CHAPTER S

EXAMPLES OF GROUPS

S.1. Cyclic groups

Definition S.1.1. —
- A **cyclic group** is a group G that contains an element $g \in G$ such that the group generated by g is G, $\langle g \rangle = G$.

The following facts follow from the definition.

(1) If G is cyclic with generator g then all elements of G are of the form
$$g^k = \underbrace{g \cdot g \cdots g}_{k \text{ times}} \qquad \text{or} \qquad g^{-k} = \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{k \text{ times}}$$
with $k \in \mathbb{Z}_{\geqslant 0}$.

(2) If G is cyclic with generator g and G is finite and $\mathrm{Card}(G) = n$ then
$$G = \{1, g, g^2, \ldots, g^{n-1}\}.$$

(3) If G is cyclic then G is abelian since if $i, j \in \mathbb{Z}$ then $g^i g^j = g^{i+j} = g^j g^i$.

(4) If G is cyclic then all subgroups of G are normal since G is abelian.

HW: Let G be a group of order p, where p is a prime. Show that G is cyclic.

S.1.1. The integers $\mathbb{Z}$. —

Definition S.1.2. —
- The group of **integers** $\mathbb{Z}$ is the set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ with the operation of addition.

HW: Show that $\mathbb{Z}$ is an abelian group.

HW: Show that both the element $1 \in \mathbb{Z}$ and the element $-1 \in \mathbb{Z}$ generate $\mathbb{Z}$.

HW: Show that $\mathbb{Z}$ is a cyclic group.

HW: Show that every element of $\mathbb{Z}$ is in a conjugacy class by itself.

Notes of Arun Ram aram@unimelb.edu.au, Version: 4 April 2020

S.1.1.1. Subgroups and cosets. —

Theorem S.1.1. —

(a) *Let H be a subset of the integers $\mathbb{Z}$. Then H is a subgroup of $\mathbb{Z}$ if and only if there exists $m \in \mathbb{Z}_{\geqslant 0}$ such that $H = m\mathbb{Z}$.*
(b) *Let $m, n \in \mathbb{Z}_{\geqslant 0}$. Then $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if n divides m.*
(c) *Let $n \in \mathbb{Z}_{\geqslant 0}$. Then the quotient group $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group with n elements.*

HW: Show that every subgroup of $\mathbb{Z}$ is normal subgroup of $\mathbb{Z}$.

Example. The subgroup $5\mathbb{Z}$ of the integers $\mathbb{Z}$ consists of all multiples of 5.

$$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}.$$

The subgroup $15\mathbb{Z}$ is contained in the subgroup $5\mathbb{Z}$.

$$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} \quad \supseteq \quad 15\mathbb{Z} = \{\ldots, -30, -15, 0, 15, 30, \ldots\}.$$

The sets

$$\begin{aligned}
&0 + 5\mathbb{Z} = 5 + 5\mathbb{Z} = 10 + 5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\} = 5\mathbb{Z},\\
&1 + 5\mathbb{Z} = -4 + 5\mathbb{Z} = -9 + 5\mathbb{Z} = \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\},\\
&2 + 5\mathbb{Z} = 32 + 5\mathbb{Z} = -23 + 5\mathbb{Z} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, 27, 32, \ldots\},\\
&3 + 5\mathbb{Z} = -7 + 5\mathbb{Z} = 8 + 5\mathbb{Z} = \{\ldots, -7, -2, 3, 8, 13, \ldots\},\\
&4 + 5\mathbb{Z} = 404 + 5\mathbb{Z} = -236 + 5\mathbb{Z} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$

are cosets of the subgroup $5\mathbb{Z}$ in the group $\mathbb{Z}$. In fact

$$\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$$

is the set of cosets of $5\mathbb{Z}$ in $\mathbb{Z}$. As a group $\mathbb{Z}/5\mathbb{Z}$ is a cyclic group with 5 elements.

S.1.1.2. Homomorphisms. —

Proposition S.1.2. — *A function $f\colon \mathbb{Z} \to \mathbb{Z}$ is a group homomorphism if and only if there exists $m \in \mathbb{Z}$ such that $f = \varphi_m$, where*

$$\begin{array}{rccc} \varphi_m\colon & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & mn, \end{array} \qquad \text{for } m \in \mathbb{Z}.$$

HW: Show that $\ker \varphi_m = \mathbb{Z}$ if $m = 0$.

HW: Show that φ_m is injective if $m \neq 0$.

HW: Show that φ_m is bijective if and only if $m = 1$ or $m = -1$.

HW: Show that $\varphi_1 = \mathrm{id}_{\mathbb{Z}}$, is the identity mapping.

HW: Show that the automorphism group of $\mathbb{Z}$, $\mathrm{Aut}(\mathbb{Z}) = \{\varphi_1, \varphi_{-1}\} \simeq \mathcal{Z}_2$.

HW: Show that inner automorphisms of $\mathbb{Z}$ are $\mathrm{Inn}(\mathbb{Z}) = \{\varphi_1\}$.

S.1.1.3. Presentations. —

Proposition S.1.3. — *The group of integers $\mathbb{Z}$ is isomorphic to the free group on one generator.*

S.1.2. The finite cyclic groups μ_n. —

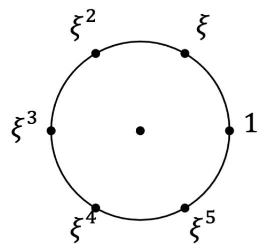
Definition S.1.3. — Let $n \in \mathbb{Z}_{\geqslant 1}$ and let g be a symbol. If $a \in \mathbb{Z}$ let $a \bmod n$ denote the element $r \in \{0, 1, \ldots, n-1\}$ such that $a = bn + r$ with $b \in \mathbb{Z}$.

- The **cyclic group of order** n, or n**-clock**, is the set

$$\mathcal{Z}_n = \{1, g, g^2, \ldots, g^{n-1}\} \qquad \text{with the operation given by} \qquad g^i g^j = g^{(i+j) \bmod n}.$$

There are other favorite instances of the n-clock.

(1) Let μ_n be the group given by $\mu_n = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$, where $\xi = e^{\frac{2\pi i}{n}} \in \mathbb{C}$, with the operation of multiplication of complex numbers. In the complex plane the elements of μ_n all lie on the circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.



The group μ_5

(2) Let $\mathbb{Z}/n\mathbb{Z}$ be the group given by $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ with operation given by $\bar{i} + \bar{j} = \overline{(i+j) \bmod n}$. This operation is **addition modulo** n.

HW: Show that the group homomorphism $\phi \colon \mathcal{Z}_n \to \mu_n$ given by $\phi(g^i) = \xi^i$ is an isomorphism.

HW: Show that the group homomorphism $\varphi \colon \mu_n \to \mathbb{Z}/n\mathbb{Z}$ given by $\varphi(\xi^i) = \bar{i}$ is an isomorphism.

S.1.2.1. Subgroups and cosets. —

Theorem S.1.4. — *Let $n \in \mathbb{Z}_{\geqslant 1}$ and let $\mathcal{Z}_n = \{1, g, \ldots, g^{n-1}\}$ be the n-clock.*

(a) The subgroups of $\mathcal{Z}_n$ are the subgroups generated by the elements g^m,

$$\langle g^m \rangle \qquad \text{with} \quad m \in \{0, 1, \ldots, n-1\}.$$

(b) Let $m \in \{0, 1, \ldots, n-1\}$ and let $d = \gcd(m, n)$. Then

$$\langle g^m \rangle = \langle g^d \rangle \quad \text{where } d = \gcd(m,n), \quad \text{and} \qquad \mathrm{Card}(\langle g^d \rangle) = n/d.$$

