

5. Modular Arithmetic : The Units

5.1. Lemma : Let $n \in \mathbb{N}$ fixed. If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then

$$ab = cd \pmod{n}$$

Proof. If $a = c + nk$ and $b = d + n\ell$, then

$$ab = cd + nkd + n\ell c + n^2 k\ell$$

□

5.2. Definition : For $[a], [b] \in \mathbb{Z}_n$, $[a] \times [b] = [ab]$ is well-defined.

Note: $(\mathbb{Z}_n, \times)$ is not a group because $[0]$ does not have a multiplicative inverse.

5.3. Lemma : If $a \equiv c \pmod{n}$ and $(a, n) = 1$, then $(c, n) = 1$.

Proof. By I.2.4, $\exists s, t \in \mathbb{Z}$ such that $as + tn = 1$. Also, $\exists k \in \mathbb{Z}$ such that $a = c + kn$. Hence,

$$cs + (ks + t)n = 1$$

and hence $(c, n) = 1$. □

5.4. Definition :

(i) $\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n : (a, n) = 1\}$ [Note: This is well-defined by 5.3.]

(ii) $\varphi(n) = |\mathbb{Z}_n^*|$ is called the *Euler Phi function*

5.5. Theorem : $(\mathbb{Z}_n^*, \times)$ is a group, called the *group of units modulo n*

Proof. (i) Closure: If $[a], [b] \in \mathbb{Z}_n^*$, then $(a, n) = (b, n) = 1$, so $\exists s_1, t_1 \in \mathbb{Z}$ such that

$$as_1 + nt_1 = 1$$

Similarly, $\exists s_2, t_2 \in \mathbb{Z}$ such that

$$bs_2 + nt_2 = 1$$

Multiplying, we see that

$$abs_1s_1 + n(as_1t_2 + bs_2t_1 + nt_1t_2) = 1$$

and so $(ab, n) = 1$

(ii) Associativity: Follows from associativity of multiplication of integers.

(iii) Identity: $[1] \in \mathbb{Z}_n^*$

(iv) Inverse: If $(a, n) = 1$, then $\exists b, t \in \mathbb{Z}$ such that

$$ab + tn = 1$$

But then $(b, n) = 1$ and clearly $[ab] = [1]$ in $\mathbb{Z}_n^*$. Hence, $[a] \times [b] = [1]$.

□

5.6. Examples :

(i) If p prime, then $\mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\}$, $\varphi(p) = p - 1$

(ii) If p prime, then $[a] \in \mathbb{Z}_{p^k}$ iff $p \nmid a$. Hence, $\varphi(p^k) = p^k - p^{k-1}$

(iii) $\mathbb{Z}_8^*$ is not cyclic.

Proof. Write $\mathbb{Z}_8^* = \{[1], [3], [5], [7]\}$, and note that

$$[3]^2 = [9] = [1], [5]^2 = [25] = [1], \text{ and } [7]^2 = [49] = [1]$$

Hence there is no element of order 4. □

(iv) $\mathbb{Z}_{p^k}^*$ is cyclic if p odd prime, $k \in \mathbb{N}$ (Proof Later)

5.7. Euler's theorem : If $n \in \mathbb{N}$ and $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

Proof. Because $\varphi(n) = |\mathbb{Z}_n^*|$, this follows from Corollary 2.7. □

5.8. Fermat's Little Theorem : If $a \in \mathbb{Z}$ and p a prime, then $a^p \equiv a \pmod{p}$

Proof. Because $\varphi(p) = p - 1$, $a^{p-1} \equiv 1 \pmod{p}$, so multiply both sides by a, and use Lemma 5.1. □

III. Symmetry

(See [Artin, §6])

1. Isometries of $\mathbb{R}^n$

1.1. Motivation : Recall

(i) D_n = symmetries of regular $n-$gon

(ii) V_4 = symmetries of water molecule

More generally, if $\Delta \subset \mathbb{R}^n$, we are interested in the symmetries of Δ

Examples :

(i) [Human figure] has only one non-trivial symmetry, namely reflection.

(ii) [Square] has 8 symmetries, the group D_4

(iii) [Infinite arrows] has infinitely many symmetries - translation by any $k \in \mathbb{Z}$

(iv) [Glide symmetry] has infinitely many symmetries - translation + flip

(v) [Sphere] has infinitely many symmetries - all rotations, and reflections

(vi) [Cube] has finitely many - some reflections, some rotations. How many are there?

(End of Day 11)

1.2. Definition :

(i) For $x = (x_i), y = (y_i) \in \mathbb{R}^n$,

$$\langle x, y \rangle := \sum_{i=1}^{n} x_i y_i$$

and

$$|x - y| := \sqrt{\sum_{i=1}^{n} (x_i - y_i^2} = \langle x - y, x - y \rangle^{1/2}$$

(ii) An isometry of $\mathbb{R}^n$ is a map $T : \mathbb{R}^n \to \mathbb{R}^n$ such that

$$|T(x) - T(y)| = |x - y| \quad \forall x, y \in \mathbb{R}^n$$

(iii) E_n is the set of isometries of $\mathbb{R}^n$. Note : We will show that E_n is a group, called the *Euclidean Group*

1.3. Examples :

(i) Translation $\tau_b : x \mapsto x + b$ for any fixed $b \in \mathbb{R}^n$

(ii) An orthogonal linear operator $T : \mathbb{R}^n \to \mathbb{R}^n$ has the property that $\langle Tx, Ty \rangle = \langle x, y \rangle$. Hence $|T(x) - T(y)| = |x - y|$ so T is an isometry.

(iii) The composition of two isometries is an isometry. Hence, if $A \in \mathcal{O}_n(\mathbb{R})$ and $b \in \mathbb{R}^n$, then the map $g : \mathbb{R}^n \to \mathbb{R}^n$ given by

$$g(x) = Ax + b$$

is an isometry.

1.4. Lemma : Let $u, v \in \mathbb{R}^n$ such that $\langle u, u \rangle = \langle v, v \rangle = \langle u, v \rangle$, then $u = v$

Proof. Consider

$$\langle u - v, u - v \rangle = \langle u, u \rangle - 2\langle u, v \rangle + \langle v, v \rangle = 0$$

Hence $u = v$. □

1.5. Theorem : Let $g \in E_n$ such that $g(0) = 0$, then $\exists A \in O_n(\mathbb{R})$ such that $g(x) = Ax$ for all $x \in \mathbb{R}^n$

Proof. (i) g preserves dot products: If $x, y \in \mathbb{R}^n$ then $\langle g(x), g(y) \rangle = \langle x, y \rangle$. Since g is an isometry with $g(0) = 0$, we have

$$\langle g(x) - g(y), g(x) - g(y) \rangle = |g(x) - g(y)|^2 = |x - y|^2 = \langle x - y, x - y \rangle$$

In particular,

$$\langle g(x), g(x) \rangle = \langle x, x \rangle \text{ and } \langle g(y), g(y) \rangle = \langle y, y \rangle$$

Expanding out the first equation, we get

$$\langle g(x), g(y) \rangle = \langle x, y \rangle$$

(ii) g is additive: If $x, y \in \mathbb{R}^n$, then $g(x) + g(y) = g(x + y)$. Let $z := x + y$, and let

$$u = g(z) = g(x + y) \text{ and } v = g(x) + g(y)$$

To show $u = v$, it suffices by Lemma 1.4 to show that

$$\langle u, u \rangle = \langle v, v \rangle = \langle u, v \rangle$$

So note that

$$\begin{aligned}
\langle u, u \rangle &= \langle g(z), g(z) \rangle = \langle z, z \rangle \\
&= \langle x, x \rangle + 2\langle x, y \rangle + \langle y, y \rangle \\
&= \langle g(x), g(x) \rangle + 2\langle g(x), g(y) \rangle + \langle g(y), g(y) \rangle \\
&= \langle g(x) + g(y), g(x) + g(y) \rangle = \langle v, v \rangle
\end{aligned}$$

Also, consider

$$\begin{aligned}\langle u, v\rangle &= \langle g(z), g(x) + g(y)\rangle \\ &= \langle g(z), g(x)\rangle + \langle g(z), g(y)\rangle \\ &= \langle z, x\rangle + \langle z, y\rangle \\ &= \langle z, x + y\rangle \\ &= \langle g(x + y), g(x + y)\rangle = \langle u, u\rangle\end{aligned}$$

Hence g is additive.

(iii) $g(\lambda x) = \lambda g(x)$ for all $x \in \mathbb{R}^n, \lambda \in \mathbb{R}$: Let $z = \lambda x$, then we WTS:

$$g(z) = \lambda g(x)$$

so let $u = g(z), v = \lambda g(x)$, and check

$$\begin{aligned}\langle u, u\rangle &= \langle g(z), g(z)\rangle = \langle z, z\rangle \\ &= \langle \lambda x, \lambda x\rangle = \lambda^2\langle x, x\rangle \\ &= \lambda^2\langle g(x), g(x)\rangle \\ &= \langle \lambda g(x), \lambda g(x)\rangle = \langle v, v\rangle\end{aligned}$$

and similarly, $\langle u, v\rangle = \langle u, u\rangle$

(iv) Hence, g is linear and preserves the dot product. By I.4.2, $g(x) = Ax$ for some $A \in O_n(\mathbb{R})$.

□

1.6. Corollary : If $g \in E_n$, then $\exists A \in O_n(\mathbb{R})$ and $b \in \mathbb{R}^n$ such that $g(x) = Ax + b$ for all $x \in R^n$

Proof. Consider $b := g(0)$, then $h(x) := g(x) - b$ is also an isometry, and satisfies $h(0) = 0$. By Theorem 1.5, $\exists A \in O_n(\mathbb{R})$ such that $h(x) = Ax$, so that $g(x) = Ax+b$ for all $x \in \mathbb{R}^n$. □

1.7. Corollary : Every $g \in E_n$ is bijective, and E_n is a group.

Proof. (i) If $g \in E_n$, then write $g(x) = Ax + b$ as above. Define

$$h(x) := A^{-1}(x - b) = A^{-1}x - A^{-1}b$$

Then $h \in E_n$ by Example 1.3(iii). Furthermore,

$$g(h(x)) = Ah(x) + b = (x - b) + b = x$$

Hence, $gh = \mathrm{id}_{\mathbb{R}^n}$. Similarly, $hg = \mathrm{id}_{\mathbb{R}^n}$, so g is bijective.

(ii) Clearly, E_n is now a group under composition with identity $\mathrm{id}_{\mathbb{R}^n}$.

□

1.8. Remark: Note that if $A \in O_n(\mathbb{R})$, we get a unique isometry $T_A \in E_n$ given by $T_A(x) = A(x)$. This map

$$A \mapsto T_A$$

is an injective group homomorphism. Therefore, we identify $O_n(\mathbb{R})$ with its image in E_n.

1.9. Theorem : There is a surjective homomorphism $\pi : E_n \to O_n$ such that $\ker(\pi) \cong \mathbb{R}^n$. Thus

$$E_n/\mathbb{R}^n \cong O_n(\mathbb{R})$$

Proof. Define $\pi : E_n \to O_n$ by

$$\pi(g) := \tau_{-g(0)} \circ g$$

Then

(i) π is well-defined: If $g \in E_n$, then $h := \tau_{-g(0)} \circ g$ has the property that $h(0) = g(0) - g(0) = 0$, and so $h \in O_n(\mathbb{R})$ by 1.5.

(ii) If $h \in O_n(\mathbb{R})$ and $b \in \mathbb{R}^n$, then

$$h \circ \tau_b(x) = h(x + b) = h(x) + h(b) = \tau_{h(b)} \circ h(x)$$

and so $h \circ \tau_b = \tau_{h(b)} \circ h$

(iii) π is a homomorphism: If $g_1, g_2 \in E_n$, then let $h_i := \pi(g_i)$, then

$$g_1 = \tau_{a_1} \circ h_1 \text{ and } g_2 = \tau_{a_2} \circ h_2$$

and $h_i \in O_n(\mathbb{R})$. Hence,

$$g_1 g_2 = \tau_{a_1} h_1 \tau_{a_2} h_2 = \tau_{a_1} \tau_{h_1(a_2)} h_1 h_2 = \tau_{a_1 + h_1(a_2)} h_1 h_2$$

Also, $g_1 g_2(0) g_1(g_2(0)) = g_1(a_2) = \tau_{a_1}(h_1(a_2)) = h_1(a_2) + a_1$. Hence,

$$\pi(g_1 g_2) = h_1 h_2$$

as required.

(iv) π is surjective: Clearly, because $O_n(\mathbb{R}) \subset E_n$ as in Remark 1.8.

(v) $\ker(\pi) \cong \mathbb{R}^n$: By definition, $g \in \ker(\pi)$ iff $\exists b \in \mathbb{R}^n$ such that $g = \tau_b$. Hence,

$$\ker(\pi) = \{\tau_b : b \in \mathbb{R}^n\}$$

The map $b \mapsto \tau_b$ is a group isomorphism from $\mathbb{R}^n$ to $\ker(\pi)$ [Check!]

□

(End of Day 12)

2. Symmetries of Platonic Solids

2.1. Definition: A polyhedron is a region in $\mathbb{R}^3$ bounded by planes. It is said to be regular if all its faces, edges and vertices are equal. This implies that each face is the same regular polygon. There are exactly five such objects, the Platonic solids

(i) Tetrahedron (T): 4 faces.

(ii) Cube (C): 6 faces.

(iii) Octahedron (O): 8 faces.

(iv) Dodecahedron (D): 12 faces.

(v) Icosahedron (I): 20 faces.

Imagine each embedded in the unit sphere $S^2 \subset \mathbb{R}^3$

2.2. Definition : Given $\Delta \subset \mathbb{R}^n$, $M(\Delta) = \{g \in M(\mathbb{R}^n) : g(\Delta) = \Delta\}$ is called the (full) group of symmetries of Δ. Note : This does not mean that $g(x) = x$ for all $x \in \Delta$.

2.3. Remark : Let Δ be a platonic solid. Then

(i) $M(\Delta) \cap \ker(\pi) = \{e\}$, and so $\pi : M(\Delta) \to \pi(M(\Delta))$ is an isomorphism

(ii) Reflection about a plane is a physical impossibility. In fact, any isometry that "switches" two axes is not physically possible in $\mathbb{R}^3$. We are only going to be interested in those symmetries which preserve the order of the axes, which happens iff $det(g) = +1$

2.4. Definition : For $\Delta \subset \mathbb{R}^n$ with $M(\Delta) < O_n(\mathbb{R})$, we write

$$G(\Delta) = \pi(M(\Delta)) \cap SO_n(\mathbb{R}) = \{g \in SO_3(\mathbb{R}) : g(\Delta) = \Delta\}$$

for the group of rotational (or *orientation-preserving*) symmetries of Δ

2.5. Example : Let $\Delta = T =$The tetrahedron

(i) $G(T)$ permutes the set $X = \{v_1, v_2, v_3, v_4\}$ of vertices.

(ii) $G(T)$ has 12 elements, because any rotation must send v_1 to four possible vertices, v_2 to any of the remaining three, and then the last two positions are determined.

2.6. Lemma : There is an injective homomorphism $f : G(T) \to S_X$ where $f(g) = \sigma_g$ as above.

Proof. Given $g \in G(T)$, consider $X \subset T$, then g must permute X. Hence, define

$$\sigma_g := g|_X \colon X \to X$$

Clearly, $\sigma_g \in S_X$ because g is bijective, and maps X to X. Hence, $f : G(T) \to S_X$ given by $f(g) = \sigma_g$ is well-defined. It is clearly a homomorphism because the operation on both sides is composition.

Finally, f is injective, because if $\sigma_g = \mathrm{id}_X$, then g fixes all vertices, hence all edges, and hence all faces. Thus, $g = \mathrm{id}_T$. $\square$

2.7. Theorem : $G(T) \cong A_4$

Proof. We identify $G(T) \cong f(G(T)) < S_4$, and list out the elements:

(i) The identity $e \in G(T)$

(ii) If 1 is fixed, we get two non-trivial rotations:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

(iii) Similarly, if two rotations each when each vertex is fixed. So far we have 9 elements.

(iv) Consider the product

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

This is an element of order 2, therefore not in our list yet. Similarly, we get two more elements of order 2 of the form

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Thus, we get 12 elements. This must exhaust all of $G(T)$.

(v) Now observe that all these elements are in A_4. Furthermore, $|A_4| = 24/2 = 12$, so this exhausts A_4.

□

(End of Day 13)

2.8. Example : Let $\Delta = C =$The cube

(i) $G(C)$ has 24 elements: There are 8 choices for the first vertex, three subsequent choices for an adjacent second vertex (because vertex 2 must be connected to vertex 1 by an edge). Finally, there are two choices for vertex 3 (adjacent to vertex 1) because it must remain adjacent to vertex 1, but cannot go where vertex 2 has gone. However, if we consider only orientation preserving maps, then there is only one choice. Hence, there are $8 \times 3 = 24$ such symmetries.

