Automorphism Groups

Contents

1 Automorphism groups of small groups

1. $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$. In particular, for $\mathbb{Z}_p$ where p is prime, $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{F}_p$.

2. If G and H have no common direct factor, then

   $\mathrm{Aut}(G \times H) \cong \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) : \alpha \in \mathrm{Aut}(G), \beta \in \mathrm{Hom}(H, Z(G)), \gamma \in \mathrm{Hom}(G, Z(H)), \delta \in \mathrm{Aut}(H) \right\}$.

   If G_i are all abelian, then $\mathrm{Aut}(\bigoplus_{i=1}^n G_i)$ is the group of all invertible $n \times n$ matrices with (i, j) entries in $\mathrm{Hom}(G_i, G_j)$.

   In particular, for $\mathbb{Z}_p$ where p is prime, $\mathrm{Aut}(\bigoplus_{i=1}^n \mathbb{Z}_p) \cong \mathrm{GL}_n(\mathbb{F}_p)$. $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

3. $\mathrm{Aut}(A_n) \cong S_n$ for $n \geqslant 4$, $n \neq 6$. $\mathrm{Aut}(S_n) \cong S_n$ for $n \neq 2, 6$.

   $\mathrm{Aut}(A_1) = \mathrm{Aut}(A_2) = \mathrm{Aut}(S_2) = 1$. $\mathrm{Aut}(A_3) \cong \mathbb{Z}_2$. $\mathrm{Aut}(A_6) = \mathrm{Aut}(S_6) \cong S_6 \rtimes \mathbb{Z}_2$.

4. $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

   Let $\mathbb{Z}_8 = \langle a \rangle$. $\mathrm{Aut}(\mathbb{Z}_8)$ is generated by $a \mapsto 3a$ and $a \mapsto 5a$.

5. $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4) \cong D_4$.

   Let $\mathbb{Z}_2 \times \mathbb{Z}_4 = \langle a \rangle \oplus \langle b \rangle$, $o(a) = 2$, $o(b) = 4$. We have

element	1	a	b	$2b$	$3b$	$a+b$	$a+2b$	$a+3b$
order	1	2	4	2	4	4	2	4

   Automorphisms are given by

image of a	a	a	a	a	$a+2b$	$a+2b$	$a+2b$	$a+2b$
image of b	b	$a+b$	$a+3b$	$3b$	b	$a+b$	$a+3b$	$3b$
order	1	2	2	2	2	4	4	2
element	id	ψ	$\rho^2\psi$	ρ^2	$\psi\rho = \rho^3\psi$	ρ	ρ^3	$\rho\psi$

   Therefore, $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4) \cong D_4$.

6. $\mathrm{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_6$.

   Let $\mathbb{Z}_9 = \langle a \rangle$. $\mathrm{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_6$ is generated by $a \mapsto 2a$.

2 Automorphism groups of dihedral Groups D_n

♚ For finite dihedral group $D_n \coloneqq \langle a, b \mid a^n = b^2 = 1, (ab)^2 = 1 \rangle$, $\mathrm{Aut}(D_n) \cong \mathbb{Z}_n \rtimes \mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$.

In $\mathbb{Z}_n \rtimes \mathrm{Aut}(\mathbb{Z}_n)$, $(m_1, f_1) \cdot (m_2, f_2) = (m_1 \cdot f_1(m_2), f_1 \circ f_2)$ where $m_1, m_2 \in \mathbb{Z}_n$ and $f_1, f_2 \in \mathrm{Aut}(\mathbb{Z}_n)$.

♛ **Proof:**

If $\mathbb{Z}_n$ is generated by c, then each element in $\mathrm{Aut}(\mathbb{Z}_n)$ maps c to c^k for some $k \in \{0, \ldots, n-1\}$ with $(k, n) = 1$.

Denote this element by $\gamma_k \in \mathrm{Aut}(\mathbb{Z}_n)$. $D_n \coloneqq \langle a, b \mid a^n = b^2 = 1, (ab)^2 = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2 b, \ldots, a^{n-1} b\}$.

For each $\psi \in \mathrm{Aut}(D_n)$, ψ is uniquely determined by $\psi(a)$ and $\psi(b)$.