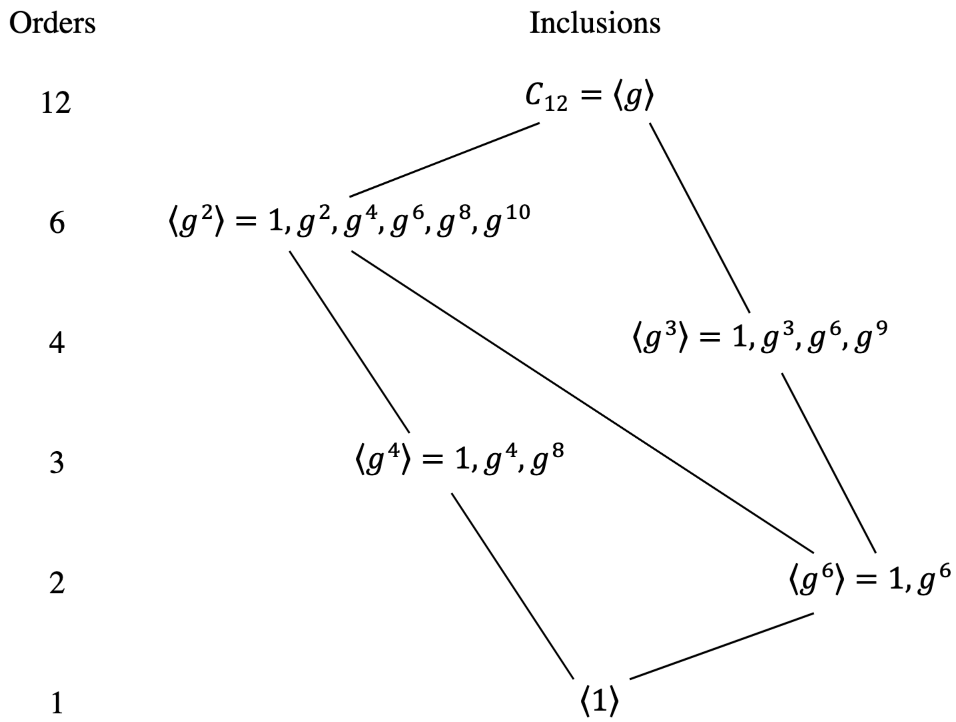
(c) Let $m, k \in \{0, 1, \ldots, n-1\}$. Then

$$\langle g^m \rangle \subseteq \langle g^k \rangle \quad \text{if and only if} \quad \gcd(k, n) \text{ divides } \gcd(m, n).$$

(d) Let $d \in \{0, 1, \ldots, n\}$ and suppose that d divides n. Then the quotient group

$$\frac{\mathcal{Z}_n}{\langle g^d \rangle} \simeq \mathcal{Z}_{n/d}.$$

Example. The subgroup lattice of the group $\mathcal{Z}_{12}$ is given by: FIX THIS PICTURE



The set of cosets $\mathcal{Z}_{12}/\langle g^3 \rangle = \{H, gH, g^2H\}$, where

$$H = \{1, g^3, g^6, g^9\}, \qquad gH = \{g, g^4, g^7, g^{10}\}, \qquad \text{and} \qquad g^2H = \{g^2, g^5, g^8, g^{11}\}.$$

Proposition S.1.5. — *Let $\mathbb{C}^\times = \mathbb{C} - \{0\}$ with the operation of multiplication of complex numbers and let n be a positive integer. Every homomorphism from $\mathcal{Z}_n$ to $\mathbb{C}^\times$ is of the form*

$$\begin{array}{rccc} \varphi_k\colon & \mathcal{Z}_n & \to & \mathbb{C}^\times \\ & g & \mapsto & \xi^k \end{array} \qquad \textit{where} \quad \xi = e^{\frac{2\pi i}{n}} \ \textit{and}\ k \in \{0, 1, \ldots, n-1\}.$$

S.1.2.2. Presentation. —

Proposition S.1.6. — *The cyclic group $\mathcal{Z}_n$ has a presentation with generator g and relation*

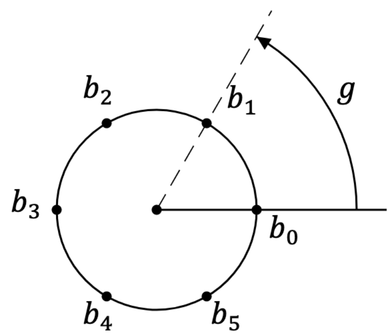
$$g^n = 1.$$

S.1.2.3. The action of $\mathcal{Z}_n$ on an n-necklace. —

Proposition S.1.7. — *Let S be a circular necklace with n equally spaced beads $b_0, b_1, \ldots, b_{n-1}$, numbered counterclockwise around S.*

(a) *There is an action of the cyclic group $\mathcal{Z}_n$ on the necklace S such that g acts by rotating S counterclockwise by an angle of $2\pi/n$.*

(b) *This action has one orbit, $\mathcal{Z}_n b_0 = \{b_0, b_1, \ldots, b_{n-1}\}$ and the stabilizer of each bead is the subgroup* (1).


b_2
b_1
g
b_3
b_0
b_4
b_5

S.2. The dihedral groups D_n, $n \geqslant 2$

Definition S.2.1. —
- The **dihedral group** is the set $D_n = \{1, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}$ with the operation given by

$$(x^iy^j)(x^ky^l) = x^{(i+k) \bmod n}y^{(j+l) \bmod 2}.$$

HW: Show that the cardinality of the dihedral group D_n is $2n$.

Proposition S.2.1. — *The orders of the elements in the dihedral group D_n are*

$$o(1) = 1, \qquad o(x^k) = \gcd(k, n), \qquad \textit{and} \qquad o(x^ky) = 2 \quad \textit{for } k \in \{0, 1, \ldots, n-1\}.$$

S.2.1. Conjugacy classes, normal subgroups, and the center. —

Proposition S.2.2. —
(a) *The conjugacy classes of the dihedral group D_2 are the sets*

$$\mathcal{C}_1 = \{1\}, \qquad \mathcal{C}_x = \{x\}, \qquad \mathcal{C}_y = \{y\}, \qquad \textit{and} \qquad \mathcal{C}_{xy} = \{xy\}.$$

(b) *If n is even and $n \neq 2$, then the conjugacy classes of the dihedral group D_n are the sets*

$$\mathcal{C} = \{1\}, \qquad \mathcal{C}_{x^{n/2}} = \{x^{n/2}\}, \qquad \mathcal{C}_{x^k} = \{x^k, x^{-k}\}, \quad \textit{for } k \in \{0, 1, \ldots, n/2\},$$

$$\mathcal{C}_y = \{y, x^2y, x^4y, \ldots, x^{n-2}y\}, \qquad \mathcal{C}_{xy} = \{xy, x^3y, x^5y, \ldots, x^{n-1}y\}.$$

(c) *If n is odd then the conjugacy classes of the dihedral group D_n are the sets*

$$\mathcal{C}_1 = \{1\}, \qquad \mathcal{C}_{x^k} = \{x^k, x^{-k}\} \quad \textit{for } k \in \{0, 1, \ldots, n/2\}, \quad \textit{and}$$

$$\mathcal{C}_y = \{y, xy, x^2y, x^3y, \ldots, x^{n-1}y\}.$$

Proposition S.2.3. — *Let $\langle a, b, \cdots \rangle$ denote the subgroup generated by elements $a, b, \ldots$.*
(a) *The normal subgroups of the dihedral group D_2 are the subgroups*

$$\langle x \rangle, \qquad \langle y \rangle \qquad \textit{and} \qquad \langle xy \rangle.$$

(b) *If n is even and $n \neq 2$ then the normal subgroups of the dihedral group D_n are the subgroups*

$$\langle x^k \rangle \quad \textit{for } k \in \{0, 1, \ldots, n-1\} \qquad \textit{and} \quad \langle x^2, y \rangle \quad \textit{and} \quad \langle x^2, xy \rangle.$$

(c) *If n is odd then the normal subgroups of the dihedral group D_n are the subgroups*

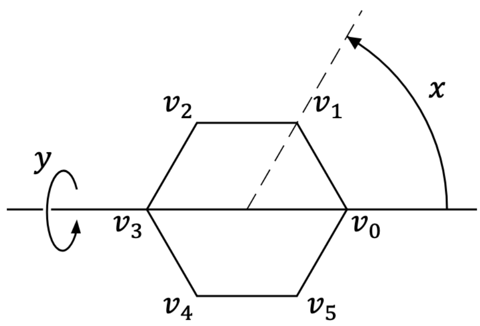
$$\langle x^k \rangle \quad \textit{for } k \in \{1, \ldots, n-1\}.$$

Proposition S.2.4. —
(a) *The center of the dihedral group D_2 is the subgroup $Z(D_2) = D_2$.*
(b) *If n is even and $n \neq 2$ then the center of the dihedral group D_n is the subgroup $Z(D_n) = \{1, x^{n/2}\}$.*
(c) *If n is odd then the center of the dihedral group D_n is the subgroup $Z(D_n) = \{1\}$.*

S.2.2. The action of D_n on an n-gon. —

Proposition S.2.5. — *Let F be an n-gon with vertices $v_0, v_1, \ldots, v_{n-1}$ numbered counterclockwise around F. Then there is an action of the group D_n on the n-gon F such that*

x acts by rotating the n-gon by an angle of $2\pi/n$;
y acts by reflecting about the line which contains the vertex v_0 and the center of F.