(ii) $G(C)$ permutes the set $X = \{D_1, D_2, D_3, D_4\}$ of principal diagonals

2.9. Theorem : $G(C) \cong S_4$

Proof. Let $X = \{D_1, D_2, D_3, D_4\}$ denote the set of principal diagonals. Then $G(C)$ permutes X, so, as before, we get a group homomorphism

$$f : G(C) \to S_X$$

which is injective. Since $|G(C)| = 24 = |S_X|$, it follows that f is an isomorphism. □

2.10. Remark :

(i) An octahedron can be obtained from a cube by joining mid-points of adjacent faces and filling up the solid. We say that O is dual to C. This implies that$O$ has the same group of symmetries as C. ie. $G(O) \cong S_4$

(ii) Similarly, the dodecahedron D is dual to the icosahedron I. Hence, $G(D) \cong G(I)$. We will discuss this group later.

(iii) The tetrahedron is dual to itself.

3. Group Actions

3.1. Definition : Let G be a group, and X any set. We say that G acts on X if there is a function

$$\alpha : G \times X \to X$$

such that, for all $g_1, g_2 \in G$ and $x \in X$

$$\alpha(e, x) = x \text{ and } \alpha(g_1 g_2, x) = \alpha(g_1, \alpha(g_2, x))$$

If this happens, we write $G \curvearrowright_\alpha X$, or just $G \curvearrowright X$. Furthermore, we write

$$g \cdot x := \alpha(g, x)$$

3.2. Examples :

(i) $G(T)$ acts on the set of vertices of T

(ii) $G(C)$ acts of the set of principal diagonals of C

(iii) D_n acts on the set of vertices of a regular n-gon.

(iv) $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by $(A, x) \mapsto A(x)$. Similarly, $SL_n(\mathbb{R}), O_n(\mathbb{R})$ and $SO_n(\mathbb{R})$ act on $\mathbb{R}^n$

(v) S_n acts on $\{1, 2, \ldots, n\}$

(vi) Any group G acts on itself by the *left regular action* [See HW 2]

3.3. Lemma (Permutation Representation) : If G acts on X, then there is a homomorphism, $G \to S_X$

Proof. Given a group action $\alpha : G \times X \to X$, let $g \in G$, and define $\sigma_g : X \to X$ by

$$\sigma_g(x) := \alpha(g, x)$$

Then

(i) $\sigma_g \in S_X$: Note that

$$\sigma_{g^{-1}} \circ \sigma_g(x) = \sigma_{g^{-1}}(\alpha(g, x)) = \alpha(g^{-1}, \alpha(g, x)) = \alpha(gg^{-1}, x) = \alpha(e, x) = x$$

Hence, $\sigma_{g^{-1}} \circ \sigma_g = \mathrm{id}_X$. Similarly,

$$\sigma_g \circ \sigma_{g^{-1}} = \mathrm{id}_X$$

Hence, $\sigma_g \in S_X$.

(ii) Define $f : G \to S_X$ by $f(g) = \sigma_g$. As in the previous step, it follows that

$$\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}$$

so f is a homomorphism.

□

3.4. Definition : Let $G \curvearrowright X$

(i) For $x, y \in X$, write $x \sim y$ iff $\exists g \in G$ such that $y = g \cdot x$. This is an equivalence relation on X. [Why?]

(ii) For $x \in X$, the orbit of x is the set

$$\mathcal{O}(x) := \{g \cdot x : g \in G\}$$

Note : Orbits partition X (See II.1.4)

(iii) We say that the action is transitive if it has exactly one orbit. ie. For any $x, y \in X, \exists g \in G$ such that $y = g \cdot x$.

(End of Day 14)

3.5. Examples :

(i) $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ as before. Then the orbit of the origin is the origin itself. The orbit of any other point is $\mathbb{R}^n \setminus \{0\}$

(ii) $SO_2(\mathbb{R})$ acts on $\mathbb{R}^2$. If $x \sim y$, then $|x| = |y|$, and so the orbit of any point $x \in \mathbb{R}^2$ is the circle of radius $|x|$

(iii) S_n acts transitively on $\{1, 2, \ldots, n\}$

3.6. Definition : For $x \in G$, the stabilizer of x is

$$Stab(x) := \{g \in G : g \cdot x = x\}$$

Note that $Stab(x) < G$.

3.7. Proposition : Let $G \curvearrowright X$. Let $x \in X$ and $H = Stab(x)$. Then there is a bijection $\eta : G/H \to \mathcal{O}(x)$

Proof. Define $\eta : G/H \to \mathcal{O}(x)$ by

$$gH \mapsto g \cdot x$$

(i) η is well-defined: If $g_1 H = g_2 H$, then $g_1^{-1} g_2 \in H = Stab(x)$, so $(g_1^{-1} g_2) \cdot x = x$, so (applying g_1 to both sides),

$$g_1 \cdot x = g_2 \cdot x$$

(ii) η is surjective: Obvious.

(iii) η is injective: If $g_1 \cdot x = g_2 \cdot x$, then $(g_2^{-1} g_1) \cdot x = x$, whence $g_2^{-1} g_1 \in H$, so

$$g_1 H = g_2 H$$

□

3.8. (Orbit-Stabilizer Theorem) Let G be a finite group acting on a set X. Let $x \in X$, then $|G| = |\mathcal{O}(x)||Stab(x)|$. In particular, if G acts transitively on X, then $|G| = |X||Stab(x)|$

Proof. Let $H := Stab(x)$, then by Lagrange's theorem and 3.7,

$$|\mathcal{O}(x)| = |G/H| = [G : H] = \frac{|G|}{|H|}$$

□

3.9. Example : Let D be the regular dodecahedron, then $|G(D)| = 60$

Proof. The dodecahedron has 12 faces, each of which is a pentagon. Let $x \in D$ be the center of one such face, then $\mathcal{O}(x)$ consists of the centers of all the faces of D. Hence,

$$|\mathcal{O}(x)| = 12$$

Also, $Stab(x)$ consists of those elements $g \in G$ that fix x, and hence the face containing x. The only such elements are elements that rotate the pentagon, and there are five such elements.

$$|Stab(x)| = 5$$

So by the Orbit-Stabilizer theorem, $|G(D)| = 60$. □

4. Cayley's Theorem

4.1. Remark : G acts on itself by left multiplication by the formula

$$g \cdot h := gh$$

4.2. Cayley's Theorem : Let G be a finite group with $n = |G|$, then G is isomorphic to a subgroup of S_n

Proof. Let $f : G \to S_G \cong S_n$ be the group homomorphism induced by the left-multiplication action. We claim that f is injective. Suppose $g \in \ker(f)$, then

$$\sigma_g = \mathrm{id}_G$$

In other words, for any $h \in H$

$$h = \sigma_g(h) = g \cdot h = gh$$

By cancellation, this implies $g = e$, so $\ker(f) = \{e\}$ as required. Hence, $f : G \to \mathrm{Image}(f) < S_n$ is an isomorphism. □

4.3. Definition: Let G be a group, and $H < G$. Let $X = G/H$, then G acts on X by left multiplication.

$$g \cdot (xH) := (gx)H$$

Let $f_H : G \to S_X$ be the induced permutation representation.

4.4. Lemma : $\ker(f_H) \subset H$

Proof. Let $g \in \ker(f_H)$, then $\sigma_g = \mathrm{id}_{G/H}$. In other words,

$$g \cdot (xH) = xH \quad \forall xH \in G/H$$

In particular, this implies

$$gH = g \cdot (eH) = eH = H$$

and so $g \in H$. □

4.5. Lemma : Let G be a finite group, and $K < H < G$, then $[G : K] = [G : H][H : K]$

Proof. By Lagrange's theorem, $[G : H] = |G|/|H|$. So

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G : H][H : K]$$

□

4.6. (Strong Cayley Theorem) Let G be a finite group, and p the smallest prime dividing $|G|$. Then any subgroup of index p is normal in G. In particular, any subgroup of index 2 is normal in G.

Proof. Let $H < G$ such that $[G : H] = p$ where p is the smallest prime dividing $|G|$. Consider the map

$$f_H : G \to S_p$$

as above, then by the first isomorphism theorem,

$$G/\ker(f_H) : G \cong \mathrm{Image}(f_H) < S_p$$

By Lagrange,

$$|\mathrm{Image}(f_H)| \mid p!$$

But $|\mathrm{Image}(f_H)| = [G : \ker(f_H)] \mid |G|$. Hence,

$$|\mathrm{Image}(f_H)| \mid gcd(|G|, p!) = p$$

Since p is prime, $|\mathrm{Image}(f_H)| = p$ or 1. Hence,

$$[G : \ker(f_H)] \in \{p, 1\}$$

But $\ker(f_H) \subset H$, so

$$[G : \ker(f_H)] = [G : H][H : \ker(f_H)] = p[H : \ker(f_H)] \geq p$$

Hence, $[G : \ker(f_H)] = p$, whence $[G : \ker(f_H)] = [G : H]$, so that $[H : \ker(f_H)] = 1$. Hence,

$$H = \ker(f_H) \lhd G$$

□

(End of Day 15)

5. The Class Equation

5.1. Definition :

(i) Define $\alpha : G \times G \to G$ by

$$\alpha(g, h) := ghg^{-1}$$

Then α is a group action of G on G, called the conjugation action.

(ii) Two elements $x, y \in G$ are conjugate iff $\exists g \in G$ such that $y = gxg^{-1}$ (ie. they lie in the same orbit)

5.2. Examples :

(i) Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be an invertible linear operator, and A_1, A_2 be two representations of T w.r.t two different bases, then A_1 is conjugate to A_2 in $GL_n(\mathbb{R})$

(ii) Let $G = M(\mathbb{R}^2), x = \rho_\theta, g = \tau_v$, then gxg^{-1} is the rotation by θ about v

(iii) Let $G = D_3, x =$ the reflection about v_1, $g =$ rotation by 120 degrees clockwise, then gxg^{-1} is the reflection about v_3. ie. Conjugation is "looking at the group from different perspectives/change of coordinates in the group"

5.3. Definition : G a group, $x \in G$

(i) The conjugacy class of x in G is

$$C(x) := \{gxg^{-1} : g \in G\} = \mathcal{O}(x)$$

(ii) The centralizer of x in G is

$$Z(x) := \{g \in G : gxg^{-1} = x\} = Stab(x)$$

5.4. Remark : Let G be a finite group

(i) By the orbit-stabilizer theorem, $|G| = |Z(x)||C(x)|$

(ii) In particular, for any $x \in G, |C(x)| \mid |G|$

(iii) By 3.4, G is partitioned into conjugacy classes. Hence

$$|G| = |C(x_1)| + |C(x_2)| + \ldots + |C(x_n)|$$

where the sum is taken over all distinct conjugacy classes

(iv) $|C(x)| = 1$ iff $gxg^{-1} = x$ for all $g \in G$. Equivalently, $|C(x)| = 1$ iff $xg = gx$ for all $g \in G$

5.5. Definition : The Center of the group is

$$Z(G) = \{x \in G : gx = xg \quad \forall g \in G\}$$

5.6. Remark :

(i) $Z(G) \lhd G$ (HW)

(ii) $Z(G) = G$ iff G is abelian

(iii) $x \in Z(G)$ iff $|C(x)| = 1$

5.7. (The class equation) : Let G be a finite group, then

$$|G| = |Z(G)| + \sum_{|C(x_i)|>1} |C(x_i)|$$

where the sum on the RHS is taken over all distinct conjugacy classes whose cardinality is > 1. Furthermore, each term on the RHS divides $|G|$

Proof. We simply take the equation

$$|G| = |C(x_1)| + |C(x_2)| + \ldots + |C(x_n)|$$

Each term on the RHS equal to one constitutes an element of $Z(G)$, so we collect all these terms to get $|Z(G)|$. □

5.8. Corollary : Let G be a group such that $|G| = p^n$, where p is prime, then $Z(G) \neq \{e\}$

Proof. If $x \in G$ such that $|C(x)| > 1$, then $|C(x)| \mid |G|$, so $p \mid |C(x)|$. Hence, the class equation reads

$$|G| \equiv |Z(G)| \pmod{p}$$

Since $|G| \equiv 0 \pmod{p}$, it follows that $p \mid |Z(G)|$. Hence, $Z(G) \neq \{e\}$. □

5.9. Lemma : If $G/Z(G)$ is cyclic, then G is abelian. [HW]

5.10. Theorem : If $|G| = p^2$, where p is prime, then G is abelian

Proof. By Corollary 5.8, $|Z(G)| \in \{p, p^2\}$. If $|Z(G)| = p^2$, then $G = Z(G)$, so G is Abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic, whence G is abelian. Thus, $Z(G) = G$, so this is not possible. □

6. The Icosahedral Group

(See [Artin, §7.4])

6.1. Remark : $G(D)$ is the group of rotational symmetries of a regular dodecahedron. Note that D has 20 vertices, 12 faces and 30 edges.

(i) By 3.9, $|G(D)| = 60$

(ii) What are these elements?

(a) The identity (1)

(b) Rotation by $2\pi/3$ about every vertex (+20)

(c) Rotation by π about the centre of an edge. There are 30 edges, but each such rotation accounts for 2 edges (+15)

(d) Rotation by $2\pi/5$ about the centre of a face (+12) [This accounts for a rotation by $8\pi/5$]

(e) Rotation by $4\pi/5$ about the centre of a face (+12) [This accounts for a rotation by $6\pi/5$]

(End of Day 16)

6.2. Lemma : Let $x = \rho_{u,\alpha} \in SO_3(\mathbb{R})$

(i) $trace(x) = 1 + 2\cos(\alpha)$

(ii) Let $g \in SO_3(\mathbb{R})$ and $v = g(u)$, then $gxg^{-1} = \rho_{v,\alpha}$

Proof. (i) HW

(ii) Note that $gxg^{-1}(v) = v$. Let α' be the angle of rotation of gxg^{-1}, then

$$1 + 2\cos(\alpha') = Tr(gxg^{-1}) = Tr(x) = 1 + 2\cos(\alpha)$$

Hence, $\alpha' = \pm\alpha$. WTS: $\alpha' = \alpha$. So write $g = \rho_{w,\theta}$, and define a continuous function $f : [0,1] \to SO_3(\mathbb{R})$ by

$$f(t) = \rho_{w,t\theta} x \rho_{w,t\theta}^{-1}$$

Note that $f(0) = \rho_{w,0} x \rho_{w,0}^{-1} = IxI^{-1} = x$ and $f(1) = gxg^{-1}$. Since the angle of rotation is continuous along this path, and takes only two values $\{\pm\alpha\}$, it must be constant. Hence, $\alpha' = \alpha$.

□

6.3. Remark (Class Equation of $G(D)$)

(i) If $e \in G(D)$ is the identity, then $|C(e)| = 1$

(ii) If u is a vertex, $\alpha = 2\pi/3$, let $x_1 = \rho_{u,\alpha}$, then $|C(x_1)| = 20$

Proof. If $g \in G(D)$, then $gx_1g^{-1} = \rho_{u',\alpha}$ for some other vertex u'. There are 20 such vertices. Furthermore, if v is any other vertex, $\exists g \in G(D)$ such that $g(u) = v$, so $|C(x_1)| = 20$. □

(iii) If e is the centre of an edge, and $\alpha = \pi$, let $x_2 = \rho_{e,\alpha}$, then $|C(x_2)| = 15$

Proof. If $g \in G(D)$, then $gx_2g^{-1} = \rho_{e',\alpha}$ for some other mid-point e' of and edge of D. Potentially, this give 30 elements, but

$$\rho_{e,\pi} = \rho_{-e,-\pi}$$

so we get only 15 rotations. □

(iv) If f is the centre of a face, and $\alpha = 2\pi/5$, let $x_3 = \rho_{f,\alpha}$, then $|C(x_3)| = 12$

Proof. If $g \in G(D)$, then $gx_3xg^{-1} = \rho_{f',2\pi/5}$ for some other centre f' of a face of D. There are 12 such faces. □

(v) Similarly, If f is the centre of a face, and $\alpha = 4\pi/5$, let $x_4 = \rho_{f,\alpha}$, then $|C(x_4)| = 12$.

So the class equation is : $60 = 1 + 20 + 15 + 12 + 12$

6.4. Lemma : Let G be a group, $N \lhd G$, then

(i) If $x \in N$, then $C(x) \subset N$

(ii) $|N|$ is the sum of the cardinalities of disjoint conjugacy classes in G

Proof. (i) If $x \in N$ and $g \in G$, then $gxg^{-1} \in N$, so $C(x) \subset N$.

(ii) For any $x \in G$, it follows that

$$C(x) \cap N = \emptyset \text{ or } C(x) \subset N$$

Hence, N is the disjoint union of conjugacy classes in G.

□

6.5. Definition : A group G is said to be simple if it contains no non-trivial normal subgroups. ie. $\{e\}$ and G are the only normal subgroups of G.

6.6. Theorem : $G(D)$ is a simple group

Proof. If $N \lhd G(D)$, then $|N| \mid 60$, and $|N|$ must be 1+ a sum of some subset of $\{20, 15, 12, 12\}$. This is impossible unless $|N| = 1$ or $|N| = 60$. □

(End of Day 17)

6.7. Theorem : $G(D) \cong A_5$. In particular, A_5 is a simple group.

Proof. Let X denote the set of 5 cubes embedded in the dodecahedron. Then G acts on X, so this gives a group homomorphism $f : G \to S_5$. Since G acts non-trivially on X, it follows that f is not constant. Since G is simple, $\ker(f) = \{e\}$, so f is injective. Hence, we get an isomorphism

$$f : G \to \text{Image}(f)$$

We claim that $\text{Image}(f) = A_5$.