We have $\psi(a) = a^r$, $\psi(b) = a^s b$ for some $r \in \{0, \ldots, n-1\}$ with $(r, n) = 1$ and $s \in \{0, \ldots, n-1\}$.

Denote this automorphism by $\psi_{r,s} \in \mathrm{Aut}(D_n)$. $\varphi : \mathrm{Aut}(D_n) \to \mathbb{Z}_n \rtimes \mathrm{Aut}(\mathbb{Z}_n), \psi_{r,s} \mapsto (c^s, \gamma_r)$ is isomorphism. $\square$

For $n = 3, 4, 6$, $\mathrm{Aut}(\mathbb{Z}_n) = \mathbb{Z}_2$. $\mathrm{Aut}(D_3) \cong D_3$, $\mathrm{Aut}(D_4) \cong D_4$, $\mathrm{Aut}(D_6) \cong D_6$, $\mathrm{Aut}(D_2) = \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3 \cong D_3$.

♚ For infinite dihedral group $D_\infty \coloneqq \langle a, b \mid a^2 = b^2 = 1 \rangle = \mathbb{Z}_2 * \mathbb{Z}_2$, $\mathrm{Aut}(D_\infty) \cong D_\infty$.

♛ **Proof:**

$\langle ab \rangle$ is cyclic group of infinite order and is subgroup of index 2 in D_∞. $D_\infty = \langle ab \rangle \sqcup b\langle ab \rangle$.

Elements in $\langle ab \rangle$ have infinite order, and elements in $b\langle ab \rangle$ have order 2. $\psi \in \mathrm{Aut}(D_\infty)$ preserves order of elements.

Suppose $\psi(ab) = (ab)^p$ and $ab = \psi((ab)^q)$ for $p, q \in \mathbb{Z}$, then $(ab) = (ab)^{pq}$, $p = q = 1$ or $p = q = -1$.

1. $\psi(ab) = ab$. ψ has form $\psi_{1,m}(a) = (ba)^m \cdot a$ and $\psi_{1,m}(b) = (ba)^m \cdot b$ for some $m \in \mathbb{Z}$.

$\psi_{1,m}(a \cdot (ba)^m) = a$, $\psi_{1,m}(b \cdot (ba)^m) = b$, so $\psi_{1,m}$ is indeed an automorphism of D_∞.

Define $\sigma \in \mathrm{Aut}(D_\infty)$ by $\sigma(x) = axa^{-1} = axa$. $\sigma(a) = a, \sigma(b) = aba, \sigma^2 = \mathrm{id}$.

Define $\omega \in \mathrm{Aut}(D_\infty)$ by $\omega(a) = b, \omega(b) = a$. $\omega^2 = \mathrm{id}$. Then we have $\psi_{1,m} = (\omega \circ \sigma)^m$.

2. $\psi(ab) = ba$. ψ has form $\psi_{2,m}(a) = (ba)^m \cdot b$ and $\psi_{2,m}(b) = (ba)^m \cdot a$ for some $m \in \mathbb{Z}$.

$\psi_{2,n}(b \cdot (ba)^n) = a, \psi_{2,n}(a \cdot (ba)^n) = b$, so $\psi_{2,n}$ is indeed an automorphism of D_∞, and $\psi_{2,n} = \omega \circ (\sigma \circ \omega)^n$.

Combining 1 and 2, we have $\mathrm{Aut}(D_\infty) = \{\psi_{1,m}, \psi_{2,n} \mid m, n \in \mathbb{Z}\}$ is generated by σ and ω with $\sigma^2 = \omega^2 = \mathrm{id}$.

Therefore, $\mathrm{Aut}(D_\infty) = \langle \sigma, \omega \mid \sigma^2 = \omega^2 = \mathrm{id} \rangle \cong D_\infty$. $\square$

3 Automorphism group of quaternion group Q_8

♚ For $Q_8 = \{-1, \mathrm{i}, \mathrm{j}, \mathrm{k} \mid \mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1\}$, $\mathrm{Aut}(Q_8) \cong S_4$.

♛ Geometric interpretation:

1. Decorate six faces of a cube as follows. Choose a vertex v, look at the vertex and mark 3 sides counterclockwise around v as $\mathrm{i}, \mathrm{j}, \mathrm{k}$. Mark $\mathrm{i}, \mathrm{j}, \mathrm{k}$ on the opposite faces respectively.