S.2.3. Generators and relations. —

Theorem S.2.6. — *The dihedral group D_n has a presentation by generators x, y and relations*

$$x^n = 1, \quad y^2 = 1, \quad \text{and} \quad yx = x^{-1}y.$$

S.3. The symmetric groups S_m

Definition S.3.1. —

- Let $\mathbb{Z}_{[1,m]}$ denote the set $\{1, 2, \ldots, m\}$. A **permutation** of m is a bijective map
$$\sigma\colon \quad \mathbb{Z}_{[1,m]} \to \mathbb{Z}_{[1,m]}.$$
- The **symmetric group** S_m is the set of permutations of m with the operation of composition of functions.

HW: Show that the cardinality of the symmetric group S_m is $m! = m(m-1)(m-2)\cdots 2{\cdot}1$.

There are several convenient ways of representing a permutation σ.

(1) As a two line array $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & m \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(m) \end{pmatrix}$.
(2) As a one line array $\sigma = \big(\sigma(1)\sigma(2)\ldots\sigma(m)\big)$.
(3) As an $m \times m$ matrix which has the $\big(\sigma(i), i\big)^{\text{th}}$ entry equal to 1 for all i and all other entries equal to 0.
(4) As a function diagram consisting of two rows, of m dots each, such that the i^{th} dot of the upper row is connected by an edge to the $\sigma(i)^{\text{th}}$ dot of the lower row.
(5) In cycle notation, as a collection of sequences $(i_1, i_2, \ldots, i_k)$ such that $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots,$ $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$. We often leave out the cycles containing only one element when we write σ in cycle notation.

HW: Show that, in function diagram notation, the product $\tau\sigma$ of two permutations τ and σ is given by placing the diagram of σ above the diagram of τ and connecting the bottom dots of σ to the top dots of τ.

HW: Show that, in function diagram notation, the identity permutation is represented by m vertical lines.

HW: Show that, in function diagram notation, σ^{-1} is represented by the diagram of σ flipped over.

HW: Show that, in matrix notation, the product $\tau\sigma$ of two permutations τ and σ is given by matrix multiplication.

HW: Show that, in matrix notation, the identity permutation is the diagonal matrix with all 1's on the diagonal.

HW: Show that, in matrix notation, the matrix of σ^{-1} is the transpose of the matrix of σ.

HW: Show that the matrix of a permutation is always an orthogonal matrix.

S.3.1. Sign of a permutation. —

Proposition S.3.1. — *For each permutation $\sigma \in S_m$, let* $\det(\sigma)$ *denote the determinant of the matrix which represents the permutation σ. The map*
$$\begin{array}{rccc} \varepsilon\colon & S_m & \to & \{\pm 1\} \\ & \sigma & \mapsto & \det(\sigma) \end{array}$$
is a homomorphism from the symmetric group S_m to the group $\mu_2 = \{\pm 1\}$.

Notes of Arun Ram aram@unimelb.edu.au, Version: 7 April 2020

Definition S.3.2. —
• The **sign homomorphism** of the symmetric group S_m is the homomorphism

$$\begin{array}{cccc} \varepsilon\colon & S_m & \to & \{\pm 1\} \\ & \sigma & \mapsto & \det(\sigma) \end{array}$$

where $\det(\sigma)$ denote the determinant of the matrix which represents the permutation σ.
• The **sign** of a permutation σ is the determinant $\varepsilon(\sigma)$ of the permutation matrix representing σ.
• A permutation σ is **even** if $\varepsilon(\sigma) = +1$ and is **odd** if $\varepsilon(\sigma) = -1$.

S.3.2. Conjugacy Classes. —

Definition S.3.3. —
• A **partition** $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ of m is a weakly decreasing sequence of positive integers which sum to m, i.e.

$$\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k > 0, \qquad \text{and} \qquad \sum_{i=1}^{k} \lambda_i = m.$$

The elements of a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ are the **parts** of the partition λ. Sometimes we represent a partition λ in the form $\lambda = (1^{m_1} 2^{m_2} \cdots)$ if λ has m_1 1's, m_2 2's, and so on. Write $\lambda \vdash m$ if λ is a partition of m.
• The **cycles** of a permutation σ are the ordered sequences $(i_1, i_2, \dots, i_k)$ such that $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$.
• The **cycle type** $\tau(\sigma)$ of a permutation $\sigma \in S_m$ is the partition of m determined by the sizes of the cycles of σ.

Example. A permutation σ can have several different representations in cycle notation. In cycle notation,

$$(12345)(67)(89)(10), \qquad (51234)(67)(89), \qquad (45123)(67)(89)(10),$$
$$(34512)(89)(67), \quad \text{and} \quad (34512)(10)(98)(67)$$

all represent the same permutation in S_{10}, which, in two line notation, is given by

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

Example. If σ is the permutation in S_9 which is given, in cycle notation, by

$$\sigma = (1362)(587)(49)$$

and π is the permutation in S_9 which is given, in 2-line notation, by

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

then $\pi\sigma\pi^{-1}$ is the permutation which is given, in cycle notation, by

$$\pi\sigma\pi^{-1} = (4196)(582)(37) = (1964)(258)(37).$$

Theorem S.3.2. —
(a) *The conjugacy classes of S_m are the sets*

$$\mathcal{C}_\lambda = \{ \textit{ permutations } \sigma \textit{ with cycle type } \lambda\},$$

where λ is a partition of m.

(b) *If* $\lambda = (1^{m_1}2^{m_2}\cdots)$ *then the size of the conjugacy class* $\mathcal{C}_\lambda$ *is*

$$\mathrm{Card}(\mathcal{C}_\lambda) = \frac{m!}{m_1!1^{m_1}m_2!2^{m_2}m_3!3^{m_3}\cdots}.$$

The proof of Theorem S.3.2 will use the following lemma.

Lemma S.3.3. — *Suppose* $\sigma \in S_m$ *has cycle type* $\lambda = (\lambda_1, \lambda_2, \ldots)$ *and let* γ_λ *be the permutation in* S_m *which is given, in cycle notation, by*

$$\gamma_\lambda = (1, 2, \cdots, \lambda_1)(\lambda_1+1, \lambda_1+2, \ldots, \lambda_1+\lambda_2)(\lambda_1+\lambda_2+1, \cdots)\cdots.$$

(a) *Then* σ *is conjugate to* γ_λ.
(b) *If* $\tau \in S_m$ *is conjugate to* σ *then* τ *has cycle type* λ.
(c) *Suppose that* $\lambda = (1^{m_1}2^{m_2}\cdots)$. *Then the order of the stabilizer of the permutation* γ_λ, *under the action of* S_m *on itself by conjugation, is*

$$1^{m_1}m_1!2^{m_2}m_2!\cdots.$$

Example. The sequence $\lambda = (66433322111)$ is a partition of 32 and can also be represented in the form $\lambda = (1^3 2^2 3^3 4\, 5^0 6^2) = (1^3 2^2 3^3 4\, 6^2)$. The conjugacy class

$$\mathcal{C}_\lambda \quad \text{in } S_{32} \quad \text{has} \quad \frac{32!}{1^3\cdot 3!\cdot 2^2\cdot 2!\cdot 3^3\cdot 3!\cdot 4\cdot 6^2\cdot 2!} \quad \text{elements.}$$

S.3.3. Generators and relations. —

Definition S.3.4. —
- The **simple transpositions** in S_m are the elements $s_i = (i, i+1)$, $1 \leqslant i \leqslant m-1$.