Since $|\text{Image}(f)| = |G| = 60 = |A_5|$, it suffices to show that $\text{Image}(f) \subset A_5$. Now consider $sgn \circ f : G \to \{\pm 1\}$. Since $|G| = 60$, this map cannot be injective. Since G is simple, it must happen that $\ker(sgn \circ f) = G$. Hence, $\text{Image}(f) \subset A_5$ as required. □

7. Conjugation in S_n and A_n

7.1. Definition : Fix $n \in \mathbb{N}$ and $m \leq n$

(i) An m-cycle in S_n is a permutation $\sigma \in S_n$ such that, there is a subset $\{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$ such that

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{m-1}) = a_m, \sigma(a_m) = a_1$$

and furthermore, $\sigma(j) = j$ if $j \notin \{a_1, a_2, \ldots, a_m\}$. We write such an m-cycle as

$$(a_1 a_2 \ldots a_m)$$

Note that any cyclic permutation of this symbol also represents the same element.

(ii) Two cycles $(a_1 a_2 \ldots a_m)$ and $(b_1 b_2 \ldots b_k)$ are said to be disjoint if

$$\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots, b_k\} = \emptyset$$

(iii) The length of a cycle

(iv) A 2 cycle is called a transposition.

7.2. Proposition : Every $\sigma \in S_n$ can be written as a product of disjoint cycles.

Proof. Given $\sigma \in S_n$, follow the algorithm given below:

(i) Start with $x_1 := 1 \in \{1, 2 \ldots, n\} =: X$ and let $a_1 = \sigma(1)$. This starts a new cycle

$$(1 a_2$$

(ii) Determine $a_k = \sigma^k(1)$. Since σ has finite order, $\exists k \in \mathbb{N}$ such that $\sigma^k(1) = 1$ and $\sigma^j(1) \neq 1$ if $j < k$. Consider the set

$$S_1 = \{1, a_1, a_2, \ldots, a_{k-1}\}$$

If $a_i = a_j$ for $0 \leq i, j \leq k-1$, then $\sigma^{j-i}(1) = 1$ must hold. This is impossible by minimality of k, so these k elements are distinct. This is the first cycle

$$\sigma_1 := (1 a_1 a_2 \ldots a_{k-1})$$

(iii) If $S = X$, then stop, else choose $x_2 \in X \backslash S$ which is smallest with this property. Repeat the above 3 steps. If $\sigma^i(x_2) = \sigma^j(x_1)$, then $x_2 \in S$ must hold. Thus, the corresponding set S_2 must be disjoint from S_1. This gives a second cycle σ_2

(iv) Continue this process until we exhaust all of X. This must happen because $|X| < \infty$. Now we have obtained disjoint cycles $\sigma_1 \sigma_2 \ldots \sigma_k$.

(v) Finally, remove all cycles of length 1.

Claim : $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$ To see this, choose $x \in X$, then $\exists 1 \leq j \leq k$ such that $x \in S_j$. Write $x = \sigma^\ell(x_j)$, then

$$\sigma(x) = \sigma^{\ell+1}(x_j) = \sigma_j(x)$$

Since the other σ_i are disjoint, $\sigma_i(x) = x$ and $\sigma_i(\sigma(x)) = x$ for all $i \neq j$. Hence,

$$\sigma(x) = \sigma_1\sigma_2 \dots \sigma_k(x)$$

This is true for all $x \in X$ as required. $\square$

7.3. Remark:

(i) Let $\sigma \in S_n$ and $H := \langle \sigma \rangle$. Then H acts on $X = \{1, 2 \dots, n\}$, so X decomposes as a disjoint union or orbits under this action. These orbits are precisely the sets S_j constructed above.

(ii) Example: If $\sigma \in S_{10}$ is given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 1 & 5 & 6 & 7 & 9 & 10 & 3 & 8 \end{pmatrix}$$

Then

$$\sigma = (1, 2, 4, 5, 6, 7, 9, 3)(8, 10)$$

(End of Day 18)

(iii) Disjoint cycles commute.

(iv) The cycle decomposition is unique upto order in which the elements are written, and upto cyclic permutation of a cycle.

(v) If $\sigma = \sigma_1\sigma_2 \dots \sigma_k$ as above, then [HW]

$$O(\sigma) = lcm(O(\sigma_1), O(\sigma_2), \dots, O(\sigma_k))$$

(vi) For $m \leq n$, the number of m-cycles in S_n is [Why?]

$$\frac{1}{m}\frac{n!}{(n-m)!} = \frac{n(n-1)\dots(n-m+1)}{m}$$

7.4. Proposition : If $\sigma \in S_n$ has the cycle decomposition

$$(a_1a_2 \dots a_{\ell_1})(b_1b_2 \dots b_{\ell_2}) \dots$$

and $\tau \in S_n$, then $\tau\sigma\tau^{-1}$ has the cycle decomposition

$$(\tau(a_1)\tau(a_2) \dots \tau(a_{\ell_1}))(\tau(b_1)\tau(b_2) \dots \tau(b_{\ell_2})) \dots$$

Proof. If $\sigma(i) = j$, then

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$$

Hence, if (ij) appears in a cycle within σ, then $(\tau(i)\tau(j))$ appears within the corresponding cycle in $\tau\sigma\tau^{-1}$ $\square$

7.5. Definition :

(i) Given $\sigma \in S_n$, express it uniquely as a product of disjoint cycles

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$$

The cycle-type of σ is the tuple $(\ell_1, \ell_2, \ldots, \ell_k)$, where ℓ_i is the length of σ_i. To ensure well-definedness, we require that $\ell_1 \leq \ell_2 \leq \ldots \leq \ell_k$.

(ii) A partition of n is a tuple $(\ell_1, \ell_2, \ldots, \ell_k)$ where $\ell_i \leq \ell_{i+1}$ such that $n = \sum_{j=1}^{k} \ell_j$

7.6. Theorem : For $\sigma \in S_n$, the conjugacy class of σ consists of all those elements in S_n with the same cycle-type as σ

Proof. If $\sigma, \tau \in S_n$, then $\tau\sigma\tau^{-1}$ has the same cycle type as σ by 7.4. Conversely, suppose $\eta \in S_n$ has the same cycle type as σ, then write

$$\eta = \eta_1 \eta_2 \ldots \eta_k \text{ and } \sigma = \sigma_1 \sigma_2 \ldots \sigma_k$$

where $\ell_i =$ length of $\sigma_i =$ length of η_i, and include the 1-cycles as well. Write

$$\sigma_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,\ell_i}) \text{ and } \eta_i = (b_{i,1}, b_{i,2}, \ldots, b_{i,\ell_i})$$

Define $\tau(a_{i,j}) := b_{i,j}$, then τ is a permutation of $\{1, 2, \ldots, n\}$ because the cycles are disjoint. Furthermore, $\tau\sigma\tau^{-1} = \eta$ by 7.4. $\square$

7.7. Corollary : The number of conjugacy classes in S_n is equal to the number of partitions of n

7.8. Examples:

(i) If $\sigma_1 = (1)(2)(35)(46)$ and $\sigma_2 = (2)(6)(13)(45)$, then we may choose

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$$

so that $\tau\sigma_1\tau^{-1} = \sigma_2$

(ii) We may also choose

$$\tau' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix}$$

so that $\tau'\sigma_1\tau'^{-1} = \sigma_2$, so there is no uniqueness in this expression.

(iii) If $n = 5$, the conjugacy classes are as follows:

Partition of 5	Representative of Conjugacy class	Number of elements
1,1,1,1,1	e	1
1,1,1,2	(12)	$10 = \frac{1}{2}\frac{5!}{3!}$
1,1,3	(123)	20
1,4	(1234)	30
5	(12345)	$24 = \frac{1}{5}\frac{5!}{1}$
1,2,2	(12)(34)	15 [Why?]
2,3	(12)(345)	20 [Why?]

7.9. Corollary : Let $\sigma \in S_n$ be an m-cycle $(a_1 a_2 \dots a_m)$

(i) $|C(\sigma)| = \dfrac{n!}{m(n-m)!}$

(ii) $|Z(\sigma)| = m(n-m)!$

(iii) $Z(\sigma) = \{\sigma^i \tau : 0 \leq i \leq m-1, \tau \in H\}$ where

$$H = \{\tau \in S_n : \tau(a_i) = a_i \quad \forall 1 \leq i \leq m\}$$

Proof. (i) By 7.3(vi), the number of m-cycles in S_n is given by

$$\frac{n(n-1)\dots(n+m-1)}{m} = \frac{n!}{m(n-m)!} = |C(\sigma)|$$

(ii) By the Orbit-Stabilizer theorem,

$$|Z(\sigma)| = \frac{|S_n|}{|C(\sigma)|} = m(n-m)!$$

(iii) If $\tau \in H$, then $\tau\sigma = \sigma\tau$. Furthermore, $\sigma^i \in Z(\sigma)$, so clearly

$$A := \{\sigma^i \tau : 0 \leq i \leq m-1, \tau \in H\} \subset Z(\sigma)$$

Note that $O(\sigma) = m$ and $H \cong S_{n-m}$, so $|A| = (n-m)!m$, so $A = Z(\sigma)$

□

(End of Day 19)

7.10. Definition:

(i) A permutation $\sigma \in S_n$ is said to be even if $\sigma \in A_n$, and is said to be odd otherwise.

(ii) For an element $\sigma \in A_n$, we write $C_{S_n}(\sigma)$ for its conjugacy class in S_n, while we write

$$C_{A_n}(\sigma) := \{\tau\sigma\tau^{-1} : \tau \in A_n\}$$

Note that $C_{A_n}(\sigma) \subset C_{S_n}(\sigma)$

(iii) Similarly, we write $Z_{S_n}(\sigma)$ and $Z_{A_n}(\sigma)$ for the corresponding centralizers.

7.11. Lemma: Let $\sigma \in A_n$

(i) If σ commutes with an odd permutation, then $C_{A_n}(\sigma) = C_{S_n}(\sigma)$

(ii) If σ does not commute with any odd permutation, then

$$C_{S_n}(\sigma) = C_{A_n}(\sigma) \sqcup C_{A_n}((12)\sigma(12))$$

In particular,

$$|C_{A_n}(\sigma)| = \frac{|C_{S_n}(\sigma)|}{2}$$

Proof. (i) Let $\tau \in S_n$ be an odd permutation such that $\sigma\tau = \tau\sigma$, then WTS: $C_{S_n}(\sigma) \subset C_{A_n}(\sigma)$, so suppose $\eta \in C_{S_n}(\sigma)$, so $\exists \delta \in S_n$ such that

$$\eta = \delta\sigma\delta^{-1}$$

If $\delta \in A_n$, then $\eta \in C_{A_n}(\sigma)$. If $\delta \notin A_n$, then $\delta' := \tau\delta \in A_n$, and

$$\eta = \delta'\sigma\delta'^{-1}$$

Hence, $\eta \in C_{A_n}(\sigma)$ as required.

(ii) If σ does not commute with any odd permutation, then by definition

$$Z_{S_n}(\sigma) = Z_{A_n}(\sigma)$$

Hence,

$$|C_{A_n}(\sigma)| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{1}{2}\frac{|S_n|}{|Z_{S_n}(\sigma)|} = \frac{|C_{S_n}(\sigma)|}{2}$$

Now observe that

$$C_{S_n}(\sigma) = \{\delta\sigma\delta^{-1} : \delta \in A_n\} \sqcup \{\delta\sigma\delta^{-1} : \delta \text{ odd }\}$$

Note that these sets are disjoint because if $\delta \in A_n$ and θ is odd such that

$$\delta\sigma\delta^{-1} = \theta\sigma\theta^{-1}$$

Then $\theta^{-1}\delta$ is an odd permutation that commutes with σ. Since there is no such permutation, these sets must be disjoint. Now $\delta \in S_n$ is odd if and only if $\eta := (12)\delta$ is even. Hence,

$$\{\delta\sigma\delta^{-1} : \delta \text{ odd}\} = \{\eta(12)\sigma(12)\eta^{-1} : \eta \in A_n\}$$

Hence,

$$C_{S_n}(\sigma) = C_{A_n}(\sigma) \sqcup C_{A_n}((12)\sigma(12))$$

□

7.12. Example: Examine the conjugacy classes in S_5 from 7.8(iii)

e	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
1	10	20	30	24	15	20

Of these, $(12) \notin A_5, (1234) \notin A_5, (123)(45) \notin A_5$. Also,

$$(123)(45) = (45)(123) \Rightarrow C_{A_5}((123)) = C_{S_5}((123))$$
$$(12)(12)(34) = (12)(34)(12) \Rightarrow C_{A_5}((12)(34)) = C_{S_5}((12)(34))$$

However, if $\sigma = (12345)$, then by 7.9,

$$Z_{S_5}(\sigma) = \{\sigma^i : 0 \leq i \leq 4\} \subset A_5$$

Hence, σ does not commute with any odd permutation. By 7.11, this implies that

$$C_{S_5}(\sigma) = C_{A_5}(\sigma) \sqcup C_{A_5}(12)\sigma(12))$$

Note that $(12)\sigma(12) = (13452)$, so we get the conjugacy classes of A_5 to be

e	(123)	(12345)	(13452)	(12)(34)
1	20	12	12	15

Compare this example with 6.3.

7.13. Example: Consider the conjugacy classes in S_4

e	(12)	(123)	(1234)	(12)(34)
1	6	8	6	3

Once again, $(12) \notin A_4, (1234) \notin A_4$. Also,

$$(12)(34)(12) = (12)(12)(34)$$

so $C_{A_4}((12)(34)) = C_{S_4}((12)(34))$. Now observe that

$$(12)^{-1}(123)(12) = (132) \neq (123)$$

Similarly, (123) does not commute with any transposition. Also,

$$(1234)^{-1}(123)(1234) = (2143)(123)(1234) = (124) \neq (123)$$

Similarly, (123) does not commute with any 4-cycle. Hence, (123) does not commute with any odd transposition. Hence,

$$C_{S_4}((123)) = C_{A_4}((123)) \sqcup C_{A_4}((132))$$

So the class equation of A_4 can be read of from

e	(123)	(132)	(12)(34)
1	4	4	3

7.14. Corollary: A_4 does not have a subgroup of order 6. Hence, the converse of Lagrange's theorem fails.

Proof. If $H < A_4$ of order 6, then $H \lhd A_4$, so H must be a union of conjugacy classes. If $(123) \in H$, then $(132) = (123)^{-1} \in H$, so $|H| \geq 1 + 4 + 4 = 9$. Hence, $|H| = 12$, so $H = A_4$.

Hence, $(123) \notin H$ and $(132) \notin H$. Hence,

$$H \subset \{e, (12)(34), (13)(24), (14)(23)\}$$

so $|H| \neq 6$. □

7.15. Remark:

(i) A_4 is not simple, because the subgroup

$$\{e, (12)(34), (13)(24), (14)(23)\} \lhd A_4$$

(ii) A_n is simple for all $n \geq 5$. We have proved this for $n = 5$, but will not prove it for $n \geq 6$ (See [Conrad])

(End of Day 20)

IV. Structure of Finite Groups

All groups in this chapter will be assumed to be finite.

1. Direct Products

1.1. Definition : Let $(G_1, *), (G_2, \cdot)$ be two groups. The external direct product, $G = G_1 \times G_2$, is the set $G_1 \times G_2$ together with the binary operation

$$(x_1, y_1) \circ (x_2, y_2) := (x_1 * x_2, y_1 \cdot y_2)$$

Note that $G_1 \times G_2$ is a group.

1.2. Lemma : If $G = G_1 \times G_2$, $\widehat{G_1} = \{(a, e_2) : a \in G_1\} \lhd G$ and

$$G/\widehat{G_1} \cong G_2$$

Proof. Define $\pi_2 : G \to G_2$ be given by $(a, b) \mapsto b$, then π_2 is a surjective group homomorphism with

$$\ker(\pi_2) = \widehat{G_1}$$

So the result follows from the first isomorphism theorem. □

1.3. Lemma : If $g = (a, b) \in G_1 \times G_2$, then $O(g) = lcm(O(a), O(b))$

Proof. Let $n := lcm(O(a), O(b))$, then

$$g^n = (a^n, b^n) = (e_1, e_2) \Rightarrow O(g) \mid n$$

Furthermore, if $m = O(g)$, then $g^m = (e_1, e_2)$, then $a^m = e_1, b^m = e_2$, so

$$O(a) \mid m \text{ and } O(b) \mid m$$

Hence, $n \mid m$, so $O(g) = n$. □

1.4. Theorem : Let G_1, G_2 be finite cyclic groups, then $G_1 \times G_2$ is cyclic iff $(|G_1|, |G_2|) = 1$

Proof. (i) Suppose $(|G_1|, |G_2|) = 1$, let $a \in G_1, b \in G_2$ be the generators of G_1 and G_2 respectively. Then if $g = (a, b)$, then

$$O(g) = lcm(|G_1|, |G_2|) = |G_1||G_2| = |G_1 \times G_2|$$

Hence, $G_1 \times G_2$ is cyclic with generator g.

(ii) Suppose $(|G_1|, |G_2|) \neq 1$, let $m = lcm(|G_1|, |G_2|)$, then $m < |G_1 \times G_2|$. Furthermore, for any $g = (a, b) \in G_1 \times G_2$,

$$g^m = (a^m, b^m) = (e_1, e_2)$$

by Corollary I.2.7. Hence, $G_1 \times G_2$ does not have a generator.