2. The multiplication in Q_8 is represented by the cube as follows.

(1) If x and y have a unique vertex s.t. x and y are counterclockwise, then product xy is the third face at the vertex, e.g. $\mathrm{ij} = \mathrm{k}$. Otherwise $x = y$ (where $xy = -1$) or $x = -y$ (where $xy = 1$).

(2) If we x and y are clockwise in a vertex, then $xy = -z$ where z is the third face.

3. For $\psi \in \mathrm{Aut}(Q_8)$, ψ fixes ± 1, so ψ is uniquely determined by $\psi(\mathrm{i})$ and $\psi(\mathrm{j})$.

4. Rotation of this cube is determined by where it sends each of four main diagonals to, so the rotation group is S_4.

5. $\mathrm{Aut}(Q_8)$ is isomorphic to the rotation group of this cube.

Algebraic proof:

$\mathrm{Aut}(Q_8)$ fixes $\langle \mathrm{i} \rangle, \langle \mathrm{j} \rangle, \langle \mathrm{k} \rangle$. Action of $\mathrm{Aut}(Q_8)$ on $\langle \mathrm{i} \rangle, \langle \mathrm{j} \rangle, \langle \mathrm{k} \rangle$ induces a homomorphism $\Phi : \mathrm{Aut}(Q_8) \to S_3$.

Define $\psi_1, \psi_2 \in \mathrm{Aut}(Q_8)$ by $\psi_1(\mathrm{i}) = \mathrm{j}, \psi_1(\mathrm{j}) = \mathrm{i}$ and $\psi_2(\mathrm{i}) = \mathrm{k}, \psi_2(\mathrm{k}) = \mathrm{i}$. $\Phi(\psi_1) = (12), \Phi(\psi_2) = (13)$, Φ is surjective.

$\ker \Phi = \{\varphi \in \mathrm{Aut}(Q_8) \mid \varphi(\langle \mathrm{i} \rangle) = (\langle \mathrm{i} \rangle), \varphi(\langle \mathrm{j} \rangle) = (\langle \mathrm{j} \rangle)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. $\langle \psi_1, \psi_2 \rangle \cong \mathbb{Z}_3$, $\ker \Phi \cap \langle \psi_1, \psi_2 \rangle = 1$.

$\mathrm{Aut}(Q_8) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3$. Element in S_3 doesn't commute with any element in $\mathbb{Z}_2 \times \mathbb{Z}_2$, so action of S_3 on $\mathbb{Z}_2 \times \mathbb{Z}_2$ by conjugation is faithful. Therefore $\mathrm{Aut}(Q_8) \cong S_4$. $\square$

4 Automorphism groups of permutation group S_n

♚ $\mathrm{Aut}(S_n) \cong S_n$ $(n \neq 2, 6)$

♛ **Proof:**

1. Prerequisites: (1) $Z(S_n) = 1$ $(n \neq 2)$. (2) S_n is generated by transpositions $\{(1, i) : i > 1\}$.

2. For $1 \leqslant k \leqslant \frac{n}{2}$, the number of products of k disjoint transpositions in S_n is $\dfrac{n!}{2^k \cdot k!(n-2k)!}$.

Product of k disjoint transpositions in S_n has form $(a_1, b_1) \cdots (a_k, b_k)$.

Note that the order of (a_i, b_i) doesn't matter, so the number of choices is

$$\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2} = \frac{n!}{2^k \cdot k!(n-2k)!}$$

3. For $\varphi \in \mathrm{Aut}(S_n)$, if φ maps transpositions to transpositions, then $\varphi \in \mathrm{Inn}(S_n)$.

Suppose $\varphi(1, r) = (a_r, b_r)$ for each r, then $\varphi((1, 2)(1, r)) = (a_2, b_2)(a_r, b_r)$.

If $n \geqslant 3$, $(1, 2)(1, r) = (1, r, 2)$ is of order 3, so $a_r \in \{a_2, b_2\}$ or $b_r \in \{a_2, b_2\}$. WLOG we can assume $a_r \in \{a_2, b_2\}$.

Claim: $a_r = a_2$ for all r or $a_r = b_2$ for all r.