Proposition S.3.4. —
(a) S_m *is generated by the simple transpositions* s_i, $1 \leqslant i \leqslant m-1$.
(b) *The simple transpositions* s_i, $1 \leqslant i \leqslant m-1$, *in* S_m *satisfy the relations*

$$\begin{aligned} s_is_j &= s_js_i, && \text{if } j \notin \{i-1, i+1\},\\ s_is_{i+1}s_i &= s_{i+1}s_is_{i+1}, && \text{if } i \in \{1, \ldots, m-2\},\\ s_i^2 &= 1, && \text{if } i \in \{1, \ldots, m-1\}. \end{aligned}$$

Definition S.3.5. —
- A **reduced word** for $\sigma \in S_m$ is an expression

$$\sigma = s_{i_1}\ldots s_{i_p}$$

of σ as a product of simple transpositions such that the number of factors is as small as possible.
- The **length** $\ell(\sigma)$ of σ is the number of factors in a reduced word for the permutation σ.
- The set of **inversions** of σ is the set

$$\mathrm{inv}(\sigma) = \{(i,j) \mid i, j \in \{1, \ldots, m\},\ i < j \text{ and } \sigma(i) > \sigma(j)\}.$$

HW: Show that the sign $\varepsilon(s_i)$ of a simple transposition s_i in the symmetric group S_n is -1.

Proposition S.3.5. — *Let* σ *be a permutation. Let* $\ell(\sigma)$ *be the length of* σ *and let* $\mathrm{inv}(\sigma)$ *be the set of inversions of the permutation* σ. *Then*
(a) *The sign of* σ *is* $\varepsilon(\sigma) = (-1)^{\ell(\sigma)}$.
(b) $Card(\mathrm{inv}(\sigma)) = \ell(\sigma)$

(c) *The number of crossings in the function diagram of* σ *is* $\ell(\sigma)$.

Theorem S.3.6. — *The symmetric group* S_m *has a presentation by generators,* $s_1, s_2, \ldots, s_{m-1}$ *and relations*

$$\begin{aligned} s_i s_j &= s_j s_i, && \text{if } j \notin \{i-1, i+1\}, \\ s_i s_{i+1} s_i &= s_{i+1} s_i s_{i+1}, && \text{if } i \in \{1, \ldots, m-2\}, \\ s_i^2 &= 1, && \text{if } i \in \{1, \ldots, m-1\}. \end{aligned}$$

S.4. Alternating group

Definition S.4.1. —
- The **alternating group** A_n is the subgroup of even permutations of S_n.

Proposition S.4.1. — *The alternating group A_n is the kernel of the sign homomorphism of the symmetric group;*

$$A_n = \ker(\varepsilon), \qquad \textit{where} \qquad \begin{matrix} \varepsilon\colon & S_n & \to & \{\pm 1\} \\ & \sigma & \mapsto & \det(\sigma). \end{matrix}$$

HW: Show that A_n is a normal subgroup of S_n.

HW: Show that $\mathrm{Card}(A_n) = n!/2$.

S.4.1. Conjugacy classes. — Since A_n is a normal subgroup of S_n, A_n is a union of conjugacy classes of S_n. Let $\mathcal{C}_\lambda$ be a conjugacy class of S_n corresponding to a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$. Then the following Proposition says:

(1) The conjugacy class $\mathcal{C}_\lambda$ is contained in A_n if an even number of the λ_i are even numbers.
(2) If the parts λ_i of λ are all odd and are all distinct then $\mathcal{C}_\lambda$ is a union of two conjugacy classes of A_n and these two conjugacy classes have the same size.
(3) Otherwise $\mathcal{C}_\lambda$ is also a conjugacy class of A_n.

Proposition S.4.2. — *Suppose that $\sigma \in A_n$. Let $\mathcal{C}_\sigma$ denote the conjugacy class of σ in S_n and let $\mathcal{A}_\sigma$ denote the conjugacy class of σ in A_n.*
(a) *Then σ has an even number of cycles of even length.*
(b)

$$\mathrm{Card}(\mathcal{A}_\sigma) = \begin{cases} \dfrac{\mathrm{Card}(\mathcal{C}_\sigma)}{2}, & \textit{if all cycles } \sigma \textit{ are of different odd lengths,} \\ \mathrm{Card}(\mathcal{C}_\sigma), & \textit{otherwise.} \end{cases}$$

The proof of Proposition (1.4.2) uses the following lemma.

Lemma S.4.3. — *Let $\sigma \in A_n$ and let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ be the cycle type of σ. Let γ_λ be the permutation given, in cycle notation, by*

$$\gamma_\lambda = (1, 2, \cdots, \lambda_1)(\lambda_1 + 1, \lambda_1 + 2, \ldots, \lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + 1, \cdots) \cdots .$$

Let S_σ denote the stabilizer of σ under the action of S_n on itself by conjugation. Then,
(a) *$S_\sigma \subseteq A_n$ if and only if $S_{\gamma_\lambda} \subseteq A_n$.*
(b) *$S_{\gamma_\lambda} \subseteq A_n$ if and only if γ_λ has all odd cycles of different lengths.*

S.4.2. A_n is simple if $n \neq 4$. — A group is simple if it has no nontrivial normal subgroups. The trivial normal subgroups are the whole group and the subgroup containing only the identity element.

Theorem S.4.4. —
(a) *If $n \neq 4$ then A_n is simple.*
(b) *The alternating group A_4 has a single nontrivial proper normal subgroup given by*

$$N = \{(1234), (2143), (3412), (4321)\},$$

where the permutations are represented in one-line notation.

Notes of Arun Ram aram@unimelb.edu.au, Version: 4 April 2020

The proof of Theorem (1.4.4) uses the following lemma.

Lemma S.4.5. — *Suppose N is a normal subgroup of A_n, $n > 4$, and N contains a 3-cycle. Then $N = A_n$.*

S.5. Exercises for symmetric groups

Exercise 1.14.1. Let σ be a permutation in S_m. Show that the order of σ is the least common multiple of the lengths of its cycles.

Exercise 1.14.2. Show that the center $Z(S_2) = S_2$ and that if $m \in \mathbb{Z}_{>2}$ then the center $Z(S_m) = (1)$.

Exercise 1.14.3.

(a) Show that the proper normal subgroups of S_4 are

$$N = \{XXXXX\}$$

(1) and the alternating group A_4.

(b) Show that if $m \neq 4$ then the only proper normal subgroup of S_m is the alternating group A_m.

Exercise 1.14.3. Let $\{\varepsilon_1, \ldots, \varepsilon_m\}$ be a basis of $\mathbb{C}^m$. Let S_m act on the vectors ε_i by

$$\sigma\varepsilon_i = \varepsilon_{\sigma(i)}.$$

Define the sets of vectors

$$\Phi^+ = \{\varepsilon_i - \varepsilon_j \mid i, j \in \{1, \ldots, m\} \text{ and } i < j\} \quad \text{and} \quad \Phi^- = \{\varepsilon_j - \varepsilon_i \mid i, j \in \{1, \ldots, m\} \text{ and } i < j\}$$

to be the sets of **positive roots** and **negative roots** respectively. Show that the length $\ell(\sigma)$ of a permutation σ is the same as the number of positive roots that are taken to negative roots by the action of σ.

S.6. Exercises for alternating groups

Exercise 1.14.4. Let σ be an element of A_m.
Show that the order of σ is the least common multiple of the lengths of the cycles of σ.

Exercise 1.14.5. What is the center of A_m?

Exercise 1.14.6. Suppose that $\sigma \in A_m$. How can one tell if σ is conjugate to γ_λ in A_m?

Exercise 1.14.7. Show that the elements γ_μ, $\mu \vdash n$, and the elements $s_1\gamma_\mu s_1^{-1}$, where $\mu \vdash n$ is a partition with all parts odd and distinct, are a set of representatives of the conjugacy classes of A_n.