□

1.5. Corollary : If $(n_1, n_2) = 1$, and $n = n_1 n_2$, then $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. In particular, if

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

is the prime decomposition of n, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

1.6. Definition : If $H, K \subset G$, $HK := \{hk : h \in H, k \in K\}$

1.7. Lemma : Let $H, K < G$, then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof. Note that HK is a union of left cosets

$$HK = \bigcup_{h \in H} hK$$

Now, $h_1 K = h_2 K \Leftrightarrow h_2^{-1} h_1 \in K \Leftrightarrow h_2^{-1} h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K)$. Hence, the number of distinct left cosets is equal to

$$[H : H \cap K]$$

Hence,

$$|HK| = [H : H \cap K]|K| = \frac{|H||K|}{|H \cap K|}$$

□

1.8. Proposition : $HK < G$ iff $HK = KH$

Proof. (i) Suppose $HK < G$. Since $K < HK$ and $H < HK$, it follows that $KH < HK$. By the previous lemma, $|KH| = |HK|$, so $KH = HK$.

(ii) Suppose $KH = HK$ and $a, b \in HK$. Write $a = h_1 k_1, b = h_2 k_2$. Then

$$ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$$

Now $h_1(k_1 k_2^{-1}) \in HK = KH$, so $\exists k_3 \in K, h_3 \in H$ such that

$$h_1(k_1 k_2^{-1}) = k_3 h_3$$

Hence,

$$ab^{-1} = k_3 h_3 h_2^{-1} \in KH = HK$$

So $HK < G$.

□

1.9. Corollary : If $K \lhd G$, and $H < G$, then $HK < G$

Proof. If $K \lhd G$, then for any $h \in H$,

$$hKh^{-1} \subset K \Rightarrow hK \subset Kh \Rightarrow HK \subset KH$$

Since $|HK| = |KH|$, we have $HK = KH$. □

1.10. Corollary : If $G = G_1 \times G_2$, then $G = \widehat{G_1}\widehat{G_2}$

Proof. Since $\widehat{G_1} \lhd G$, $\widehat{G_1}\widehat{G_2} < G$. Also,

$$|\widehat{G_1}\widehat{G_2}| = \frac{|\widehat{G_1}||\widehat{G_2}|}{|\widehat{G_1} \cap \widehat{G_2}|} = \frac{|G_1||G_2|}{1} = |G|$$

Hence, $G = \widehat{G_1}\widehat{G_2}$ □

1.11. Definition: If G is a group and $H, K < G$ such that $G = HK$, then G is said to be an internal direct product of H and K.

(End of Day 21)

1.12. Remark/Example:

(i) By Corollary 1.10, if G is an external direct product of G_1 and G_2, then it is an internal direct product of $\widehat{G_1}$ and $\widehat{G_2}$. Since $\widehat{G_i} \cong G_i$, we simply say that G is a direct product of G_1 and G_2

(ii) If $G = HK$, it does not necessarily imply that $G \cong H \times K$. ie. An internal direct product is not necessarily an external direct product.

(iii) Let $G = S_3$ and $H = A_3 = \{e, (123), (132)\}$. Then $H \lhd G$. Furthermore, if $K := \{e, (12)\}$, then $K < G$. Hence,

$$HK < G$$

Furthermore, $|H \cap K| \mid (3, 2) = 1$. Hence, $|HK| = |H||K| = 6$. Hence, $HK = G$. However,

$$S_3 \ncong H \times K$$

because $H \times K$ is Abelian and S_3 is not.

1.13. Theorem: Let G be a group and $H, K < G$ such that

(i) $H \lhd G, K \lhd G$.

(ii) $H \cap K = \{e\}$

Then $HK \cong H \times K$.

Proof. Since $H \lhd G, HK < G$ by 1.9. If $h \in H$ and $k \in K$, then consider $x := hkh^{-1}k^{-1}$. By normality,

$$x = (hkh^{-1})k^{-1} \in K \text{ and } x = h(kh^{-1}k^{-1}) \in H$$

Hence, $x \in H \cap K = \{e\}$, so $hkh^{-1}k^{-1} = e$, whence

$$hk = kh \quad \forall h \in H, k \in K$$

Define $f : H \times K \to HK$ by $(h, k) \mapsto hk$.

(i) f is a homomorphism: If $(h_1, k_1), (h_2, k_2) \in H \times K$, then

$$f((h_1, k_1)(h_2, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = f(h_1, k_1)f(h_2, k_2)$$

(ii) f is injective: If $(h, k) \in \ker(f)$, then

$$hk = e \Rightarrow h = k^{-1} \in H \cap K = \{e\}$$

Hence $h = k = e$, so $\ker(f) = \{(e, e)\}$.

(iii) f is surjective: Obvious.

□

1.14. Proposition : Let $|G| = p^2$, then

$$G \cong \begin{cases} \mathbb{Z}_{p^2} & : \text{ if } G \text{ cyclic} \\ \mathbb{Z}_p \times \mathbb{Z}_p & : \text{ otherwise} \end{cases}$$

Proof. Suppose $\exists x \in G$ such that $O(x) = p^2$, then G is cyclic. So

$$G \cong \mathbb{Z}_{p^2}$$

by II.4.3. Now suppose $O(x) = p$ for all $x \in G, x \neq e$. Fix $x \in G$, and consider $H := \langle x \rangle$. Since $H \neq G, \exists y \in G \setminus H$. Let $K := \langle y \rangle$.

Since G is Abelian by III.5.10, $H \lhd G, K \lhd G$, so $HK < G$. Also, since $|K| = p$, and

$$H \cap K < K \Rightarrow H \cap K = \{e\} \text{ or } K \subset H$$

Since $y \in K \setminus H$, it follows that $H \cap K = \{e\}$, so

$$|HK| = p^2 = |G| \Rightarrow G = HK$$

By Theorem 1.13, it follows that

$$G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

□

2. Cauchy's Theorem

2.1. Remark: Let G be a finite group.

(i) By Lagrange's theorem, if $H < G$, then $|H| \mid |G|$.

(ii) However, the converse is not true. For instance, if $G = A_4$, then $6 \mid |A_4|$, but A_4 does not have a subgroup of order 6. (See III.7.14)

Cauchy's theorem can be thought of a partial converse to Lagrange's theorem.

2.2. Lemma: Let G be a group and $g \in G$. If $d \mid O(g)$, then G contains an element of order d.

Proof. Let $m := O(g)$ and $x := g^{m/d}$ then we claim that $O(x) = d$.

First note that $x^d = g^m = e$, so $O(x) \mid d$. Furthermore, if $k = O(x)$, then $x^k = e$, so $g^{mk/d} = e$. Hence, $m \mid mk/d$. So $\exists \ell \in \mathbb{N}$ such that

$$\frac{mk}{d} = \ell m \Rightarrow k = \ell d \Rightarrow d \mid k$$

Hence, $d = k$ as required. □

2.3. Lemma: Let $\varphi : G \to G'$ be a homomorphism and $x \in G$, then $O(\varphi(x)) \mid O(x)$

Proof. Let $m := O(x)$, then $x^m = e$, so $\varphi(x)^m = \varphi(e) = e'$. Hence, $O(\varphi(x)) \mid m$. □

2.4. Theorem (Abelian Case): Let G be an Abelian group and p a prime such that $p \mid |G|$, then $\exists x \in G$ such that $O(x) = p$. Equivalently, G has a subgroup of order p.

Proof. We induct on the number $P(G)$ of prime factors of $|G|$. Since $p \mid |G|$, $P(G) \geq 1$. If $P(G) = 1$, then $|G| = p$, so G contains an element of order p by I.2.6. Now suppose $P(G) \geq 2$ and assume that the result is true for any group G' such that $P(G') \leq P(G) - 1$.

Fix $x \in G$. If $p \mid O(x)$, then $\exists y \in G$ such that $O(y) = p$ by Lemma 2.1. Hence, assume $p \nmid O(x)$. Set $H := \langle x \rangle$. Then $H \lhd G$ since G is Abelian, so define

$$G' := G/H \text{ and set } \pi : G \to G'$$

the natural homomorphism. Since $p \nmid |H|$, it follows that $p \mid |G'|$. Also, by definition,

$$|G'| = |G|/p$$

so $P(G') \leq P(G) - 1$. So by induction hypothesis, $\exists x' \in G'$ such that $O(x') = p$. However, $x' = \pi(y)$ for some $y \in G$, so we have

$$O(\pi(y)) = p$$

By Lemma 2.2,

$$p \mid k = O(y)$$

By Lemma 2.1, G contains an element of order p. □

2.5. Remark:

(i) The class equation reads

$$|G| = |Z(G)| + \sum_{|C(x_i)|>1} |C(x_i)| = |Z(G)| + \sum_{|C(x_i)|>1} [G : Z(x_i)]$$

(ii) If $H < G$ such that $H \subset Z(G)$, then $H \lhd G$

(iii) If $x \notin Z(G)$, then $|C(x)| > 1$, so the centralizer

$$Z(x) = \{g \in G : gx = xg\}$$

is a proper subgroup of G. ie. $Z(x) \neq G$

(iv) $Z(G)$ is an Abelian subgroup of G.

The following argument is a more sophisticated version of what we saw in trying to prove that the center of a p-group is non-trivial (III.5.8).

2.6. Theorem (Non-Abelian Case): Let G be any group and p a prime such that $p \mid |G|$. Then G contains an element of order p. Equivalently, G contains a subgroup of order p.

Proof. We induct on $|G|$. If $|G| = p$, then G is cyclic, and contains an element of order p. Now suppose $|G| \geq p + 1$, and assume that the theorem is true for any group G' such that $|G'| < |G|$.

Consider the class equation

$$|G| = |Z(G)| + \sum_{|C(x_i)|>1} [G : Z(x_i)]$$

We consider the following cases:

(i) Suppose $\exists x \notin Z(G)$ such that $p \mid |Z(x)|$: If $x \notin Z(G)$, then $Z(x)$ is a proper subgroup of G. Suppose $p \mid |Z(x)|$, then by the induction hypothesis, $Z(x)$ contains an element of order p. Hence, G contains an element of order p.

(ii) Suppose that $p \nmid |Z(x)|$ for all $x \notin Z(G)$: Then, since $p \mid |G| = |Z(x)||C(x)|$, we see that

$$p \mid |C(x_i)|$$

for any x_i such that $|C(x_i)| > 1$. Since $p \mid |G|$, we see from the class equation that

$$0 \equiv |Z(G)| \pmod{p}$$

Hence, $p \mid |Z(G)|$. But $Z(G)$ is Abelian, so by Theorem 2.2, $\exists x \in Z(G)$ of order p.

□

2.7. Corollary : If $|G| = 6$, then

$$G \cong \begin{cases} \mathbb{Z}_6 & : \text{ if } G \text{ is abelian} \\ S_3 & : \text{ otherwise} \end{cases}$$

Proof. By Cauchy's theorem, $\exists H < G$ such that $|H| = 3$ and $K < G$ such that $|K| = 2$. Since $|G| = 6$, it follows by the Strong Cayley theorem that $H \lhd G$. Hence, $HK < G$. By order considerations,

$$G = HK$$

We thus have two cases:

(i) If $K \lhd G$, then by 1.14, $G \cong H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$ by 1.4.

(ii) If K is not normal in G, then consider the action of G on G/K by left-multiplication. This gives a map

$$f : G \to S_3$$

since $[G : K] = 3$. By III.4.4, $\ker(f) \subset K$. Since K is not normal in G, $\ker(f) \neq K$. Since $|K| = 2$, it must follow that $\ker(f) = \{e\}$. Hence, f is injective. Since $|G| = |S_3|$, we conclude that

$$G \cong S_3$$

□

2.8. Corollary: $D_3 \cong S_3$

2.9. Corollary : If $|G| = 15$, then $G \cong \mathbb{Z}_{15}$

Proof. By Cauchy's theorem, $\exists H, K < G$ such that $|H| = 5, |K| = 3$. Once again, by the Strong Cayley theorem, $H \lhd G$, so $HK < G$. Once again, by order considerations,

$$G = HK$$

We claim: $K \lhd G$. To this end, consider the action of K on H by conjugation: For each $k \in K$, define $\varphi_k : H \to H$ by

$$\varphi_k(h) := khk^{-1}$$

Note that $\varphi_k \in Aut(H)$. Furthermore,

$$\varphi_{k_1} \circ \varphi_{k_2} = \varphi_{k_1 k_2}$$

Hence, we get a group homomorphism

$$f : K \to Aut(H)$$

Now $|H| = 5$, so $H \cong \mathbb{Z}_5$. By HW 3,

$$\mathrm{Aut}(H) \cong \mathbb{Z}_5^* \Rightarrow |\mathrm{Aut}(H)| = 4$$

Now,

$$|\mathrm{Image}(f)| \mid 4 \text{ and } |\mathrm{Image}(f)| = [K : \ker(f)] \mid |K| = 3$$

Hence, $|\text{Image}(f)| = 1$, whence f is trivial. Hence, for each $k \in K, h \in H$,

$$khk^{-1} = h \Rightarrow hk = kh$$

It follows as in Theorem 1.13 that

$$HK \cong H \times K$$

Hence, $G \cong H \times K \cong \mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$ by 1.5. □

(End of Day 22)

3. Sylow's Theorems

Cauchy's theorem gives is a partial converse to Lagrange's theorem: If $p \mid |G|$, then G has a subgroup of order p. We now wish to extend this theorem to powers of primes. We will show: If p is prime, and $p^i \mid |G|$, then G has a subgroup of order p^i. This is called Sylow's first theorem, and the proof is similar to that of Cauchy's theorem (2.6)

3.1. Lemma: Let G be a group, $H \lhd G$ and $K' < G/H$. If $\pi : G \to G/H$ is the quotient map, and $K := \pi^{-1}(K')$, then $K < G$ and

$$|K| = |K'||H|$$

Proof. That $K < G$ follows from the Second Isomorphism theorem (II.4.6). Furthermore, $H \subset K$. Restriction of π gives a surjective map group homomorphism

$$\widetilde{\pi} : K \to K'$$

Now, $\ker(\widetilde{\pi}) = \ker(\pi) \cap K = H \cap K = H$. So by the first isomorphism theorem,

$$K/H \cong K'$$

The result follows. □

3.2. Remark:

(i) Once again, recall the class equation reads

$$|G| = |Z(G)| + \sum_{|C(x_i)|>1} |C(x_i)|$$

(ii) If $H < G$ such that $H \subset Z(G)$, then $H \lhd G$

(iii) If $x \notin Z(G)$, then $|C(x)| > 1$, so the centralizer

$$Z(x) = \{g \in G : gx = xg\}$$

is a proper subgroup of G. ie. $Z(x) \neq G$

3.3. (Sylow I): Let G be any group and p a prime number, $i \in \mathbb{N}$. If $p^i \mid |G|$, then G has a subgroup of order p^i.

Proof. We induct on i and $|G|$ simultaneously. Let $P(i, n)$ be the statement "If G is a group of order n and $p^i \mid n$, then G has a subgroup of order p^i". Note that

(i) $P(1, n)$ is true for all n by Cauchy's theorem.

(ii) $P(i, 1)$ is true for all i trivially.

(iii) For fixed $(i, n) \in \mathbb{N} \times \mathbb{N}$, assume that, if $1 \leq j \leq i - 1$ and $1 \leq k \leq n - 1$

(a) $P(j, k)$ is true.

(b) $P(i, k)$ is true.

(c) $P(j, n)$ is true.

then WTS $P(i, n)$ is true: So let G be a group of order n and $p^i \mid |G|$. Consider the class equation of G

$$|G| = |Z(G)| + \sum_{|C(x_i)|>1} |C(x_i)|$$

We consider two cases:

(a) Suppose that for one x_i appearing on the RHS, $p^i \mid |Z(x_i)|$, then, since $P(i, k)$ is true for all $k < n$ and $|Z(x_i)| < |G|$, it would follow by induction hypothesis that $Z(x_i)$ has a subgroup of order p^i. This would also be the required subgroup of G.

(b) Suppose that for each x_i appearing on the RHS, $p^i \nmid |Z(x_i)|$. Since

$$p^i \mid |G| = |Z(x_i)||C(x_i)|$$

it follows that $p \mid |C(x_i)|$. Since $p \mid |G|$, going modulo p, we see that

$$|Z(G)| \equiv 0 \pmod{p}$$

Hence, $p \mid |Z(G)|$. By Cauchy's theorem, $Z(G)$ has a subgroup H of order p. By Remark 4.3(ii),

$$H \lhd G$$

Now set $G' := G/H$. Then $p^{i-1} \mid |G'|$. Since $P(i - 1, |G'|)$ is true, G' has a subgroup K' of order p^{i-1}. By Lemma 3.1, G has a subgroup of order p^i.

□

3.4. Definition: Let G be a group, p a prime, and suppose $k \in \mathbb{N}$ such that

$$p^k \mid |G| \text{ but } p^{k+1} \nmid |G|$$

By the First Sylow theorem, there is $P < G$ such that $|P| = p^k$. Such a subgroup is called a $p-$Sylow subgroup of G

Note: This subgroup may not be unique.