Otherwise there exists $s \neq t$ s.t. $a_s = a_2,\ a_t = b_2$. Note that $(1, s, 2)(1, t, 2) = (1, s)(2, t)$ has order 2, but

$\varphi((1, s, 2)(1, t, 2)) = \varphi((1, 2)(1, s)(1, 2)(1, t)) = (a_2, b_2)(a_2, b_s)(a_2, b_2)(b_2, b_t) = (b_2, b_t, b_s)$ has order 3. Contradiction.

WLOG assume $a_r = a_2$ for all r, then $\varphi(1, r) = (a_2, b_r)$. Since φ is 1-1, $b_r \neq b_s$ for $r \neq s$.

Define $\sigma \in \mathrm{Aut}(S_n)$ by $\sigma(1) = a_2$, $\sigma(r) = b_r$ for $r \geq 3$. $\varphi(1, r) = (a_2, b_r) = \sigma(1, r)\sigma^{-1}$, therefore $\varphi \in \mathrm{Inn}(S_n)$.

4. If $n \neq 2, 6$, then every automorphism of S_n is inner.

For $\varphi \in \mathrm{Aut}(S_n)$ and transposition $\sigma \in S_n$, there're $\binom{n}{2}$ transpositions in S_n.

$\varphi(\sigma)$ has order 2, it's product of k disjoint transpositions for some $k \geqslant 1$.

φ maps conjugacy class to conjugacy class, so it maps transpositions to products of k disjoint transpositions.

From 2, we have $\dfrac{n(n-1)}{2} = \dfrac{n!}{2^k \cdot k! \cdot (n-2k)!}$, i.e. $(n-2)! = 2^{k-1} \cdot k! \cdot (n-2k)!$.

Set $p = n-2, q = k-1$, we have $\binom{p}{2q} = \dfrac{q+1}{(2q-1)!!}$. The only solution of this is $p = 4$, $q = 2$.

Besides, $\dfrac{n(n-1)}{2} = \dfrac{n!}{2^k \cdot k!(n-2k)!}$ only holds when $k = 1$ or $n = 6, k = 3$.

Therefore, for $n \neq 2, 6$, every automorphism of S_n is inner, and $\mathrm{Aut}(S_n) \cong \mathrm{Inn}(S_n) \cong S_n/Z(S_n) = S_n$. □

5 Automorphism groups of alternating groups A_n

♚ $\mathrm{Aut}(A_n) \cong S_n$ ($n \geqslant 4$ and $n \neq 6$)

♛ **Proof:**

1. Prerequisites:

(1) $Z(A_n) = 1$ ($n \neq 3$). (2) A_n is generated by 3-cycles.

(3) Four possibilities for products of 3-cycles:

(i) $(abc)(abd) = (ab)(bc)$. (ii) $(abc)(adb) = (bcd)$. (iii) $(abc)(ade) = (abcde)$. (iv) $(abc)(def)$.

2. For $1 \leqslant k \leqslant \frac{n}{3}$, the number of products of k disjoint 3-cycles in S_n is $\frac{n!}{2^k \cdot k!(n-2k)!}$.

Product of k disjoint 3-cycles in A_n has form $(a_1, b_1, c_1) \cdots (a_k, b_k, c_k)$.

Note that the order of (a_i, b_i, c_i) doesn't matter, so the number of choices is

$$\frac{1}{k!} \times \frac{n(n-1)(n-2)}{3} \times \cdots \times \frac{(n-3k+3)(n-3k+2)(n-3k+1)}{3} = \frac{n!}{3^k k!(n-3k)!}$$

3. If $\varphi \in \mathrm{Aut}(A_n)$ maps 3-cycles to 3-cycles, then φ is an inner automorphism of S_n restricted on A_n.

For $i \geqslant 3$, let $u_i = (1, 2, i)$ and $v_i = \varphi(u_i)$. $u_i u_j = (1i)(2j)$ is of order 2 for $i \neq j$, and $\varphi(u_i u_j) = v_i v_j$ also has order 2.

v_3, v_4 is product of two 3-cycles, from 1(3), there exist a_1, a_2 s.t. v_3, v_4 have form $v_3 = (a_1, a_2, c)$ and $v_4 = (a_1, a_2, d)$.