S.7. Proofs for cyclic groups

Theorem S.7.1. —
(a) *Let H be a subset of the integers $\mathbb{Z}$. Then H is a subgroup of $\mathbb{Z}$ if and only if there exists $m \in \mathbb{Z}_{\geqslant 0}$ such that $H = m\mathbb{Z}$.*
(b) *Let m and n be positive integers. Then $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if n divides m.*
(c) *Let n be a positive integer. Then the quotient group $\mathbb{Z}/n\mathbb{Z} \simeq \mathcal{Z}_n$.*

Proof. —
To show: (a) If H is a subgroup of $\mathbb{Z}$ then there exists $m \in \mathbb{Z}_{\geqslant 0}$ such that $H = m\mathbb{Z}$.
(b) If m is a positive integer then $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. □

Theorem S.7.2. — *Let $\mathcal{Z}_n$ be the cyclic group of order n generated by g.*
(a) *The subgroups of the cyclic group $\mathcal{Z}_n$ are $\langle g^m \rangle$, $0 \leqslant m \leqslant n-1$.*
(b) *Let $m \in \{0, 1, \ldots, n-1\}$ and let $d = \gcd(m, n)$. Then $\langle g^m \rangle = \langle g^d \rangle$ where $d = \gcd(m, n)$ and $\mathrm{Card}(\langle g^d \rangle) = n/d$.*
(c) *Let $m, k \in \{0, 1, \ldots, n-1\}$. Then $\langle g^m \rangle \subseteq \langle g^k \rangle$ if and only if $\gcd(k, n)$ divides $\gcd(m, n)$.*
(d) *Let $d \in \{0, 1, \ldots, n\}$ and suppose that d divides n. Then the quotient group*

$$\mathcal{Z}_n/\langle g^d \rangle \simeq \mathcal{Z}_{n/d}.$$

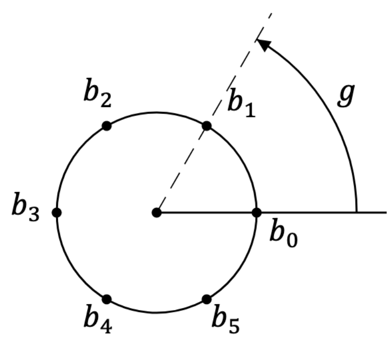
Proposition S.7.3. — *Let $\mathbb{C}^\times = \mathbb{C} - \{0\}$ with the operation of multiplication. If $\varphi \colon \mathbb{Z} \to \mathbb{C}^\times$ is a group homomorphism then there exists $k \in \{0, 1, \ldots, n-1\}$ such that $\varphi = \phi_k$ where*

$$\begin{array}{rccc} \varphi_k \colon & \mathbb{Z}_n & \to & \mathbb{C}^\times \\ & g & \mapsto & \xi^k \end{array}, \qquad \text{where} \qquad \xi = e^{\frac{2\pi i}{n}}.$$

Proposition S.7.4. — *Let S be a circular necklace with n equally spaced beads $b_0, b_1, \ldots, b_{n-1}$, numbered counterclockwise around S.*
(a) *There is an action of the cyclic group $\mathcal{Z}_n$ on the necklace S such that*

g acts by rotating S counterclockwise by an angle of $2\pi/n$.

(b) *This action has one orbit, $\mathcal{Z}_n b_0 = \{b_0, b_1, \ldots, b_{n-1}\}$ and the stabilizer of each bead is the subgroup (1).*



Proposition S.7.5. — *If $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ is a group homomorphism then there exists $m \in \mathbb{Z}$ such that $\varphi = \varphi_m$ where*

$$\varphi_m\colon \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ n & \mapsto & mn \end{array}.$$

S.8. Proofs for the dihedral groups D_n

Proposition S.8.1. —

(a) *The conjugacy classes of D_2 are*

$$\mathcal{C}_1 = \{1\}, \qquad \mathcal{C}_x = \{x\}, \mathcal{C}_y = \{y\}, \qquad \mathcal{C}_{xy} = \{xy\}.$$

(b) *If n is even and $n \neq 2$, then the conjugacy classes of D_n are the sets*

$$\mathcal{C}_1 = \{1\}, \qquad \mathcal{C}_{x^{n/2}} = \{x^{n/2}\}, \qquad \mathcal{C}_{x^k} = \{x^k, x^{-k}\}, \qquad \textit{for } k \in \{0, 1, \ldots, n/2\},$$
$$\mathcal{C}_y = \{y, x^2y, x^4y, \ldots, x^{n-2}y\}, \qquad \mathcal{C}_{xy} = \{xy, x^3y, x^5y, \ldots, x^{n-1}y\}$$

(c) *If n is odd then the conjugacy classes of D_n are the sets*

$$\mathcal{C}_1 = \{1\} \qquad \mathcal{C}_y = \{y, xy, x^2y, x^3y, \ldots, x^{n-1}y\} \quad \textit{and} \quad \mathcal{C}_{x^k} = \{x^k, x^{-k}\} \quad \textit{for } k \in \{0, 1, \ldots, n/2\}.$$

Proof. — (Sketch of Proof.)
(a) The group D_2 is abelian, so each element is in a conjugacy class by itself.
(b) and (c): By the multiplication rule,

$$\begin{array}{c} x(x^k)x^{-1} = x^k, \\ y(x^k)y = x^{-k}y^2 = x^{-k}, \end{array} \qquad \text{and} \qquad \begin{array}{c} x(x^ky)x^{-1} = x^{k+2}y, \\ y(x^ky) = yx^k = x^{-k}y. \end{array}$$

Thus, (1) if x^k is in a conjugacy class then x^{-k} is also in the conjugacy class, and
(2) if x^ky is in a conjugacy class then $x^{k+2}y$ and $x^{-k}y$ are also in the conjugacy class.
One checks case by case that the sets given in the statement of the proposition satisfy these two properties.
Since these sets partition the group D_n, they must be the conjugacy classes. □

Proposition S.8.2. —

(a) *D_n is generated by the elements x and y.*

(b) *The elements x and y in D_n satisfy the relations*

$$x^n = 1, \qquad y^2 = 1, \qquad yx = x^{-1}y.$$

Proof. — Both parts follow directly from the definition of the dihedral group D_n. THIS IS A VERY BAD PROOF. □

Theorem S.8.3. — *The dihedral group D_n has a presentation by generators x and y and relations*

$$x^n = 1, \qquad y^2 = 1, \qquad yx = x^{-1}y.$$

Proposition S.8.4. — *Let $\langle a, b, \cdots \rangle$ denote the subgroup generated by elements $a, b, \ldots$.*

(a) *The normal subgroups of the dihedral group D_2 are the subgroups*

$$\langle x \rangle, \qquad \langle y \rangle, \qquad \langle xy \rangle,$$

(b) *If n is even and $n \neq 2$ then the normal subgroups of the dihedral group D_n are the subgroups*

$$\langle x^k \rangle \quad \textit{for } k \in \{0, 1, \ldots, n-1\} \qquad \textit{and} \qquad \langle x^2, y \rangle, \qquad \langle x^2, xy \rangle.$$

(c) *If n is odd then the normal subgroups of the dihedral group D_n are the subgroups*

$$\langle x^k \rangle \quad \text{for } k \in \{1, \ldots, n-1\}.$$

Proof. — The subgroups given in the statement of the proposition are unions of conjugacy classes of D_n as follows.

$$\begin{aligned} \langle x^k \rangle &= \bigcup \mathcal{C}_{x^{jk}} \\ \langle x^2, y \rangle &= \mathcal{C}_y \cup \langle x^2 \rangle \\ \langle x^2, xy \rangle &= \mathcal{C}_{xy} \cup \langle x^2 \rangle \end{aligned}$$

Thus these subgroups are normal.
It remains to show that these are all the normal subgroups. □

Proposition S.8.5. — *The orders of the elements in the dihedral group D_n are*

$$o(1) = 1, \qquad o(x^k) = \gcd(k, n), \qquad o(x^k y) = 2, \qquad 0 < k \leqslant n-1.$$

Proof. — This follows from the definition of the multiplication in D_n. THIS IS A BAD PROOF □

Proposition S.8.6. — *Let F be an n-gon with vertices v_i numbered 0 to $n-1$ counterclockwise around F. There is an action of the group D_n on the n-gon F such that*

x acts by rotating the n-gon by an angle of $2\pi/n$.
y acts by reflecting about the line which contains the vertex v_0 and the center of F.

Proof. — □

S.9. Proofs for the symmetric group

Proposition S.9.1. — *For each permutation $\sigma \in S_m$, let $\det(\sigma)$ denote the determinant of the matrix which represents the permutation σ. The map*

$$\begin{array}{rccc} \varepsilon\colon & S_m & \to & \pm 1 \\ & \sigma & \mapsto & \det(\sigma) \end{array}$$

is a homomorphism from the symmetric group S_m to the group $\mathbb{Z}_2 = \{\pm 1\}$.

Proof. —
To show: (a) If σ and τ are permutation matrices then $\det(\sigma\tau) = \det(\sigma)\det(\tau)$.
(b) If σ is a permutation matrix then $\det(\sigma) = \pm 1$.

(a) This follows from Proposition (??????).
(b) Any permutation matrix is an orthogonal matrix, i.e. $\sigma\sigma^t = 1$.