3.5. Examples:

(i) If $|G| = p^n$, then G itself is a p-Sylow subgroup of G.

(ii) If $G = \mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, then

$$H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \{0\}$$

is a 2-Sylow subgroup. Furthermore,

$$K := \{0\} \times \{0\} \times \mathbb{Z}_3$$

is a 3-Sylow subgroup. We will show later that these are the only Sylow subgroups of G.

(iii) Let $G = S_3$, then $|G| = 6 = 2 \times 3$

(a) $A_3 < S_3$ is a 3-Sylow subgroup. Also, this is the unique subgroup of G of order 3 (Check!)

(b) Any subgroup of order 2 is a 2-Sylow subgroup. For instance,

$$K_1 := \{(12), e\}, \text{ and } K_2 := \{(13), e\}$$

are distinct 2-Sylow subgroups.

(iv) If $G = A_4$, then $|G| = 12 = 2^2 \times 3$.

(a) We know a 2-Sylow subgroup of G

$$H := \{e, (12)(34), (13)(24), (14)(23)\}$$

By Remark III.7.15, $H \lhd A_4$. We will show that this is a unique 2-Sylow subgroup of G.

(b) Any subgroup of order 3 is a 3-Sylow subgroup. For instance,

$$K_1 := \{e, (123), (132)\} \text{ and } K_2 := \{e, (124), (142)\}$$

are distinct 3-Sylow subgroups.

(v) Let $G = S_4$, then $|G| = 24 = 2^3 \times 3$.

(a) Any subgroup of order 3 is a 3-Sylow subgroup. For instance, the subgroups listed above for A_4 work.

(b) Any subgroup of order 8 is a 2-Sylow subgroup. For instance, consider $D_4 < S_4$ by using the action of D_4 on the set of vertices of the square. Then $|D_4| = 8$, so D_4 is a 2-Sylow subgroup of S_4.

Note: If we relabel the vertices, then we get another subgroup of S_4 of order 8, which is isomorphic to D_4, but not the same subgroup of S_4. Thus, the 2-Sylow subgroup is not unique.

(End of Day 23)

3.6. Definition: A group G is called a p-group if p is a prime, and $|G| = p^n$ for some $n \in \mathbb{N}$

3.7. (Fixed Point Lemma): Let G be a p-group acting on a finite set X. Define the fixed point set

$$X^G := \{x \in X : g \cdot x = x \quad \forall g \in G\}$$

Then

$$|X| \equiv |X^G| \pmod p$$

In particular, if $p \nmid |X|$, then X has a fixed point.

Proof. Write X as a disjoint union of orbits. Note that an orbit is a singleton set $\{x\}$ iff $x \in X^G$. Hence, we may write

$$X = X^G \sqcup \mathcal{O}(x_1) \sqcup \mathcal{O}(x_2) \sqcup \ldots \sqcup \mathcal{O}(x_k)$$

where $|\mathcal{O}(x_i)| > 1$ for all $1 \leq i \leq k$. Taking cardinalities, we see that

$$|X| = |X^G| + \sum_{i=1}^{k} |\mathcal{O}(x_i)|$$

By the orbit-stabilizer theorem, $|\mathcal{O}(x_i)| = [G : \mathrm{Stab}(x_i)]$. Since G is a p-group, it follows that

$$p \mid |\mathcal{O}(x_i)| \quad \forall 1 \leq i \leq k$$

Hence the result. □

3.8. Definition: Let G be a group and $H, K < G$ be two subgroups. We say that H and K are conjugate to each other if $\exists g \in G$ such that $gHg^{-1} = K$.

3.9. Remark:

(i) Conjugacy is an equivalence relation on the set of all subgroups of G.

(ii) If $H < G$, then $gHg^{-1} < G$.

(iii) If two subgroups are conjugate, then they have the same cardinality. In particular, if H is a p-Sylow subgroup, then so is K.

3.10. (Sylow II): Let G be a group, then any two p-Sylow subgroups of G are conjugate to each other.

Proof. Let P be a p-Sylow subgroup, and Q any other p-Sylow subgroup. Since conjugacy is an equivalence relation, it suffices to show that $\exists g \in g$ such that $gPg^{-1} = Q$. Set $X = G/P$ and let Q act on X by left-multiplication. Since P is a p-Sylow subgroup,

$$|X| = [G : P] \Rightarrow p \nmid |X|$$

Hence by the Fixed Point Lemma, $\exists x \in X$ such that

$$g \cdot x = x \quad \forall g \in Q$$

Write $x = g_0P$, then we see that, forall $g \in Q$,

$$gg_0P = g_0P \Rightarrow g_0^{-1}gg_0 \in P$$

Hence,

$$g_0^{-1}Qg_0 \subset P$$

But $|g_0^{-1}Qg_0| = |Q| = |P|$, so $g_0^{-1}Qg_0 = P$. Equivalently,

$$Q = g_0Pg_0^{-1}$$

□

3.11. Definition : Normalizer of a subgroup $H < G$, denoted by $N_G(H)$

3.12. Lemma :

(i) $N_G(H) < G$

(ii) $H \subset N_G(H)$ and $H \lhd N_G(H)$

Proof. (i) Let G act on $X := G/H$ by conjugation. Then consider the stabilizer

$$\mathrm{Stab}(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$$

Thus, $N_G(H) < G$.

(ii) Clearly, $H \subset N_G(H)$. Since $H < G$, it follows that $H < N_G(H)$. That $H \lhd N_G(H)$ follows from the definition of $N_G(H)$.

□

3.13. Lemma: Let H be a subgroup of G and let H act on $X := G/H$ by left-multiplication. Then for any $x \in G$,

$$xH \in X^H \Leftrightarrow x \in N_G(H)$$

Hence,

$$|X^H| = [N_G(H) : H]$$

Proof. If $xH \in X^H$, then for any $h \in H$,

$$h \cdot (xH) = xH \Rightarrow x^{-1}hx \in H \Rightarrow x^{-1}Hx \subset H \Rightarrow x^{-1}Hx = H \Rightarrow x \in N_G(H)$$

Conversely, all the arrows are reversible. Thus, it follows that

$$X^H = N_G(H)/H$$

so the result follows. □

(End of Day 24)

3.14. (Sylow I') Let $H < G$ be a $p-$group, then there exists a $p-$Sylow subgroup $P < G$ such that $H \subset P$

Proof. If H is a p-Sylow subgroup, then there is nothing to show. So assume H is not a p-Sylow subgroup. In that case,

$$p \mid [G : H]$$

Let $X = G/H$, and let H act on X by left-multiplication. By the Fixed Point Lemma,

$$[G : H] = |X| \equiv |X^H| \pmod p$$

Hence, $p \mid |X^H| = [N_G(H) : H]$. Since $H \lhd N_G(H)$, it follows that $N_G(H)/H$ is a group. Since

$$p \mid |N_G(H)/H|$$

$N_G(H)/H$ has a subgroup K' of order p by Cauchy's theorem. Let $\pi : N_G(H) \to N_G(H)/H$ be the quotient map, then

$$H \subset K := \pi^{-1}(K') < G$$

has the cardinality, $|K| = |K'||H| = p|H|$. If K is a p-Sylow subgroup, then we may stop. Else, we may proceed inductively, until we obtain a p-Sylow subgroup of G containing H. □

3.15. Remark: By Cauchy's theorem and induction, this provides another proof of Sylow I using induction.

3.16. (Sylow III) : Let G be a group and p a prime. Suppose that

$$|G| = p^k m \text{ where } p \nmid m$$

Let n_p denote the number of p-Sylow subgroups in G, then

(i) $n_p \equiv 1 \pmod p$

(ii) For any p-Sylow subgroup P, $n_p = [G : N_G(P)]$

(iii) $n_p \mid m$

Proof. Let $X := \mathrm{Syl}_p(G)$ denote the set of all p-Sylow subgroups of G. Then G acts on X by conjugation. Furthermore, by Sylow II, this action is transitive. Note that $n_p = |X|$

(i) Let P be a p-Sylow subgroup, and let P act on X by conjugation. Then by the Fixed Point Lemma,

$$n_p \equiv |X^P| \pmod p$$

Now if $Q \in X^P$, then for any $p \in P$, $pQp^{-1} = Q$. Hence, $P \subset N_G(Q)$. However,

$$Q \lhd N_G(P)$$

Thus, Q and P are both p-Sylow subgroups of $N_G(Q)$. By Sylow II, $\exists g \in N_G(Q)$ such that

$$gQg^{-1} = P$$

However, $g \in N_G(Q)$, so $gQg^{-1} = Q$. Thus, $P = Q$. Hence, $X^P = \{P\}$, whence

$$n_p \equiv 1 \pmod{p}$$

as required.

(ii) Now consider the action of G on X by conjugation. This action is transitive by Sylow II, so by the Orbit-Stabilizer theorem,

$$|X| = [G : \mathrm{Stab}(P)]$$

However, $\mathrm{Stab}(P) = \{g \in G : gPg^{-1} = P\} = N_G(P)$. Hence,

$$n_p = [G : N_G(P)]$$

(iii) Since $P < N_G(P)$, we have

$$n_p = \frac{[G : P]}{N_G(P) : P]} = \frac{m}{[N_G(P) : P]}$$

Thus, $n_p \mid m$ as required.

□

3.17. Corollary: Let G be a group and p a prime dividing $|G|$, and let P be a p-Sylow subgroup of G. Then $P \lhd G$ iff $n_p = 1$

Proof. If $g \in G$, then gPg^{-1} is a p-Sylow subgroup of G. If $n_p = 1$, then $gPg^{-1} = P$ for all $g \in G$, so $P \lhd G$.

Conversely, if $P \lhd G$ and Q is any p-Sylow subgroup of G, then by Sylow II, $\exists g \in G$ such that $gPg^{-1} = Q$. Since $P \lhd G$, $Q = P$ must hold. Hence, $n_p = 1$. □

3.18. Examples:

(i) Suppose $|G| = 15$, we give another proof that $G \cong \mathbb{Z}_{15}$

Proof. Note that

$$n_3 \equiv 1 \pmod{5} \text{ and } n_3 \mid 5 \Rightarrow n_3 = 1$$

Let H be a 3-Sylow subgroup, then by 3.17, $H \lhd G$. Furthermore,

$$n_5 \equiv 1 \pmod{5} \text{ and } n_5 \mid 3 \Rightarrow n_5 = 1$$

Hence if K is the 3-Sylow subgroup, then by 3.17, $K \lhd G$. Once again

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

Hence, $G = HK \cong H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. □

(End of Day 25)

4. The Dihedral Group

4.1. Remark: Let $G = D_n$ denote the group of symmetries of a regular n-gon. Enumerate the vertices as $\{1, 2, \ldots, n\}$, so we view G as a subgroup of S_n. Define

$$r = (1, 2 \ldots, n)$$

to be the rotation in G by $2\pi/n$. Let $s \in G$ denote the reflection about the axis passing through the vertex 1 and the origin. Hence, if n is odd, then write $n = 2k+1$, then the axis passes through the edge joining $k+1$ and $k+2$

$$s = \begin{pmatrix} 1 & 2 & 3 & \ldots & k+1 & k+2 & \ldots & 2k & 2k+1 \\ 1 & 2k+1 & 2k & \ldots & k+2 & k+1 & \ldots & 3 & 2 \end{pmatrix}$$

If $n = 2k$ is even, then the axis passes through the vertex k, so

$$s = \begin{pmatrix} 1 & 2 & 3 & \ldots & k-1 & k & k+1 & \ldots & 2k \\ 1 & 2k & 2k-1 & \ldots & k+1 & k & k-1 & \ldots & 2 \end{pmatrix}$$

In each case, we may verify

(i) $\{1, r, r^2, \ldots, r^{n-1}\}$ are all distinct, because $O(r) = n$

(ii) $srs^{-1} = r^{-1}$

Proof. Suppose $n = 2k+1$ is odd, then

$$\begin{aligned} srs^{-1} = srs = & \begin{pmatrix} 1 & 2 & \ldots & k+1 & k+2 & \ldots & 2k & 2k+1 \\ 1 & 2k+1 & \ldots & k+2 & k+1 & \ldots & 3 & 2 \end{pmatrix} \\ & \begin{pmatrix} 1 & 2 & \ldots & 2k & 2k+1 \\ 2 & 3 & \ldots & 2k+1 & 1 \end{pmatrix} \\ & \begin{pmatrix} 1 & 2 & \ldots & k+1 & k+2 & \ldots & 2k & 2k+1 \\ 1 & 2k+1 & \ldots & k+2 & k+1 & \ldots & 3 & 2 \end{pmatrix} \\ & = \begin{pmatrix} 1 & 2 & \ldots & k+1 & k+2 & \ldots & 2k & 2k+1 \\ 2k+1 & 1 & \ldots & k & k+1 & \ldots & 2k-1 & 2k \end{pmatrix} \\ & = (1, 2k+1, 2k, 2k-1, \ldots, 2) \\ & = r^{-1} \end{aligned}$$

The even case is similar. □

(iii) If $1 \leq i < j \leq n-1$, then $sr^i \neq sr^j$

Hence,

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, sr, sr^2, \ldots, sr^{n-1}\}$$

If $H = \langle r \rangle$ and $K = \langle s \rangle$, then

$$[G : H] = 2 \Rightarrow H \lhd G$$

and $H \cap K = \{e\}$, so $|HK| = 2n$. Hence,

$$G = HK$$

Note that G is non-Abelian, while both H and K are cyclic, so $G \ncong H \times K$.

4.2. Theorem: Let G be a group with two elements $a, b \in G$ such that

$$a^n = b^2 = e \text{ and } bab = a^{-1}$$

Then $\exists$ a unique group homomorphism $\varphi : D_n \to G$ such that

$$\varphi(r) = a \text{ and } \varphi(s) = b$$

Proof. If $bab = bab^{-1} = a^{-1}$, then

$$ba^j b = a^{-j} \quad \forall j \in \mathbb{Z}$$

Since $b^2 = e$, we have

$$b^k a^j b^{-k} = a^{(-1)^k j} \quad \forall k, j \in \mathbb{Z}$$

Note that

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

so define $\varphi : D_n \to G$ by

$$\varphi(s^k r^j) := b^k a^j, \quad \forall k, j \in \mathbb{Z}$$

Then

(i) φ is well-defined because

$$s^k r^j = s^\ell r^m \Rightarrow k \equiv \ell \pmod 2 \text{ and } j \equiv m \pmod n$$

and in that case $b^k a^j = b^\ell a^m$ since $a^n = e = b^2$.

(ii) φ is a group homomorphism:

$$\begin{aligned}
\varphi((s^k r^j)(s^\ell r^m)) &= \varphi(r^{(-1)^k j} s^k s^\ell r^m) \\
&= \varphi(r^{(-1)^k j} s^{k+\ell} r^m) \\
&= \varphi(r^{(-1)^k j} r^{(-1)^{(k+\ell)} m} s^{(k+\ell)}) \\
&= \varphi(r^{(-1)^k j + (-1)^{(k+\ell)} m} s^{(k+\ell)}) \\
&= a^{(-1)^k j + (-1)^{(k+\ell)} m} b^{(k+\ell)} \\
&= \ldots = (b^k a^j)(b^\ell a^m)
\end{aligned}$$

(iii) Uniqueness: If $\psi : D_n \to G$ is any other homomorphism such that

$$\psi(r) = a \text{ and } \psi(s) = b$$

Then $\psi = \varphi$ because every element of D_n is a product of powers of r and s.

$\square$

4.3. Theorem: Let p be an odd prime and G be a group of order $2p$. Then

$$G \cong \begin{cases} \mathbb{Z}_{2p} & : G \text{ Abelian} \\ D_p & : G \text{ non-Abelian} \end{cases}$$

Proof. By Cauchy's theorem, G has elements $a, b \in G$ such that $O(a) = p, O(b) = 2$. Let $H := \langle a \rangle$, then $H \lhd G$ since $[G : H] = 2$. So

$$bab^{-1} = a^t$$

for some $t \in \{0, 1, \ldots, p-1\}$. Then

$$a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^tb^{-1} = (bab^{-1})^t = a^{t^2}$$

Hence, $a^{t^2-1} = e$, whence

$$p \mid (t^2 - 1) = (t-1)(t+1)$$

Since p is prime, $p \mid t-1$ or $p \mid t+1$.

(i) If $p \mid t-1$, then $a^t = a^{t-1}a = a$. Hence,

$$bab^{-1} = a \Rightarrow ba = ab$$

Since $G = \langle a, b \rangle$, it follows that G is abelian. In that case,

$$O(ab) \mid lcm(O(a), O(b)) = 2p$$

However, if $O(ab) = m$, then

$$a^m = b^{-m} \in \langle a \rangle \cap \langle b \rangle$$

But $O(a) = p$ and $O(b) = 2$. Since p is an odd prime,

$$\langle a \rangle \cap \langle b \rangle = \{e\}$$

Hence, $a^m = b^{-m} = e$. Hence,

$$p \mid m \text{ and } 2 \mid m \Rightarrow 2p \mid m$$

Hence,

$$O(ab) = 2p$$

Hence, G is cyclic, so $G \cong \mathbb{Z}_{2p}$.