Consider v_i for $i \geqslant 5$. If v_i fixes a_1, then we must have $v_i = (a_2, c, *)$ and $v_i = (a_2, d, *)$. Contradiction.

Therefore, v_i permutes a_1, and this requires $v_i = (a_1, a_2, a_i)$ for $i \geqslant 3$.

Define $x \in S_n$ by $x(i) = a_i$, then $x u_i x^{-1} = v_i = \varphi(u_i)$. Since $C_{S_n}(A_n) = 1$, this $x \in S_n$ is unique.

Thus for all $\varphi \in \mathrm{Aut}(A_n)$, φ maps 3-cycles to 3-cycles, there exists unique $x \in S_n$ s.t. $\varphi = c_x|_{A_n}$, where $c_x(\sigma) = x\sigma x^{-1}$ for $\sigma \in S_n$.

4. For $\gamma \in A_n$, let $\mathrm{Cl}_{S_n}(\gamma)$ be its conjugacy class in S_n and $\mathrm{Cl}_{A_n}(\gamma)$ be its conjugacy class in A_n.

$|\mathrm{Cl}_{S_n}(\gamma)| = [S_n : C_{S_n}(\gamma)]$, $|\mathrm{Cl}_{A_n}(\gamma)| = [A_n : C_{A_n}(\gamma)]$, and $C_{A_n}(\gamma) = A_n \cap C_{S_n}(\gamma)$. $|A_n \cdot C_{S_n}(\gamma)| = \frac{|A_n| \cdot |C_{S_n}(\gamma)|}{|C_{A_n}(\gamma)|}$.

If $C_{S_n}(\gamma) \nsubseteq A_n$, then $A_n \cdot C_{S_n}(\gamma) = S_n$, $\mathrm{Cl}_{S_n}(\gamma) = \mathrm{Cl}_{A_n}(\gamma)$. If $C_{S_n}(\gamma) \subseteq A_n$, then $|\mathrm{Cl}_{S_n}(\gamma)| = 2|\mathrm{Cl}_{A_n}(\gamma)|$.

If $\gamma = (abc)$ is 3-cycle and $n \geqslant 5$, then $(ef) \in C_{S_n}(\gamma) \setminus A_n$, $\mathrm{Cl}_{S_n}(\gamma) = \mathrm{Cl}_{A_n}(\gamma)$.

If $\gamma = \tau_1 \cdots \tau_k$ is a product of $k \geqslant 2$ disjoint 3-cycles, write $\tau_1 = (abc)$ and $\tau_2 = (def)$, then $(ad)(be)(cf) \in C_{S_n}(\gamma) \setminus A_n$, $\mathrm{Cl}_{S_n}(\gamma) = \mathrm{Cl}_{A_n}(\gamma)$.

5. If $n \geqslant 4$ and $n \neq 6$, then every automorphism of A_n maps 3-cycle to 3-cycle.

Let $\psi \in \mathrm{Aut}(A_n)$. If σ is a 3-cycle, the φ has order 3 and is product of $k \geqslant 1$ disjoint 3-cycles.

ψ maps conjugacy class in A_n of a 3-cycle to conjugacy class of a product of k disjoint 3-cycles.

If $n < 6$, then $k = 1$. If $n > 6$, $\frac{n(n-1)(n-2)}{3} = \frac{n!}{3^k k!(n-3k)!}$, the only solution is $k = 1$.

6. From 3, if $n \geqslant 4$ and $n \neq 6$, then every automorphism of A_n is the restriction of an inner automorphism of S_n on A_n, thus $\mathrm{Aut}(A_n) = \mathrm{Inn}(S_n) = \mathrm{Aut}(S_n) \cong S_n$ for $n \geqslant 4$ and $n \neq 6$. $\square$

$\operatorname{Aut}(A_6) = \operatorname{Aut}(S_6) \cong S_6 \rtimes \mathbb{Z}_2$

Proof:

$\operatorname{Aut}(A_6)$ which maps 3-cycles to 3-cycles is the restriction of a unique inner automorphism of S_6 on A_6, and any automorphism of A_6 maps 3-cycles to either 3-cycles or product of two disjoint 3-cycles, so $[\operatorname{Aut}(A_6) : \operatorname{Inn}(S_6)] \leqslant 2$.