Thus, $1 = \det(\sigma\sigma^t) = \det(\sigma)\det(\sigma^t) = \det(\sigma)^2$.
Thus $\det(\sigma) = \pm 1$. □

Lemma S.9.2. — *Suppose $\sigma \in S_m$ has cycle type $\lambda = (\lambda_1, \lambda_2, \ldots)$ and let γ_λ be the permutation in S_m which is given, in cycle notation, by*

$$\gamma_\lambda = (1, 2, \cdots, \lambda_1)(\lambda_1 + 1, \lambda_1 + 2, \ldots, \lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + 1, \cdots) \cdots.$$

(a) *Then σ is conjugate to γ_λ.*
(b) *If $\tau \in S_m$ is conjugate to σ then τ has cycle type λ.*

(c) *Suppose that* $\lambda = (1^{m_1}2^{m_2}\cdots)$. *Then the order of the stabilizer of the permutation* γ_λ, *under the action of* S_m *on itself by conjugation, is*

$$1^{m_1}m_1!2^{m_2}m_2!\cdots.$$

Proof. —

(a) To show: σ is conjugate to $\gamma_\lambda = (1,2,\cdots,\lambda_1)(\lambda_1+1,\lambda_1+2,\ldots,\lambda_1+\lambda_2)(\lambda_1+\lambda_2+1,\cdots)\cdots$.

Suppose that, in cycle notation, $\sigma = (i_1,i_2,\ldots,i_{\lambda_1})(i_{\lambda_1+1},\ldots,i_{\lambda_1+\lambda_2})\cdots$.
Let π be the permutation given by $\pi(i_j) = j$.

Then $\pi\sigma\pi^{-1} = \gamma_\lambda$.

(b) Suppose that $\tau \in S_m$ is conjugate to σ.

Then $\tau = \pi\sigma\pi^{-1}$ for some $\pi \in S_m$.
To show: The lengths of the cycles in $\pi\sigma\pi^{-1}$ are the same as the lengths of the cycles in σ.
Suppose that, in cycle notation, $\sigma = (i_1,i_2,\ldots,i_{\lambda_1})(i_{\lambda_1+1},\ldots,i_{\lambda_1+\lambda_2})\cdots$.
Then $\pi\sigma\pi^{-1}(\pi(i_j)) = \pi(\sigma(i_j)) = \pi(i_{j+1})$.
Thus, in cycle notation, $\pi\sigma\pi^{-1} = (\pi(i_1),\pi(i_2),\cdots,\pi(i_{\lambda_1}))(\pi(i_{\lambda_1+1}),\ldots,\pi(i_{\lambda_1+\lambda_2}))\cdots$.
So, the lengths of the cycles in $\pi\sigma\pi^{-1}$ are the same as the lengths of the cycles in σ.

So, τ has cycle type λ.

(c) Suppose that $\pi \in S_m$ is in the stabilizer of γ_λ.
Then $\pi\gamma_\lambda\pi^{-1} = \gamma_\lambda$.
In cycle notation, $\pi\gamma_\lambda\pi^{-1} = (\pi(1),\pi(2),\ldots,\pi(\lambda_1))(\pi(\lambda_1+1),\ldots,\pi(\lambda_1+\lambda_2))\cdots$.
Since $\pi\gamma_\lambda\pi^{-1} = \gamma_\lambda$, it follows that each of the sequences $(\pi(\lambda_j+1),\ldots,\pi(\lambda_j+\lambda_{j+1}))$ must be a

cyclic rearrangement of some cycle of γ_λ.

This means that π must be a permutation that

(1) permutes cycles of γ_λ of the same length and/or
(2) cyclically rearranges the elements of the cycles of γ_λ.

Note that,

(1) Each cycle of length k in γ_λ can be cyclically rearranged in k ways. Thus, there are a total of k^{m_k} ways of cyclically rearranging the elements of the m_k cycles of length k in γ_λ.
(2) The m_k cycles of length k in γ_λ can be permuted in $m_k!$ different ways.

Thus, there are a total of $1^{m_1}m_1!2^{m_2}m_2!\cdots$ permutations π which stabilize γ_λ under the action of conjugation. □

Proposition S.9.3. —

(a) *The conjugacy classes of* S_m *are the sets*

$$\mathcal{C}_\lambda = \{\text{ permutations } \sigma \text{ with cycle type } \lambda\},$$

where λ *is a partition of* m.

(b) *If* $\lambda = (1^{m_1}2^{m_2}\cdots)$ *then the size of the conjugacy class* $\mathcal{C}_\lambda$ *is*

$$|\mathcal{C}_\lambda| = \frac{m!}{m_1!1^{m_1}m_2!2^{m_2}m_3!3^{m_3}\cdots}.$$

Proof. —

(a) To show: (aa) If $\lambda \vdash m$ then $\mathcal{C}_\lambda$ is a conjugacy class of S_m.
(ab) Every conjugacy class is equal to $\mathcal{C}_\lambda$ for some $\lambda \vdash m$.
(aa) Let λ be a partition of m.
Let $\mathcal{O}_{\gamma_\lambda}$ denote the conjugacy class of γ_λ.
To show: $\mathcal{O}_\lambda = \mathcal{C}_\lambda$.
To show: (aaa) $\mathcal{C}_\lambda \subseteq \mathcal{O}_{\gamma_\lambda}$.
(aab) $\mathcal{C}_{\gamma_\lambda} \subseteq \mathcal{C}_\lambda$.
(aaa) Suppose that $\sigma \in \mathcal{C}_\lambda$.
Then σ has cycle type λ.
Thus, by Lemma (?????), σ is conjugate to γ_λ.
So, $\sigma \in \mathcal{O}_{\gamma_\lambda}$.
Thus, $\mathcal{C}_\lambda \subseteq \mathcal{O}_{\gamma_\lambda}$.
(aab) Suppose that $\sigma \in \mathcal{O}_{\gamma_\lambda}$.
Then, σ is conjugate to γ_λ.
Thus, by Lemma (????), σ has cycle type λ.
So, $\sigma \in \mathcal{C}_\lambda$.
So $\mathcal{O}_{\gamma_\lambda} \subseteq \mathcal{C}_\lambda$.
So $\mathcal{C}_\lambda = \mathcal{O}_{\gamma_\lambda}$.
So $\mathcal{C}_\lambda$ is a conjugacy class of S_m.
(ab) Let $\sigma \in S_m$ and let $\mathcal{O}_\sigma$ be the conjugacy class of σ.
Suppose that σ has cycle type λ.
Then, by Lemma (?????), σ is conjugate to γ_λ.
Thus, by Proposition (?????), $\mathcal{O}_\sigma = \mathcal{O}_{\gamma_\lambda}$.
So, by part (a), $\mathcal{O}_\sigma = \mathcal{O}_{\gamma_\lambda} = \mathcal{C}_\lambda$.
So every conjugacy class is equal to $\mathcal{C}_\lambda$ for some $\lambda \vdash m$. So the sets $\mathcal{C}_\lambda$, $\lambda \vdash m$, are the conjugacy classes of S_m.
(b) Let $\lambda = (1^{m_1}2^{m_2}\cdots)$ be a partition of m.
By, Lemma (???), the stabilizer of the permutation γ_λ, has order $1^{m_1}m_1!2^{m_2}m_2!\cdots$.
Thus, by Proposition (???), the order of the conjugacy class $\mathbb{C}_\lambda$ is

$$\mathrm{Card}(\mathcal{C}_\lambda) = \frac{\mathrm{Card}(S_m)}{1^{m_1}m_1!2^{m_2}m_2!\cdots} = \frac{m!}{1^{m_1}m_1!2^{m_2}m_2!\cdots}.$$

□

Proposition S.9.4. —
(a) *S_m is generated by the simple transpositions s_i, $1 \leqslant i \leqslant m-1$.*
(b) *The simple transpositions $\{s_i \mid i \in \{1,\ldots,m-1\}\}$ in S_m satisfy the relations*

$$s_i s_j = s_j s_i, \qquad \text{if } j \notin \{i_1, i+1\},$$
$$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, \qquad \text{if } i \in \{1,\ldots,m-2\},$$
$$s_i^2 = 1, \qquad \text{for } i \in \{1,\ldots,m-1\}.$$

Proof. — (a) To show: Every permutation σ can be written as a product of simple tranpositions.
This is most easily seen by "stretching out" the function diagram of σ.