(ii) If $p \mid t+1$, then $bab^{-1} = a^t = a^{t+1}a^{-1} = a^{-1}$. By the previous theorem, there is a group homomorphism

$$\varphi : D_p \to G$$

such that $\varphi(r) = a, \varphi(s) = b$. Since $G = \langle a, b \rangle$, this map is surjective. Since

$$|G| = 2p = |D_p|$$

this map is also injective. Hence, $G \cong D_p$.

□

5. Simple Groups of order ≤ 60

Recall : A group is called *simple* if its has no non-trivial normal subgroups.

5.1. Remark :

(i) Any group of of prime order is simple (by Lagrange's theorem, it has no subgroups).

(ii) If G is abelian with $|G|$ composite, then G is not simple ((HW5)

(iii) A_5 is a simple group of order 60.

(End of Day 26)

5.2. Lemma: If $|G| = p^n$, where p is prime, and $n > 1$, then G is not simple.

Proof. If G is simple, then $Z(G)$ must be trivial. Since $Z(G) \neq \{e\}$, it follows that $Z(G) = G$, whence G is Abelian. Since $|G|$ is composite, this is impossible. □

5.3. Lemma: If G has a proper subgroup H such that $|G| \nmid [G : H]!$, then G is not simple.

Proof. HW 5 □

5.4. Lemma: Let G be a group of order pqr, where $p < q < r$ are primes, then G is not simple.

Proof. Let n_p denote the number of p-Sylow subgroups of G. Since any two distinct p-Sylow subgroups intersect trivially, G must have

$$n_p(p-1)$$

elements of order p. Similarly, G has

$$n_q(q-1)$$

elements of order q and $n_r(r-1)$ elements of order r. Thus,

$$pqr = |G| \geq n_p(p-1) + n_q(q-1) + n_r(r-1) + 1$$

Now, by Sylow III

$$n_r \mid pq \text{ and } n_r \equiv 1 \pmod{r}$$

If $n_r = 1$, then the r-Sylow subgroup is normal in G. So assume $n_r \neq 1$. Then, $n_r \mid pq$ implies that

$$n_r \in \{1, p, q, pq\}$$

Since $p < q < r$, it follows that $n_r = pq$. Thus, we have

$$pqr \geq n_p(p-1) + n_q(q-1) + pq(r-1) + 1$$

Now if $n_q = 1$, we are once again done. If not, then $n_q \mid pr$, so

$$n_q \in \{1, p, r, pr\}$$

Since $n_q \equiv 1 \pmod{q}$, and $p < q$, it must happen that

$$n_q \in \{r, pr\}$$

In particular, $n_q \geq r$. Finally, if $n_p \neq 1$, then $n_p \mid qr$ implies that

$$n_p \in \{1, q, r, qr\}$$

So $n_p \geq q$. Hence, we get

$$pqr \geq q(p-1) + r(q-1) + pq(r-1) + 1$$

Hence,

$$0 \geq qr - r - q \Rightarrow 2 < q \leq \frac{r}{r-1} \leq 2$$

This is absurd. Hence, one of n_p, n_q or n_r must be one. Thus, G is non-simple. □

5.5. Theorem: If $|G| < 60$ and G is simple, then $|G|$ is a prime. (HW)

5.6. Theorem: If G is any simple group of order 60, then $G \cong A_5$

Proof. Note that

$$60 = 2^2 \times 3 \times 5$$

(i) Let n_5 denote the number of $5-$Sylow subgroups of G. Then by Sylow III,

$$n_5 \equiv 1 \pmod{5} \text{ and } n_5 \mid 12$$

Hence, $n_5 \in \{1, 6\}$. If $n_5 = 1$, then the unique Sylow subgroup would be normal, contradicting the simplicity of G. Hence,

$$n_5 = 6$$

Hence, there are

$$6(5-1) = 24$$

elements in G of order 5.

(ii) Let n_3 denote the number of 3-Sylow subgroups. Then by Sylow III,

$$n_3 \equiv 1 \pmod{3} \text{ and } n_3 \mid 20 \Rightarrow n_3 \in \{1, 4, 10\}$$

If $n_3 = 4$, then $[G : N_G(P)] = 4$ where P is any 3-Sylow subgroup. Since

$$60 \nmid 4!$$

we conclude from 5.3 that G is not simple. This is a contradiction. Hence,

$$n_3 = 10$$

Once again, this implies that there are

$$10(3-1) = 20$$

elements of order 3.

(iii) Let n_2 denote the number of 2-Sylow subgroups. Then by Sylow III,

$$n_2 \equiv 1 \pmod 2 \text{ and } n_2 \mid 15 \Rightarrow n_2 \in \{1, 3, 5, 15\}$$

(a) If $n_2 = 1$, then the Sylow subgroup is normal. This is not possible.

(b) If $n_2 = 3$, then

$$[G : N_G(Q)] = 3$$

where Q is any fixed $2-$Sylow subgroup. Once again, since $60 \nmid 3!$, this is impossible by 5.3.

(c) If $n_2 = 5$: Fix a 2-Sylow subgroup Q and set $H := N_G(Q)$. Then $[G : H] = 5$, so the action of left-multiplication on $X := G/H$ induces a group homomorphism

$$f : G \to S_5$$

Furthermore, $\ker(f) \subset H$, so $\ker(f) \neq G$. Since G is simple, $\ker(f) = \{e\}$. Hence, f is injective. Now consider the map $\varphi : G \to \{\pm 1\}$ given by

$$\varphi = sgn \circ f$$

Then φ is a group homomorphism. If $\ker(\varphi) = \{e\}$, then φ would be injective. But this is absurd because

$$|G| = 60 > 2 = |\{\pm 1\}|$$

Since G is simple, it follows that $\ker(\varphi) = G$. Hence,

$$f(G) \subset \ker(sgn) = A_5$$

Since $|f(G)| = 60 = |A_5|$, we conclude that

$$f : G \to A_5$$

is an isomorphism.

(d) If $n_2 = 15$: Let P be a fixed 2-Sylow subgroup and $x \in P$ such that $x \neq e$. Consider

$$H := Z(x)$$

Since $|P| = 4$, P is Abelian. Hence, $P \subset H$. Hence,

$$k := [G : H] \mid [G : P] = \frac{60}{4} = 15 \Rightarrow k \in \{1, 3, 5, 15\}$$

- If $k = 1$, then $G = H = Z(x)$. In which case, $x \in Z(G)$, so

$$K := \langle x \rangle \lhd G$$

  This contradicts the assumption that G is simple.

- If $k = 3$, then $|G| \nmid 3!$, so this would contradict Lemma 5.3.

- If $k = 5$, then G has a subgroup of order 5. The same argument as above would imply that $G \cong A_5$
- If $k = 15$, then $[G : H] = [G : P]$, in which case $P = H$: So suppose

$$G \ncong A_5$$

Then, for any 2-Sylow subgroup P and any $x \in P, x \neq e$, we have

$$P = Z(x)$$

In particular, if P and Q are any two Sylow subgroups, suppose $P \cap Q \neq \{e\}$, then let

$$x \in P \cap Q$$

As before, we have $P = Z(x) = Q$. Hence, any two distinct 2-Sylow subgroups must intersect trivially. Therefore, the number of elements of order 2 or 4 is

$$15(4 - 1) = 45$$

Thus the number of elements in G exceeds 60 by the calculations in Steps (i) and (ii).

□

6. Finite Abelian Groups

Notation: In this section, all groups will be finite and Abelian. In this case, we write the group operation as $+$, and we write $-g := g^{-1}$.

6.1. Remark/Definition:

(i) If G is an Abelian group and p a prime dividing $|G|$, then G has a unique p-Sylow subgroup H.

(a) If $x \in H$, then $O(x)$ is a power of p since $O(x) \mid |H|$

(b) If $x \in G$ such that $O(x)$ is a power of p, then $K := \langle x \rangle$ is a p-group. By Corollary 3.14, $K \subset H$, so $x \in H$.

Hence,

$$G(p) := \{x \in G : O(x) \text{ is a power of } p\}$$

is called the p-primary component of G.

(ii) If $G = H \times K$ and p is a prime, then

$$G(p) = \{(x, y) \in H \times K : O(x) \text{ and } O(y) \text{ is a power of } p\} = H(p) \times K(p)$$

6.2. Lemma : Let G be a finite abelian, then G is isomorphic to the direct product of its Sylow subgroups.

Proof. Consider the decomposition into prime factors of $m := |G|$:

$$m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

Let $G(p_1), G(p_2), \dots, G(p_k)$ be the Sylow subgroups of G. Let $G' := G(p_1) \times G(p_2) \times \dots \times G(p_k)$ and define $\varphi : G' \to G$ by

$$\varphi(x_1, x_2, \dots, x_k) := x_1 + x_2 + \dots + x_k$$

(i) φ is a homomorphism because G is Abelian.

(ii) φ is injective: If $\varphi(x_1, x_2, \dots, x_k) = e$, then

$$-x_1 = x_2 + \dots + x_k \in G(p_1) \cap G(p_2) \dots G(p_{k-1}) =: K$$

Since $x_i \in G(p_i)$, it follows that $\exists \ell_i \in \mathbb{N}$ such that

$$p_i^{\ell_i}(x_i) = 0 \quad \forall 1 \leq i \leq k$$

Let $n := \prod_{i=2}^{k} p_i^{\ell_i}$, then

$$n(-x_1) = nx_2 + \dots + nx_k = 0$$

But $x_1 \in G(p_1)$, so if $x_1 \neq 0$, then $p_1 \mid O(x_1)$ so $p_1 \mid n$, which is false. Hence,

$$x_1 = x_2 + \dots + x_k = 0$$

Now by induction it follows that $x_i = 0$ for all i, so φ is injective.

(iii) φ is surjective: $|G| = |G'|$

□

(End of Day 27)

6.3. Lemma: Let G be a finite Abelian p-group and let $b \in G$ and $r \in \mathbb{N}$ such that

$$p^r b \neq 0$$

Suppose $O(p^r b) = p^m$. Then

$$O(b) = p^{r+m}$$

Proof. Clearly,

$$p^{r+m} b = p^m (p^r b) = 0$$

and if $p^n b = 0$, then $n \geq r$ because $p^r b \neq 0$. Hence,

$$0 = p^{n-r}(p^r b) = 0 \Rightarrow p^m \mid p^{n-r} \Rightarrow m \leq n - r$$

Hence $n \geq r + m$. Hence, $O(b) = p^{r+m}$ □

6.4. Lemma: Let G be a finite Abelian p-group and let $a \in G$ be an element of maximal order. Define

$$H := \langle a \rangle$$

and let $\pi : G \to G/H$ be the quotient map. For any $y \in G/H, \exists x \in G$ such that

$$\pi(x) = y \text{ and } O(x) = O(y)$$

Proof. Suppose $O(a) = p^k$, and $O(y) = p^r$, then choose $b \in G$ such that $b + H = y$, so

$$p^r(b + H) = p^r b + H = H \Rightarrow p^r b \in H$$

Hence, $\exists n \in \mathbb{N}$ such that $p^r b = na$. Now write

$$n = p^\ell m \text{ where } p \nmid m$$

(i) If $\ell \geq k$, then $na = p^\ell ma = 0$. In this case,

$$p^r b = 0 \Rightarrow O(b) \leq p^r = O(y)$$

But by Lemma 2.3,

$$O(y) = O(\pi(b)) \mid O(b)$$

Hence, $O(b) = p^r$, so $x = b$ works.

(ii) If $\ell < k$, then

$$p^r b = na = p^\ell ma \neq 0$$

Furthermore, by Mid-Sem Q6,

$$O(p^r b) = O(p^\ell ma) = \frac{O(a)}{\gcd(O(a), p^\ell m)} = \frac{p^k}{\gcd(p^k, p^\ell m)} = \frac{p^k}{p^\ell} = p^{k-\ell}$$

Hence by the previous lemma, $O(b) = p^{r+k-\ell}$. Now $O(a)$ is maximal. Hence,

$$r + k - \ell \leq k \Rightarrow r \leq \ell$$

Hence define

$$x := b - p^{\ell - r} ma$$

so one has

$$x + H = b + H = y \Rightarrow p^r = O(y) \leq O(x)$$

However,

$$p^r x = p^r b - p^\ell ma = p^r b - na = 0$$

Hence, $O(x) = p^r$ as required.

$\square$

6.5. Lemma: Suppose G is a finite Abelian group, and there is an isomorphism

$$\varphi : G \to G_1 \times G_2 \times \ldots \times G_k =: G'$$

Define $\widehat{G_i} < G'$ as in Lemma 1.2, and set

$$H_i := \varphi^{-1}(\widehat{G_i})$$

Then every $x \in G$ can be uniquely expressed as a sum

$$x = x_1 + x_2 + \ldots + x_k$$

where $x_i \in H_i$. Furthermore, observe that $H_i \cong G_i$

Proof. (i) Existence: Let $x \in G$, then $\varphi(x) = (a_1, a_2, \ldots, a_k)$ for some $a_i \in G_i$. Set

$$x_i := \varphi^{-1}(0, 0, \ldots, 0, a_i, 0, \ldots, 0) \in \varphi^{-1}(\widehat{G_i}) = H_i$$

Then

$$\varphi(x) = \varphi(x_1) + \varphi(x_2) + \ldots + \varphi(x_k) = \varphi(x_1 + x_2 + \ldots + x_k)$$

Since φ is injective, we get that $x = x_1 + x_2 + \ldots + x_k$

(ii) Uniqueness: If

$$x_1 + x_2 + \ldots + x_k = y_1 + y_2 + \ldots + y_k$$

with $x_i, y_i \in H_i$, then

$$x_1 - y_1 = (y_2 + y_3 + \ldots + y_k) - (x_2 + x_3 + \ldots + x_k)$$

Applying φ, we see that

$$(a_1 - b_1, 0, 0, \ldots, 0) = (0, b_2 - a_2, b_3 - a_3, \ldots, b_k - a_k)$$

where $a_i = \varphi(x_i)$ and $b_i = \varphi(y_i)$. Hence,

$$a_i = b_i \quad \forall i \Rightarrow x_i = y_i$$

□

(End of Day 28)

6.6. (Fundamental Theorem of Finite Abelian Groups - Existence): Every finite Abelian group is a direct product of cyclic groups.

Proof. By Lemma 6.2, it suffices to prove the result for a finite Abelian p-group. So let G be a p-group, and we induct on $|G|$. If $|G| = 1$ there is nothing to prove, so assume that the result is true for any finite Abelian p-group G' such that $|G'| < |G|$.

Let $x_1 \in G$ be an element of maximal order, and let $H_1 := \langle x_1 \rangle$. Set $G' := G/H_1$ and let $\pi : G \to G'$ be the quotient map. By hypothesis, we may express

$$G' \cong L_2 \times L_3 \times \ldots \times L_s$$

for some cyclic groups L_i. By the previous lemma, there are cyclic subgroups $K_i < G'$ such that, every $z \in G'$ has a unique expression of the form

$$z = z_2 + \ldots + z_s \qquad (*)$$

where $z_i \in K_i$. Let $p^{r_i} = |K_i|$ and let y_i be its generator. By the previous lemma, $\exists x_i \in G$ such that

$$O(x_i) = p^{r_i} \text{ and } \pi(x_i) = y_i$$

Let $H_i := \langle x_i \rangle$. We claim that

$$G \cong H_1 \times H_2 \times \ldots \times H_s$$

Define $L := H_1 \times H_2 \times \ldots \times H_s$ and define $\varphi : L \to G$ by

$$(a_1, a_2, \ldots, a_s) \mapsto a_1 + a_2 + \ldots + a_s$$

Then φ is clearly a homomomorphism.

(i) φ is injective: Suppose $a_i \in H_i$ such that $a_1 + a_2 + \ldots + a_s = 0$, then $\exists m_i \in \mathbb{Z}$ such that $a_i = m_i x_i$, so we get

$$m_1 x_1 + m_2 x_2 + \ldots + m_s x_s = 0$$

Applying the quotient map to this expression, we get an equation in G'

$$\pi(0) = m_2 \pi(x_2) + \ldots + m_s \pi(x_s) = \pi(0) + \ldots + \pi(0)$$

But by the uniqueness of the expression in $(*)$, we get

$$m_i \pi(x_i) = \pi(0) \Rightarrow O(\pi(x_i)) = p^{r_i} \mid m_i \quad \forall 2 \leq i \leq s$$

But $O(x_i) = p^{r_i}$, so

$$a_i = m_i x_i = 0 \quad \forall 2 \leq i \leq s$$

Hence, the above expression yields $a_1 = m_1 x_1 = 0$ as well.

(ii) φ is surjective: If $x \in G$, then by $(*), \exists m_i \in \mathbb{N}$ such that

$$\pi(x) = m_2 \pi(x_2) + \ldots m_s \pi(x_s)$$

Hence,

$$x - m_2 x_2 - m_3 x_3 - \ldots - m_s x_s \in H_1 = \langle x_1 \rangle$$

Hence, $\exists m_1 \in \mathbb{N}$ such that

$$x - m_2 x_2 - m_3 x_3 - \ldots - m_s x_s = m_1 x_1$$

so $x = m_1 x_1 + m_2 x_2 + \ldots + m_s x_s \in \text{Image}(\varphi)$.

□

6.7. (Fundamental Theorem of Finite Abelian Groups - Uniqueness): The decomposition from the previous theorem is unique upto permutation.