For 3, fix $1 \neq \sigma \in A_n$, $c_\sigma \in \operatorname{Inn}(A_n)$ is action by conjugation of σ.

Define $\varphi : \operatorname{Aut}(S_n) \to \operatorname{Aut}(A_n)$, $\varphi(\rho) = \rho c_\sigma \rho^{-1}$ for $\rho \in \operatorname{Aut}(S_n)$. φ is monomorphism, so $\operatorname{Aut}(S_n) \leqslant \operatorname{Aut}(A_n)$

Since $[\operatorname{Aut}(S_6) : \operatorname{Inn}(S_n)] = 2$, we have $\operatorname{Aut}(A_6) = \operatorname{Aut}(S_6) \cong S_6 \rtimes \mathbb{Z}_2$. $\square$

$\operatorname{Out}(A_6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof:

$|\operatorname{Out}(A_6)| = |\operatorname{Aut}(A_6)| / |\operatorname{Inn}(A_6)| = 4$.

For all $\sigma, \rho \in \operatorname{Aut}(A_6)$, $\sigma\rho$ maps 3-cycle to 3-cycle and is an inner automorphism of S_n restricted on A_n.

$(\sigma\rho)^2$ is an inner automorphism of A_n, so $\operatorname{Out}(A_6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. $\square$

$\operatorname{Aut}(A_6)$ is not split extension of A_6.

Proof:

$$\begin{tikzcd}
1 \arrow[r] & \operatorname{Inn}(A_6) \arrow[r] & \operatorname{Aut}(A_6) \arrow[r] & \operatorname{Out}(A_6) \arrow[r] & 1 \\
1 \arrow[r] & A_6 \arrow[r] \arrow[u, "\cong"] & S_6 \rtimes \mathbb{Z}_2 \arrow[r] \arrow[u, "\cong"] & \mathbb{Z}_2 \times \mathbb{Z}_2 \arrow[r] \arrow[u, "\cong"] & 1
\end{tikzcd}$$

1. Prerequisites:

(1) Element in $\operatorname{Aut}(A_6) \setminus \operatorname{Inn}(A_6)$ swaps conjugate classes (abc) and $(abc)(def)$ in A_6.

(2) Element in $\operatorname{Aut}(S_6) \setminus \operatorname{Inn}(S_6)$ swaps conjugate classes (ab) and $(ab)(cd)(ef)$, (abc) and $(abc)(def)$ in S_6.

2. Suppose the sequence right splits and $\operatorname{Out}(A_6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \langle\sigma\rangle\langle\rho\rangle \leqslant \operatorname{Aut}(A_6)$ where $\sigma, \rho \in \operatorname{Aut}(A_6) \setminus \operatorname{Inn}(A_6)$, then $\langle\sigma\rangle\langle\rho\rangle \cap \operatorname{Inn}(A_6) = 1$. $\operatorname{Aut}(A_6) \cong \operatorname{Aut}(S_6)$, so ρ and σ can be considered as elements in $\operatorname{Aut}(S_6) \setminus \operatorname{Inn}(A_6)$.

If $\sigma, \rho \in \operatorname{Inn}(S_6) \setminus \operatorname{Inn}(A_6)$, then $\sigma\rho \in \operatorname{Inn}(A_6)$. Contradiction.

If $\rho \in \operatorname{Aut}(S_6) \setminus \operatorname{Inn}(S_6)$, $\sigma \in \operatorname{Inn}(S_6) \setminus \operatorname{Inn}(A_6)$, then $\sigma\rho \in \operatorname{Aut}(S_6) \setminus \operatorname{Inn}(S_6)$ and $\langle\sigma\rangle\langle\rho\rangle \cong \langle\sigma\rho\rangle\langle\rho\rangle$.

Therefore, we can always assume $\operatorname{Out}(A_6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \langle\sigma\rangle\langle\rho\rangle \leqslant \operatorname{Aut}(A_6)$ where $\sigma, \rho \in \operatorname{Aut}(S_6) \setminus \operatorname{Inn}(S_6)$.