PICTUREstretchout.ps

We must give some argument to show that this can always be done, for an arbitrary permutation σ.

PICTUREsigma.ps

The set of *inversions* of σ is the set

$$\mathrm{inv}(\sigma) = \{(i,j) \mid i,j \in \{1,\dots,m\} \text{ and } i<j \text{ and } \sigma(i) > \sigma(j)\}.$$

Let k_i be the number of inversions of σ that have first coordinate i.
Then define

$$\gamma(i) = \begin{cases} s_i s_{i+1} \dots s_{i+k_i-1}, & \text{if } k_i \geqslant 1, \\ 1, & \text{if } k_i = 0. \end{cases}$$

Then $\sigma = \gamma(m-1)\gamma(m-2)\cdots\gamma(1)$.

$$PICTURE gammadec.ps$$

Thus σ can be written as a product of simple transpositions.

(b) To show: (ba) If $i,j \in \{1,\dots,m-1\}$ and $j \notin \{i-1,i+1\}$ then $s_i s_j = s_j s_i$,
(bb) If $i \in \{1,\dots,m-2\}$ then $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$.
(bc) If $i \in \{1,\dots,m-1\}$ then $s_i^2 = 1$, $\quad 1 \leqslant i \leqslant m-1$.

(ba)

$$PICTURE sisjsjsi$$

(bb)

$$PICTURE sisip1$$

(bc)

$$PICTURE si2$$

□

S.10. Proofs for the alternating group

Proposition S.10.1. — *Suppose that $\sigma \in A_m$. Let $\mathcal{C}_\sigma$ denote the conjugacy class of σ in S_m and let $\mathcal{A}_\sigma$ denote the conjugacy class of σ in A_m.*

(a) *Then σ has an even number of cycles of even length.*

(b)

$$\mathrm{Card}(\mathcal{A}_\sigma) = \begin{cases} \dfrac{\mathrm{Card}(\mathcal{C}_\sigma)}{2}, & \textit{if all cycles } \sigma \textit{ are of different odd lengths}, \\ \\ \mathrm{Card}(\mathcal{C}_\sigma), & \textit{otherwise.} \end{cases}$$

Proof. —

(a) Suppose that σ has cycle type $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$.
To show: An even number of the λ_j, $1 \leqslant j \leqslant k$, are even.
Let γ_λ be the permutation given, in cycle notation, by

$$\gamma_\lambda = (1,2,\cdots,\lambda_1)(\lambda_1+1, \lambda_1+2, \dots, \lambda_1+\lambda_2)(\lambda_1+\lambda_2+1, \cdots)\cdots.$$

Since A_m is a normal subgroup of S_m and $\sigma \in A_m$ it follows that $C_\sigma = \mathcal{C}_{\gamma_\lambda} \subseteq A_m$.
So $\gamma_\lambda \in A_m$.
So the length $\ell(\gamma_\lambda)$ of γ_λ is even.
So $\ell(\gamma_\lambda) = \sum_{i=1}^k (\lambda_i - 1)$ is even.
So there are an even number of $1 \leqslant j \leqslant k$ such that $\lambda_j - 1$ is odd.
So there are an even number of $1 \leqslant j \leqslant k$ such that λ_j is even.
So σ has an even number of cycles of even length.

(b) Let S_σ be the stabilizer of σ under the action of S_m on itself by conjugation.
Let A_σ be the stabilizer of σ under the action of A_m on itself by conjugation.

Then, by Proposition (???),

$$\tfrac{1}{2}\mathrm{Card}(S_\sigma)\mathrm{Card}(\mathcal{C}_\sigma) = \frac{\mathrm{Card}(S_m)}{2} = \mathrm{Card}(A_m) = \mathrm{Card}(A_\sigma)\mathrm{Card}(\mathcal{A}_\sigma).$$

So,

$$\mathrm{Card}(\mathcal{A}_\sigma) = \begin{cases} \mathrm{Card}(\mathcal{C}_\sigma), & \text{if } \mathrm{Card}(A_\sigma) \neq \mathrm{Card}(S_\sigma), \\ \dfrac{\mathrm{Card}(\mathcal{C}_\sigma)}{2}, & \text{if } \mathrm{Card}(A_\sigma) = \mathrm{Card}(S_\sigma). \end{cases}$$

Since $A_\sigma \subseteq S_\sigma$,

$$\mathrm{Card}(\mathcal{A}_\sigma) = \begin{cases} \mathrm{Card}(\mathcal{C}_\sigma), & \text{if } S_\sigma \subseteq A_\sigma, \\ \mathrm{Card}(\dfrac{\mathcal{C}_\sigma)}{2}, & \text{if } S_\sigma \not\subseteq A_\sigma. \end{cases}$$

So,

$$\mathrm{Card}(\mathcal{A}_\sigma) = \begin{cases} \mathrm{Card}(\mathcal{C}_\sigma), & \text{if } S_\sigma \subseteq A_m, \\ \dfrac{\mathrm{Card}(\mathcal{C}_\sigma)}{2}, & \text{if } S_\sigma \not\subseteq A_m. \end{cases}$$

Then, by Lemma (???),

$$\mathrm{Card}(\mathcal{A}_\sigma) = \begin{cases} \mathrm{Card}(\mathcal{C}_\sigma), & \text{if } S_{\gamma_\lambda} \subseteq A_m, \\ \dfrac{Card(\mathcal{C}_\sigma)}{2},, & \text{if } S_{\gamma_\lambda} \not\subseteq A_m. \end{cases}$$

By Lemma (???),

$$\mathrm{Card}(\mathcal{A}_\sigma) = \begin{cases} \dfrac{\mathrm{Card}(\mathcal{C}_\sigma)}{2}, & \text{if all cycles } \sigma \text{ are of different odd lengths,} \\ \\ \mathrm{Card}(\mathcal{C}_\sigma), & \text{otherwise.} \end{cases}$$

□

Lemma S.10.2. — *Let $\sigma \in A_m$ and let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ be the cycle type of σ. Let γ_λ be the permutation given, in cycle notation, by*

$$\gamma_\lambda = (1, 2, \cdots, \lambda_1)(\lambda_1 + 1, \lambda_1 + 2, \dots, \lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + 1, \cdots) \cdots .$$

Let S_σ denote the stabilizer of σ under the action of S_m on itself by conjugation. Then,
(a) *$S_\sigma \subseteq A_m$ if and only if $S_{\gamma_\lambda} \subseteq A_m$.*
(b) *$S_{\gamma_\lambda} \subseteq A_m$ if and only if γ_λ has all odd cycles of different lengths.*

Proof. —
(a) To show: $S_\sigma \subseteq A_m$ if and only if $S_{\gamma_\lambda} \subseteq A_m$.
To show: (aa) If $S_\sigma \subseteq A_m$ then $S_{\gamma_\lambda} \subseteq A_m$.
(ab) If $S_{\gamma_\lambda} \subseteq A_m$ then $S_\sigma \subseteq A_m$.
Then, by Proposition (????), there exists $\pi \in S_m$ such that $\pi\sigma\pi^{-1} = \gamma_\lambda$.
Thus, $S_{\gamma_\lambda} = \pi S_\sigma \pi^{-1}$.
(aa) Assume $S_\sigma \subseteq A_m$.
Let $\tau \in S_{\gamma_\lambda}$.
Then $\pi^{-1}\tau\pi \in S_\sigma$.
So $\pi^{-1}\tau\pi \in A_m$.
So $1 = \varepsilon(\pi^{-1}\tau\pi)$.
Since ε is a homomorphism, $\varepsilon(\tau) = \varepsilon(\pi)^{-1}\varepsilon(\tau)\varepsilon(\pi) = \varepsilon(\pi^{-1}\tau\pi) = 1$.

So $\tau \in A_m$.
So $S_{\gamma_\lambda} \subseteq A_m$.

(ab) Assume $S_{\gamma_\lambda} \subseteq A_m$.
Let $\tau \in S_\sigma$.
Then $\pi\tau\pi^{-1} \in S_{\gamma_\lambda}$.
So $\pi\tau\pi^{-1} \in A_m$.
So $1 = \varepsilon(\pi\tau\pi^{-1})$.
Since ε is a homomorphism, $\varepsilon(\tau) = \varepsilon(\pi)\varepsilon(\tau)\varepsilon(\pi)^{-1} = \varepsilon(\pi\tau\pi^{-1}) = 1$.
So $\tau \in A_m$.