Proof. Suppose that

$$G \cong \prod_{i=1}^{k} G_i \cong \prod_{j=1}^{\ell} H_j$$

where each G_i and H_j are cyclic groups. Then for any prime p, by Remark 6.1,

$$G(p) \cong \prod_{i=1}^{k} G_i(p) \cong \prod_{j=1}^{\ell} H_j(p)$$

Hence, it suffices to prove uniqueness for p-groups. So suppose G is a finite Abelian p-group, and write

$$G \cong G_1 \times G_2 \times \ldots \times G_k$$

where each G_i is a cyclic group of order p^{r_i} and $r_1 \geq r_2 \geq \ldots \geq r_k$. Furthermore, suppose

$$G \cong H_1 \times H_2 \times \ldots \times H_m$$

where each H_j is a cyclic group of order p^{ℓ_j} and $\ell_1 \geq \ell_2 \geq \ldots \geq \ell_m$. Then ,we WTS:

(i) $m = k$

(ii) $\ell_i = r_i$ for all $1 \leq i \leq k$

So induct on $|G|$. Consider

$$pG \cong pG_1 \times pG_2 \times \ldots \times pG_k$$

Then $pG < G$ is a proper subgroup of G and is of type

$$(p^{r_1-1}, p^{r_2-1}, \ldots, p^{r_k-1})$$

with the convention that, if $r_i = 1$, then $pG_i = 0$. Similarly,

$$pG \cong pH_1 \times pH_2 \times \ldots pH_m$$

Hence it follows by induction that if $r_i \geq 2$ or $m_i \geq 2$. In this case, we have

$$r_i = m_i$$

Hence, the two decompositions are of the type

$$(p^{r_1}, p^{r_2}, \ldots, p^{r_j}, \underbrace{p, p, \ldots, p}_{s \text{ times}}) \text{ and } (p^{r_1}, p^{r_2}, \ldots, p^{r_j}, \underbrace{p, p, \ldots, p}_{t \text{ times}})$$

Comparing orders, we see that

$$|G| = p^{r_1+r_2+\ldots+r_j} p^s = p^{r_1+r_2+\ldots+r_j} p^t \Rightarrow s = t$$

□

6.8. Example :

(i) Abelian groups of order 5^4 are

(a) $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

(b) $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$

(c) $\mathbb{Z}_5 \times \mathbb{Z}_{125}$

(d) $\mathbb{Z}_{25} \times \mathbb{Z}_{25}$

(e) $\mathbb{Z}_{625}$

(ii) Abelian groups of order 100 are

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$

(c) $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

(d) $\mathbb{Z}_4 \times \mathbb{Z}_{25} \cong \mathbb{Z}_{100}$

(End of Day 29)

7. Semi-Direct Products

7.1. Remark: Let G be a group and $H, K < G$ such that $H \lhd G$. Then $HK < G$. It is possible that

$$G = HK$$

but $G \ncong H \times K$ (See Example 1.12). However, there is a map

$$\psi : K \to \mathrm{Aut}(H) \text{ given by } \psi(k)(h) := khk^{-1}$$

and $G \cong H \times K$ if and only if ψ is trivial. ie. $khk^{-1} = h$ for all $k \in K, h \in H$ (For instance, this happened in Corollary 2.9). We now wish to understand the situation when G is non-Abelian (and ψ is non-trivial).

7.2. Theorem: Let H and K be two groups, and let $\varphi : K \to \mathrm{Aut}(H)$ be a group homomorphism. Define

$$G := H \times K$$

with group multiplication given by

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1\varphi(k_1)(h_2), k_1k_2)$$

Then G is a group, and is called the semi-direct product of H and K. It is denoted by

$$H \rtimes_\varphi K$$

Proof. Clearly $\cdot$ is a binary operation on G. We now check the axioms:

(i) Associativity: Let $(h_i, k_i) \in G$ for $i = 1, 2, 3$, then

$$\begin{aligned}(h_1, k_1) \cdot [(h_2, k_2) \cdot (h_3, k_3)] &= (h_1, k_1) \cdot (h_2\varphi(k_2)(h_3), k_2k_3) \\ &= (h_1\varphi(k_1)(h_2\varphi(k_2)(h_3), k_1k_2, k_3) \\ &= (h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3), (k_1k_2)k_3) \\ &= (h_1\varphi(k_1)(h_2), k_1k_2) \cdot (h_3, k_3) \\ &= [(h_1, k_1) \cdot (h_2, k_2)] \cdot (h_3, k_3)\end{aligned}$$

(ii) Identity: Let e_H and e_K denote the identities in H and K respectively. Then, for any $(h, k) \in G$,

$$(h, k) \cdot (e_H, e_K) = (h\varphi(k)(e_H), ke_K) = (he_H, k) = (h, k)$$

and

$$(e_H, e_K) \cdot (h, k) = (e_H\varphi(e_K)(h), e_Kk) = (e_Hh, k) = (h, k)$$

(iii) Inverse: Let $(h, k) \in G$, then consider $(h', k') := (\varphi(k^{-1})(h^{-1}), k^{-1})$, so

$$\begin{aligned}(h, k) \cdot (h', k') &= (h\varphi(k)(\varphi(k^{-1}(h^{-1})), kk^{-1}) \\ &= (h\varphi(kk^{-1})(h^{-1}), e_K) \\ &= (h\varphi(e_K)(h^{-1}), e_K) \\ &= (hh^{-1}, e_K) = (e_H, e_K)\end{aligned}$$

Similarly, one can verify that $(h', k') \cdot (h, k) = (e_H, e_K)$.

□

7.3. Lemma: Let $G = H \rtimes_\varphi K$, then

(i) $|G| = |H||K|$

(ii) Define $\widehat{H} := \{(h, e_2) : h \in H\}$ and $\widehat{K} := (e_1, k) : k \in K\}$. Then $\widehat{H}$ and $\widehat{K}$ are subgroups of G. Furthermore, $H \cong \widehat{H}$ and $K \cong \widehat{K}$

(iii) $\widehat{H} \lhd G$

(iv) $\widehat{H} \cap \widehat{K} = \{(e_1, e_2)\}$. Hence, $G = \widehat{H}\widehat{K}$

(v) For all $k \in K$ and $h \in H$, we have

$$(e_1, k)(h, e_2)(e_1, k)^{-1} = (\varphi(k)(h), e_2)$$

Identifying H with $\widehat{H}$ and K with $\widehat{K}$ this reads,

$$khk^{-1} = \varphi(k)(h)$$

Proof. (i) Obvious.

(ii) Let $(h_1, e_K), (h_2, e_K) \in \widehat{H}$, then

$$(h_1, e_K) \cdot (h_2, e_K)^{-1} = (h_1, e_K) \cdot (h_2^{-1}, e_K) = (h_1 h_2^{-1}, e_K) \in \widehat{H}$$

Hence, $\widehat{H} < G$. Simlarly, $\widehat{K} < G$. Furthermore, the above argument shows that the map

$$\psi : H \to \widehat{H} \text{ given by } h \mapsto (h, e_K)$$

is a homomorphism. It is clearly bijective, so it is an isomorphism. Similarly, $K \cong \widehat{K}$ as well [Check!].

(iii) If $(h, k) \in G$ and $(x, e_K) \in \widehat{H}$, then

$$(h, k)^{-1} \cdot (x, e_K) \cdot (h, k) = (z, e_K) \in \widehat{H}$$

for some $z \in H$. Hence, $\widehat{H} \lhd G$

(iv) Obvious by a cardinality argument.

(v) Check!

□

7.4. Examples:

(i) If $G = H \times K$, then $G = H \rtimes_\varphi K$ where $\varphi : K \to \mathrm{Aut}(H)$ is the trivial map

$$\varphi(k)(h) = h \quad \forall k \in K, h \in H$$

(ii) If $G = D_n = \langle r, s \rangle$ and $H := \langle r \rangle$ and $K = \langle s \rangle$. Define $\varphi : K \to \mathrm{Aut}(H)$ by

$$\varphi(s)(r^j) := s r^j s^{-1} = r^{-j}$$

Then $G \cong H \rtimes_\varphi K$

Proof. Consider $a := (r, e) \in \widehat{H}$ and $b := (e, s) \in \widehat{K}$, then [Check!]

$$\begin{aligned} a^n &= (r^n, e) = (e, e) \\ b^2 &= (e, s^2) = (e, e) \\ bab^{-1} &= (\varphi(s)(r), e) = (srs^{-1}, e) = a^{-1} \end{aligned}$$

Hence there is a unique group homomorphism $\varphi : D_n \to G$ such that

$$\varphi(r) = a \text{ and } \varphi(s) = b$$

Since $G = \widehat{H}\widehat{K} = \langle a, b \rangle$, the map is surjective. Furthermore,

$$|D_n| = 2n = |\widehat{H}||\widehat{K}| = 2n$$

so φ is injective as well. □

(End of Day 30)

7.5. Theorem: Let G be a group and $H, K < G$ such that

(i) $H \lhd G$

(ii) $H \cap K = \{e\}$

Then $\exists \varphi : K \to \mathrm{Aut}(H)$ such that $HK \cong H \rtimes_\varphi K$

[Compare this with Theorem 1.13]

Proof. Since $H \lhd K$, for each $k \in K$, we have $kHk^{-1} = H$. Hence, we define

$$\varphi : K \to \mathrm{Aut}(H) \text{ given by } k \mapsto \varphi_k$$

where $\varphi_k(h) := khk^{-1}$. Then φ is clearly a homomorphism. Set $G' := H \rtimes_\varphi K$ and define $\mu : G' \to HK$ by

$$(h, k) \mapsto hk$$

(i) μ is a homomomorphism: If $(h_1, k_1), (h_2, k_2) \in G'$, then

$$\begin{aligned}
\mu((h_1, k_1) \cdot (h_2, k_2)) &= \mu((h_1\varphi(k_1)(h_2), k_1k_2)) \\
&= h_1\varphi(k_1)(h_2)k_1k_2 \\
&= h_1(k_1h_2k_1^{-1})k_1k_2 \\
&= (h_1k_1)(h_2k_2) \\
&= \mu((h_1, k_1))\mu((h_2, k_2))
\end{aligned}$$

(ii) μ is injective: If $\mu(h, k) = e$, then $hk = e$, so

$$h = k^{-1} \in H \cap K = \{e\} \Rightarrow h = k = e$$

(iii) μ is surjective: Since $H \lhd G$, we have $HK < G$, so

$$|HK| = \frac{|H||K|}{|H \cap K|} = |H||K| = |G'|$$

Hence, μ is surjective.

□

7.6. Theorem: Let H and K be groups and $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then TFAE:

(i) The identity map

$$H \rtimes_\varphi K \to H \times K$$

is a group homomorphism.

(ii) φ is the trivial homomorphism

(iii) $\widehat{K} \lhd H \rtimes_\varphi K$

Proof. [(i)$\Rightarrow$ (ii):] By definition of the group operation, it follows that, for any $(h_i, k_i) \in H \times K$, we have

$$(h_1\varphi(k_1)(h_2), k_1k_2) = (h_1h_2, k_1k_2)$$

Hence, $\varphi(k_1)(h_2) = h_2$ for all $k_1 \in K$ and $h_2 \in H$. Hence, $\varphi(k) = \mathrm{id}_H$ for all $k \in K$.

[(ii)$\Rightarrow$ (iii):] If φ is the trivial homomorphism, then for any $(h, k) \in H \rtimes_\varphi K$ and $(e, k') \in \widehat{K}$, we have

$$(h, k)^{-1} = (\varphi(k^{-1})(h^{-1}), k^{-1}) = (h^{-1}, k^{-1})$$

so

$$\begin{aligned}(h, k) \cdot (e, k') \cdot (h, k)^{-1} &= (h\varphi(k)(e), kk') \cdot (h^{-1}, k^{-1}) \\ &= (h, kk')(h^{-1}, k^{-1}) \\ &= (h\varphi(kk')(h^{-1}), kk'k^{-1}) \\ &= (hh^{-1}, kk'k^{-1}) = (e, kk'k^{-1}) \in \widehat{K}\end{aligned}$$

Hence, $\widehat{K} \lhd H \rtimes_\varphi K$

[(iii)$\Rightarrow$ (i):] Note that $\widehat{H} \cap \widehat{K} = \{e\}$,

$$\widehat{H} \lhd H \rtimes_\varphi K =: G \text{ and } \widehat{H}\widehat{K} = G$$

If $\widehat{K} \lhd H \rtimes_\varphi K$, then it follows by Theorem 1.13 that

$$H \rtimes_\varphi K \cong \widehat{H} \times \widehat{K} \cong H \times K$$

Furthermore, the isomorphism is explicitly given by

$$((h, e), (e, k)) \mapsto (h, e) \cdot (e, k) = (h\varphi(e)(e), k) = (h, k)$$

Hence, the identity map is an isomorphism. In particular, a homomorphism.

□

8. Meta-Cyclic Groups

8.1. Example: Let p, q be two primes such that $p < q$ and let G be a group of order pq.

(i) Suppose $p \nmid (q-1)$: Then, $\exists H, K < G$ such that $|H| = q$ and $|K| = p$. By the Strong Cayley theorem,

$$H \lhd G$$

Also, $H \cap K = \{e\}$. Hence, $G = HK$. Furthermore, by theorem 7.5, $\exists \varphi : K \to \mathrm{Aut}(H)$ such that

$$G \cong H \rtimes_\varphi K$$

However, $|K| = p$ and $|\mathrm{Aut}(H)| = q - 1$. Since $p \nmid (q-1)$, φ must be trivial. Hence, by 7.6,

$$G \cong H \times K \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$$

(ii) Now suppose $p \mid (q-1)$: Then by Cauchy's theorem, $\exists H' < \mathrm{Aut}(H)$ such that

$$|H'| = p$$

Hence, there exists a non-trivial homomorphism

$$\varphi : K \to \mathrm{Aut}(H)$$

that maps K isomorphically onto H'. By 7.6,

$$H \rtimes_\varphi K$$

is a group of order pq that is not isomorphic to $H \times K$. Furthermore, K is not normal in G, so this group is non-Abelian. We wish show later that this group is the only such group upto isomorphism, and is called the meta-cyclic group of order pq.

(iii) Note: If $p = 2$ and q is an odd prime, then by Theorem 4.3,

$$\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_2 \cong D_{2p}$$

8.2. Lemma: Let p be a prime and $r \in \mathbb{N}$, then there are atmost r elements in $\mathbb{Z}_p$ which satisfy the equation

$$a^r = 1$$

Proof. Omitted. This will be done in a course on Field theory. □

(End of Day 31)

8.3. Definition: Let $p \in \mathbb{Z}$ a prime and $d \in \mathbb{Z}$. Write $N_p(d)$ for the number of elements in $\mathbb{Z}_p^*$ of order d. Note that

$$N_p(1) = 1$$

and $N_p(d) > 0$ implies that $d \mid (p-1)$. Observe that

$$\sum_{d|(p-1)} N_p(d) = p - 1$$

8.4. Lemma: Let $d \mid (p-1)$ and $N_p(d) > 0$, then $N_p(d) = \varphi(d)$

Proof. If $N_p(d) > 0$, then $\exists x \in \mathbb{Z}_p^*$ such that $O(x) = d$. Consider the equation

$$a^d = 1$$

Then $1, x, x^2, \ldots, x^{d-1}$ are all distinct elements that satisfy this equation. By Lemma 8.1, these must be all the solutions to that equation. Hence, if $y \in \mathbb{Z}_p^*$ has order d, then

$$y = x^i \text{ for some } 0 \leq i \leq d-1$$

Now by Mid-Sem Q6,

$$d = O(y) = O(x^i) = \frac{d}{\gcd(d, i)}$$

Hence, $\gcd(d, i) = 1$. Hence, the elements of order d are precisely

$$\{x^i : \gcd(d, i) = 1\}$$

There are exactly $\varphi(d)$ such numbers. □

8.5. Theorem: For any $n \in \mathbb{N}$, we have

$$\sum_{d|n} \varphi(d) = n$$

Proof. Consider $G = \langle a \rangle \cong \mathbb{Z}_n$ be a cyclic group of order n. For each $d \mid n$, consider

$$S_d = \{x \in G : O(x) = d\}$$

By Mid-Sem Q6, G has a unique subgroup H of order d generated by $z := a^{n/d}$. Hence,

$$S_d \subset H$$

Hence, if $x \in S_d$, then $\exists i \in \mathbb{N}$ such that $x = z^i$, so

$$d = O(x) = O(z^i) = \frac{O(z)}{\gcd(O(z), i)} = \frac{d}{\gcd(d, i)} \Rightarrow \gcd(d, i) = 1$$

Once again, we conclude that

$$|S_d| = \varphi(d)$$

Now note that

$$G = \bigsqcup_{d|n} S_d$$

so we get the result. □

8.6. Corollary: For any prime p, $\mathrm{Aut}(\mathbb{Z}_p)$ is cyclic.

Proof. Note that

$$\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$$

Now applying Theorem 8.5 with $n = p - 1$, we see that

$$\sum_{d|(p-1)} \varphi(d) = p - 1 = \sum_{d|(p-1)} N_p(d) \leq \sum_{d|(p-1)} \varphi(d)$$

Hence, we conclude that $N_p(d) = \varphi(d)$ for all $d \mid (p - 1)$. In particular,

$$N_p(p - 1) = \varphi(p - 1) > 0$$

By definition, this implies that $\mathbb{Z}_p^*$ contains an element of order $(p - 1)$. Thus, it is cyclic. □

8.7. Lemma: Let H and K be groups.

(i) Let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism and $\tau : K \to K$ be an automorphism. Then

$$H \rtimes_{\varphi \circ \tau} K \cong H \rtimes_{\varphi} K$$

(ii) Let φ_1 and $\varphi_2 : K \to \mathrm{Aut}(H)$ be two injective homomomorphisms such that

$$\varphi_1(K) = \varphi_2(K)$$

Then

$$H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$$

Proof. (i) Let $G_1 := H \rtimes_{\varphi \circ \tau} K$ and $G_2 := H \rtimes_{\varphi} K$. Define

$$\mu : G_1 \to G_2 \text{ by } (h, k) \mapsto (h, \tau(k))$$

Then we claim that μ is an isomorphism. Since μ is clearly bijective, it suffices to show that it is a homomorphism. To see this, let $(h_1, k_1), (h_2, k_2) \in G_1$, then

$$\begin{aligned}
\mu((h_1, k_1) \cdot (h_2, k_2)) &= \mu(h_1 \varphi \circ \tau(k_1)(h_2), k_1 k_2) \\
&= (h_1 \varphi(\tau(k_1))(h_2), \tau(k_1 k_2)) \\
&= (h_1 \varphi(\tau(k_1))(h_2), \tau(k_1)\tau(k_2)) \\
&= (h_1, \tau(k_1)) \cdot (h_2, \tau(k_2))
\end{aligned}$$

(ii) Now suppose $\varphi_1(K) = \varphi_2(K)$, then define $\tau : K \to K$ by

$$\tau := \varphi_1^{-1} \circ \varphi_2$$

Then $\tau \in \mathrm{Aut}(K)$, and clearly

$$\varphi_1 \circ \tau = \varphi_2$$

So part (ii) follows from part (i).