So $S_\sigma \subseteq A_m$.
So $S_\sigma \subseteq A_m$ if and only if $S_{\gamma_\lambda} \subseteq A_m$.

(b) To show: $S_{\gamma_\lambda} \subseteq A_m$ if and only if γ_λ has all odd cycles of different lengths.
To show: (ba) If $S_{\gamma_\lambda} \subseteq A_m$ then γ_λ has all odd cycles of different lengths. item[]
(bb) If γ_λ has all odd cycles of different lengths then $S_{\gamma_\lambda} \subseteq A_m$.

(ba) Proof by contradiction.
Assume λ does not have all odd parts of different lengths.
To show: $S_{\gamma_\lambda} \not\subseteq A_m$.
Case 1: Assume γ_λ has an even cycle, say $(k+1, \ldots, k+2n)$.
Let π be the permutation which cyclically permutes this cycle, $\pi = (k+1, \ldots, k+2n)$.
Then $\pi \in S_{\gamma_\lambda}$.
But $\varepsilon(\pi) = (-1)^{2n-1} = -1$.
So $\pi \notin A_m$.
So $S_{\gamma_\lambda} \not\subseteq A_m$.
Case 2: Assume γ_λ has two cycles of the same odd length, say $(k+1, \ldots, k+n)$ and $(k+n+1, \ldots, k+n+n)$.
Let π be the permutation which switches these two cycles, $\pi = (k+1, k+1+n)(k+2, k+2+n)\cdots(k+n, k+n+n)$.
Then $\pi \in S_{\gamma_\lambda}$.
But $\varepsilon(\pi) = (-1)^{n^2} = -1$, since n is odd.
So $\pi \notin A_m$.
So $S_{\gamma_\lambda} \not\subseteq A_m$.

(bb) Assume γ_λ has all different odd cycles.
Suppose that $\tau \in S_{\gamma_\lambda}$.
This means that τ must be a permutation that
(1) permutes cycles of γ_λ of the same length and/or
(2) cyclically rearranges the elements of the cycles of γ_λ.
Since all cycles of γ_λ are different lengths, τ cyclically permutes the elements of the cycles of γ_λ.
Define permutations

$$c_1 = (1, 2, \ldots, \lambda_1), \quad c_2 = (\lambda_1 + 1, \lambda_1 + 2, \ldots, \lambda_1 + \lambda_2), \quad \text{etc.}$$

Then $\tau = c_1^{n_1} c_2^{n_2} \cdots c_k^{n_k}$ for some positive integers $n_1, n_2, \ldots, n_k$.
Then $\varepsilon(c_j) = (-1)^{\lambda_j - 1} = 1$, since λ_j is odd.
So $\varepsilon(tau) = \varepsilon(c_1)^{n_1}\varepsilon(c_2)^{n_2}\cdots\varepsilon(c_k)^{n_k} = 1$.
So $\tau \in A_m$.

So $S_{\gamma_\lambda} \subseteq A_m$.

$\square$

Theorem S.10.3. —
(a) *If $m \neq 4$ then A_m is simple.*
(b) *The alternating group A_4 has a single nontrivial proper normal subgroup given by*

$$\{(1234), (2143), (3412), (4321)\}$$

Proof. —

(a) *Case a:* $n = 1, 2, 3$.
The groups $A_1 = \{1\}$, $A_2 = \{1\}$ $A_3 = \{(123), (213), (312)\}$ have no nontrivial proper subgroups.
So A_1, A_2 and A_3 have no nontrivial proper normal subgroups.

(b) *Case b:* $n = 4$.
The conjugacy classes of A_4 are

$$\{1\}, \quad \{(123), (134), (243), (142)\}, \quad \{(132)(124), (234), (143)\}, \quad \{(12)(34), (13)(24), (14)(23)\}.$$

Let N be a normal subgroup of A_4.

(ba) *Case ba:* $\pi = (123) \in N$.
Then $\pi^{-1} = (132)$ and $(123)(124) = (12)(34)$ are in N.
So N contains all the conjugacy classes.
So $N = A_n$.

(bb) *Case bb:* $\pi = (132) \in N$.
Then $\pi^{-1} = (123)$ and $(123)(124) = (12)(34)$ are in N.
So N contains all the conjugacy classes.
So $N = A_n$.
Thus, the only possible union of conjugacy classes which could be a normal subgroup is

$$N = \{1, (12)(34), (13)(24), (14)(23)\}.$$

It is easy to check that this is a subgroup of A_4.

(c) *Case c:* $n \geqslant 5$.
Let N be a normal subgroup of A_n such that $N \neq (1)$.
To show: $N = A_n$.
Let $\sigma \in N$ and suppose that $sigma$ has cycle type λ.
Let γ_λ

$$SOMEHTING$$

(ca) *Case ca:* σ has a cycle $(i_1 i_2 \cdots i_r)$ of length $r > 3$.
Then $\sigma^{-1} \in N$ and $(i_2 i_3 i_4)\sigma(i_4 i_3 i_2) \in N$.
So $\sigma^{-1}((i_2 i_3 i_4)\sigma(i_4 i_3 i_2)) = (\sigma^{-1}(i_1 i_2 i_3)\sigma)(i_4 i_3 i_2) = (i_1 i_2 i_3)(i_4 i_3 i_2) = (i_1 i_2 i_4) \in N$.
Thus, by Lemma (???), $N = A_n$.

(cb) *Case cb:* σ does not have all odd cycles of different lengths and σ has a cycle of length > 2.
Then, by Propositions (???) and (???), $\mathcal{A}_\sigma = \mathcal{C}_\sigma = \mathcal{C}_{\gamma_\lambda}$.
Since N is normal, $\mathcal{C}_{\gamma_\lambda} = \mathcal{A}_\sigma \subseteq N$.
So $\gamma_\lambda \in N$ and $s_1 \gamma_\lambda s_1 \in N$.
Since N is a subgroup $\gamma_\lambda^{-1} \in N$.
So $\gamma_\lambda^{-1}(s_1 \gamma_\lambda s_1) = (\gamma_\lambda^{-1} s_1 \gamma_\lambda) s_1 = s_2 s_1 = (123) \in N$.
Thus, by Lemma (), $N = A_n$.

(cc) *Case cc:* σ has all cycles of length 2 or 1.
Since $\sigma \in A_n$, σ has at least two cycles of length 2.

Thus, by Proposition (), $\mathcal{A}_\sigma = \mathcal{C}_\sigma = \mathcal{C}_{\gamma_\lambda}$.
Since N is normal, $\mathcal{C}_{\gamma_\lambda} = \mathcal{A}_\sigma \subseteq N$.
So $\gamma_\lambda \in N$ and $s_2\gamma_\lambda s_2 \in N$.
Since N is a subgroup $\gamma_\lambda^{-1} \in N$.
So $\gamma_\lambda^{-1} s_2 \gamma_\lambda s_2 = (14)(23) \in N$.
So $\pi_1 = (12)(34)(5)$ and $\pi_2 = (12)(3)(45) \in N$.
So $\pi_1\pi_2 = (345) \in N$.

Thus, by Lemma (), $N = A_n$.

□

Lemma S.10.4. — *Suppose N is a normal subgroup of A_n, $n > 4$, and N contains a 3-cycle. Then $N = A_n$.*

Proof. — To show: $A_n \subseteq N$.
Let $\pi = (i_1, i_2, i_3)$ be a 3-cycle in N.
Since $n > 4$, π has more than one 1-cycle and it follows from Proposition (), that $\mathcal{A}_\pi = \mathcal{C}_\pi$.
Thus, since N is normal, $\mathcal{C}_\pi \subseteq N$.
So (123) and (143) are elements of N.
Then $\sigma = (143)(123) = (12)(34) = s_1 s_3 \in N$.
Since σ has an even cycle, it follows from Proposition (), that $\mathcal{A}_\sigma = \mathcal{C}_\sigma \subseteq N$.
Then

$$s_i s_j \in \begin{cases} \mathcal{C}_\pi, & \text{if } j = i+1, \\ \mathcal{C}_\sigma, & \text{otherwise.} \end{cases}$$

So $s_i s_j \in N$ for all i, j.
By, Proposition () and Proposition (), the elements $s_i s_j$ generate A_n.
So $A_n \subseteq N$. □