□

8.8. Theorem: Let p and q be two primes such that $p \mid (q - 1)$. Then there is a unique non-Abelian group of order pq. This is called the meta-cyclic group of order pq and is written as

$$\mathbb{Z}_q \rtimes \mathbb{Z}_p$$

Proof. Let G be a non-Abelian group of order pq, then as argued before, $\exists H \lhd G$ and $K < G$ such that $|H| = q, |K| = p$ and

$$G \cong H \rtimes_{\varphi} K$$

for some homomorphism $\varphi : K \to \mathrm{Aut}(H)$. Since G is non-Abelian, φ is non-trivial. Since $|K| = p$, φ must be injective. Hence,

$$\varphi(K) < \mathrm{Aut}(H)$$

is a subgroup of order p. However, $\mathrm{Aut}(H)$ is cyclic, so it has a unique subgroup of order p (Mid-Sem Q6). Hence, if $\psi : K \to \mathrm{Aut}(H)$ is any other non-trivial homomomorphism, we have

$$\varphi(K) = \psi(K)$$

So by Lemma 8.7,

$$H \rtimes_\varphi K \cong H \rtimes_\psi K$$

Thus, upto isomorphism, there is only one such group. □

8.9. Corollary: Let p and q be two primes, and G be a group of order pq.

(i) If $p = q$, then G must be one of

$$\mathbb{Z}_{p^2} \text{ or } \mathbb{Z}_p \times \mathbb{Z}_p$$

(ii) If $p < q$ and $p \nmid (q-1)$, then G must be $\mathbb{Z}_{pq}$

(iii) If $p < q$ and $p \mid (q-1)$, then G must be one of

$$\mathbb{Z}_{pq} \text{ or } \mathbb{Z}_q \rtimes \mathbb{Z}_p$$

(End of Day 32)

9. Groups of Small Order

a. Groups of Order 8

9.1. Remark: Let G be a group of order 8.

(i) If G is Abelian, then G is isomorphic to one of

- $\mathbb{Z}_8$
- $\mathbb{Z}_4 \times \mathbb{Z}_2$, or
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

(ii) The group of isometries of a square, D_4 is a group of order 8. As in Section 4, write r and s for the two elements that generate D_4. They satisfy

$$r^4 = s^2 = e \text{ and } srs^{-1} = r^3$$

Note that $H := \langle r \rangle$ has order 4, and thus $H \lhd G$. Let $K := \langle s \rangle$, then

$$G \cong H \rtimes_\varphi K$$

by Theorem 7.5. Furthermore, since G is non-Abelian, K is not normal in G by Theorem 7.6.

(iii) The quaternion group Q_8 is the group of 8 complex matrices

$$Q_8 = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$$

where

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

By HW 3.10, every subgroup of Q_8 is normal in Q_8. In particular, it follows that

$$D_4 \ncong Q_8$$

(iv) Set $a := \mathbf{i}$ and $b := \mathbf{j}$. Then (Check!)

(a) $a^4 = 1$

(b) $b^2 = a^2$

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

(d) $Q_8 = \{a^n b^m : 0 \leq n < 4, 0 \leq m < 2\}$

Proof. Let $H = \langle a \rangle$ and $K = \langle b \rangle$, then by the first two steps,

$$|H| = O(a) = 4 = O(b) = |K|$$

Hence, $H \lhd G$, so $HK < G$. Furthermore, $H \neq K$ since a and b do not commute. Hence, by part (b),

$$H \cap K = \{a^2, e\}$$

Hence,

$$|HK| = \frac{|H||K|}{|H \cap K|} = 8 \Rightarrow G = HK$$

Hence,

$$Q_8 = \{a^n b^m : 0 \leq n < 4, 0 \leq m < 4\}$$

However, $b^3 = b^2 b = a^2 b$. Hence, we see that

$$Q_8 = \{a^n b^m : 0 \leq n < 4, 0 \leq m < 2\}$$

as required. □

9.2. Theorem Let G be a group with two elements $a, b \in G$ such that

$$a^4 = e, b^2 = a^2 \text{ and } b^{-1}ab = a^{-1}$$

Then there is a unique group homomorphism $\varphi : Q_8 \to G$ such that

$$\varphi(\mathbf{i}) = a \text{ and } \varphi(\mathbf{j}) = b$$

Proof. Similar to Theorem 4.2 □

9.3. Lemma: Let G be a group such that

$$(ab)^2 = a^2b^2 \quad \forall a, b \in G$$

Then G is Abelian.

Proof. It follows by hypothesis that

$$(ab)(ab) = aabb \Rightarrow ba = ab$$

for all $a, b \in G$. □

9.4. Theorem: The only non-Abelian groups of order 8 are Q_8 and D_4.

Proof. (i) Let G be a non-Abelian group of order 8. For any $a \in G, O(a) \in \{1, 2, 4, 8\}$. Since G is not cyclic, there is no element of order 8. If every element in G had order 2, then

$$(ab)^2 = e = a^2b^2 \quad \forall a, b \in G$$

By the previous lemma, this would imply that G is Abelian. Hence, $\exists a \in G$ such that $O(a) = 4$.

(ii) Set

$$H := \langle a \rangle$$

Then $|H| = 4$, so $H \lhd G$.

(iii) Let $b \in G \setminus H$. Then consider the quotient map $\pi : G \to G/H$. Since $b \notin H$, $\pi(b) \neq H$. However, $|G/H| = 2$, so

$$\langle bH \rangle = G/H$$

So if $x \in G$, then $\pi(x) \in \langle bH \rangle$. Hence, $\exists m \in \{0, 1\}$ such that $x \in b^m H$. Hence, $b^{-m}x \in H$, so $\exists n \in \mathbb{N}$ such that

$$b^{-m}x = a^n \Rightarrow x = a^n b^m$$

So G is generated by a and b.

(iv) Since $H \lhd G$, $bab^{-1} \in H$. Since $O(bab^{-1}) = O(a)$, it follows that

$$bab^{-1} = a \text{ or } bab^{-1} = a^3$$

If $bab^{-1} = a$, then $ba = ab$. Since G is generated by a and b, it follows that G is Abelian. This is a contradiction. Hence,

$$bab^{-1} = a^3 = a^{-1}$$

(v) Furthermore,

$$\pi(b^2) = \pi(b)^2 = H \Rightarrow b^2 \in H$$

If $b^2 = a$, then $O(b^2) = 4$, so $O(b) = 8$. This implies that G is cyclic, which it is not. Hence, $b^2 \neq a$. Similarly, if $b^2 = a^3$, then

$$O(b^2) = O(a^3) = \frac{O(a)}{\gcd(O(a), 3)} = \frac{4}{\gcd(4, 3)} = 4$$

which would imply that $O(b) = 8$ - a contradiction. Hence, it follows that

$$b^2 = e \text{ or } b^2 = a^2$$

Since $bab^{-1} = a^{-1}$, we have by Theorems 4.2 and 9.2, that

$$G \cong \begin{cases} D_4 & : b^2 = e \\ Q_8 & : b^2 = a^2 \end{cases}$$

□

9.5. Remark: There are no proper subgroups $H, K < Q_8$ such that

$$Q_8 \cong H \rtimes_\varphi K$$

Proof. Suppose $Q_8 \cong H \rtimes_\varphi K$, then $\widehat{K} < Q_8$. Every subgroup of Q_8 is normal, so $\widehat{K} \lhd Q_8$, but this implies by Theorem 7.6 that

$$Q_8 \cong H \times K$$

But if $H < G$ is proper, then $|H| \leq 4$, so H is Abelian. Similarly, K is Abelian, so Q_8 would be Abelian - a contradiction. □

b. Groups of order 12

9.6. Remark: Let G be a group of order 12.

(i) If G is Abelian, then G is one of

- $\mathbb{Z}_{12}$
- $\mathbb{Z}_2 \times \mathbb{Z}_6$

(ii) We know two other groups of order 12, A_4 and D_6. Note that D_6 has a subgroup of order 6. Since A_4 does not, $D_6 \ncong A_4$.

(iii) Note that, in A_4, there are many 3-Sylow subgroups

$$\{e, (123), (132)\}, \{e, (124), (142)\}, \text{ etc.}$$

Hence, A_4 does not have a normal 3-Sylow subgroup.

9.7. Lemma: Let G be a finite group and $a, b \in G$ such that $ab = ba$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$. Then

$$O(ab) = \operatorname{lcm}(O(a), O(b))$$

Proof. Exercise. $\square$

(End of Day 33)

9.8. Example: Note that $\operatorname{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_3^* \cong \mathbb{Z}_2$, so write

$$\operatorname{Aut}(\mathbb{Z}_3) = \{e, \epsilon\}$$

Let $\tau : \mathbb{Z}_4 \to \operatorname{Aut}(\mathbb{Z}_2)$ be the map

$$\tau([j]) = \epsilon^j$$

Then τ is a well-defined surjective homomorphism. Define

$$T := \mathbb{Z}_3 \rtimes_\tau \mathbb{Z}_3$$

(i) T is a non-Abelian group of order 12.

(ii) Notice that $[2] \in \ker(\tau)$. Hence,

$$([0], [2]) \cdot ([1], [0]) = ([1], [2])$$

and $\tau([2])([1]) = [1]$, so

$$([1], [0]) \cdot ([0], [2]) = ([1], [2])$$

Hence, $([0], [2])$ and $([1], [0])$ commute. Also, by the isomorphism in Lemma 7.3

$$O([0], [2]) = 2 \text{ and } O([1], [0]) = 3$$

By Lemma 9.6, $O([1], [2]) = 6$. Since A_4 does not have an element of order 6, it follows that

$$T \ncong A_4$$

(iii) Also, $O([0], [1]) = 4$. In D_6, there is no element of order 4 (Check!), so

$$T \ncong D_6$$

9.9. Lemma: Let G be a group of order 12. If G does not have a normal 3-Sylow subgroup, then $G \cong A_4$.

Proof. Let P be a 3-Sylow subgroup of G and n_3 be the number of 3-Sylow subgroups in G. Then

$$n_3 \equiv 1 \pmod 3 \text{ and } n_3 \mid 4$$

Suppose P is not normal, then $n_3 = 4$. Hence

$$4 = [G : N_G(P)] = [G : P] \Rightarrow P = N_G(P)$$

Let G act on $X := G/P$ by left multiplication. This gives a group homomorphism

$$f : G \to S_4$$

such that $\ker(f) \subset P$. Since P is not normal in G, $\ker(f) \neq P$. Since $|P| = 3$, it follows that

$$\ker(f) = \{e\}$$

Hence, f is injective. Hence, $f(G) < S_4$ is a subgroup of order 12. By HW 3.18,

$$f(G) = A_4$$

so $G \cong A_4$. □

9.10. Lemma: Let $K = \mathbb{Z}_2 \times \mathbb{Z}_2$, then $\mathrm{Aut}(K) \cong S_3$

Proof. Write $K = \{e, a_1, a_2, a_3\}$ where $a_1 = ([0],[1]), a_2 = ([1],[0])$ and $a_3 = ([1],[1])$. Then

$$a_1a_2 = a_3, a_1a_3 = a_2, \text{ and } a_2a_3 = a_1 \qquad (*)$$

S_3 acts on H by

$$(\sigma, e) \mapsto e \text{ and } (\sigma, a_i) \mapsto a_{\sigma(i)}$$

This gives a map

$$f : S_3 \to S_K$$

which is clearly injective. Furthermore, if $\sigma \in S_3$, then

$$\sigma(a_1a_2) = \sigma(a_3) = a_{\sigma(3)}$$

One can check that for each $\sigma \in S_3$,

$$a_{\sigma(3)} = a_{\sigma(1)}a_{\sigma(2)}$$

by the equation $(*)$. Hence, $f(S_3) \subset \mathrm{Aut}(K)$. Finally, if $\varphi \in \mathrm{Aut}(K)$, then $\varphi : K \to K$ is bijective, and $\varphi(e) = e$. Hence, φ is a permutation on the set $\{a_1, a_2, a_3\}$. Hence, $\varphi \in f(S_3)$, so f is surjective.

Thus, $f : S_3 \to \mathrm{Aut}(K)$ is an isomorphism. □

9.11. Theorem: There are, upto isomorphism, only three non-Abelian groups of order 12, viz. A_4, D_6 and T.

Proof. Since these three groups are not isomorphic to each other, it suffices to show that there are atmost 3 non-Abelian groups of order 12. Let G be such a group and assume $G \ncong A_4$. Let $H, K < G$ be subgroups with

$$|H| = 3 \text{ and } |K| = 4$$

Since $G \ncong A_4$, then $H \lhd G$, so $HK < G$. Since $H \cap K = \{e\}$, it follows that

$$G = HK \cong H \rtimes_\varphi K$$

for some map $\varphi : K \to \mathrm{Aut}(H)$. Since G is non-Abelian, and H and K are Abelian, it follows that φ is non-trivial. Since $|\mathrm{Aut}(H)| = 2$, φ is surjective, and write

$$\mathrm{Aut}(H) = \{e, \epsilon\}$$

(i) Case 1: $K \cong \mathbb{Z}_4$, then since φ is surjective and non-zero, it follows that

$$\varphi([1]) = \epsilon \Rightarrow \varphi([j]) = \epsilon^j$$

Hence, $G \cong T$ by construction.

(ii) Case 2: $K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then write

$$K = \{e, a_1, a_2, a_3\}$$

as before. Suppose that $i, j \in \{1, 2, 3\}$ such that

$$\varphi(a_i) = \epsilon \text{ and } \varphi(a_j) = e$$

Then, by 9.10, there is a $\tau \in \mathrm{Aut}(K)$ such that

$$\tau(a_1) = a_i \text{ and } \tau(a_2) = a_j$$

Set $\psi = \varphi \circ \tau$, then $\psi(a_1) = \epsilon$ and $\psi(a_2) = e$, and hence $\psi(a_3) = \psi(a_1 a_2) = \epsilon$. Thus, for any non-trivial $\varphi : K \to \mathrm{Aut}(H)$, there is a $\tau \in \mathrm{Aut}(K)$ such that

$$\varphi \circ \tau = \psi$$

By 8.7,

$$H \rtimes_\varphi K \cong H \rtimes_\psi K$$

so there is only one group in this case (and in fact, it must be D_6)

□

(End of Day 34)

c. Groups of order ≤ 15

Order of G	Abelian	Non-Abelian	Reference
1	$\{0\}$	None	-
2, 3, 5, 7, 11, 13	$\mathbb{Z}_p$	None	I.2.6, I.4.3
4, 9	$\mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p$	None	IV.1.14
6, 10, 14	$\mathbb{Z}_{2p}$	D_p	IV.4.3
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_8$	D_4, Q_8	Section IV.6, IV.9.4
12	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6$	A_4, D_6, T	Section IV.6, IV.9.11
15	$\mathbb{Z}_{15}$	None	IV.2.9

Review for Final Exam.

(End of Day 35)

V. Instructor Notes

0.1. Overall, the course structure is sound, and doesn't need any tinkering at all.

0.2. This semester, because of all the holidays I got only 35 lectures, which is way less than ideal. If I had had a few more lectures, I could have discussed solvability and composition series as well.

Bibliography

[Artin] M. Artin, *Algebra, 2nd Ed.*

[Herstein] I.N. Herstein, *Topics in Algebra, 2nd Ed.*

[Gallian] J.A. Gallian, *Contemporary Abstract Algebra, 7th Ed.*

[Conrad] K. Conrad, http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/Ansimple.pdf