3. $[\operatorname{Aut}(S_6) : \operatorname{Inn}(S_6)] = 2$, $\sigma \operatorname{Inn}(S_6) = \rho \operatorname{Inn}(S_6)$, $\rho^{-1}\sigma = c_\gamma \in \operatorname{Inn}(S_6)$ for some $\gamma \in S_6$, where c_γ is action of conjugation by γ. Since $\langle\sigma\rangle\langle\rho\rangle \cap \operatorname{Inn}(A_6) = 1$, $\gamma \in S_6 \setminus A_6$ is an odd permutation.

4. $(\rho^{-1}\sigma)^2 = c_\gamma^2 = 1$ gives $\gamma^2 = 1$, γ is transposition or product of three disjoint transpositions.

$\sigma\rho = \rho\sigma$ gives $\rho(\gamma) = \gamma$. But $\rho \in \operatorname{Aut}(S_6) \setminus \operatorname{Inn}(S_6)$ swaps conjugate classes (ab) and $(ab)(cd)(ef)$. Contradiction. $\square$

6 Automorphism group of permutation group S_6

Existence of outer automorphism of S_6

1. **Key step**: Construct a subgroup $H \triangleleft S_6$ which acts transitively on $\{1,2,3,4,5,6\}$ and $[S_6 : H] = 6$.

2. S_6 acts by left translation on S_6/H induces isomorphism $\varphi : S_6 \to S_6, \varphi \in \mathrm{Aut}(S_6)$.

3. Note that $\varphi(H) = S_5$, since H fixes coset H and permutes all other cosets.

4. H is transitive on $\{1,2,3,4,5,6\}$ while S_5 is not, so preimage of S_5 is not conjugacy to S_5. φ is not inner.

Construction 1:

S_5 acts by conjugation on its six Sylow 5-subgroups.

From Sylow's theorem, this action is transitive and induces homomorphism $f : S_5 \to S_6$.

This action is transitive, $\mathrm{im}(f) \geqslant 6$, so $\ker(f) = 1$. $\mathrm{im}(f)$ is transitive 120-element subgroup of S_6.

Construction 2:

$\mathrm{PGL}_2(\mathbb{F}_5)$ acts on $\mathbb{P}^1(\mathbb{F}_5)$

Definition: K is a field, $K^\times$ are its nonzero elements.

(1) $\mathrm{GL}_2(K)$ is the set of 2×2 invertible matrices, whose elements are in field K.

(2) $\mathrm{PGL}_2(K)$ is the quotient group $\mathrm{GL}_2(K)/K^\times$

(3) $\mathbb{P}^1(K)$ is the set of one-dimensional vector spaces (lines) in K^2.

There's a natural action of $\mathrm{GL}_2(K)$ on $\mathbb{P}^1(K)$, i.e. permuting the lines through origin of K^2.

Matrices of form $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ $(a \in K^\times)$ fix lines, so we have action of $\mathrm{PGL}_2(K)$ on $\mathbb{P}^1(K)$.

For $(x, y) \in K^2$ represented by $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, (x, y) is on a line of K^2 through origin, namely $[x : y]$.

If $y \neq 0$, then $[x : y] = [\dfrac{x}{y} : 1]$ corresponds to $\dfrac{x}{y} \in K$. If $y = 0$, then $[x : y] = [1 : 0]$ corresponds to the infinity point.

$\mathrm{GL}_2(K)$ acts on $\mathbb{P}^1(K)$: For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mathrm{GL}_2(K), \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in \mathbb{P}^1(K), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} ax+by \\ cx+dy \end{smallmatrix}\right) = \left(\begin{smallmatrix} a\frac{x}{y}+b \\ c\frac{x}{y}+d \end{smallmatrix}\right)$.

$\mathrm{PGL}_2(K)$ can be identified with group of linear fractional transformations $\{f(z) = \dfrac{az+b}{cz+d}, a, b, c, d \in K, ad - bc \neq 0\}$.

$f(x) = \dfrac{x-a}{x-c} \cdot \dfrac{b-c}{b-a}$ maps arbitrary (a, b, c) to $(0, 1, \infty)$, so $\mathrm{PGL}_2(K)$ acts on $\mathbb{P}^1(K)$ transitively.

Let $K = \mathbb{F}_p$, $|\mathrm{PGL}_2(K)| = \dfrac{|\mathrm{GL}_2(K)|}{p-1}$. $|\mathrm{GL}_2(K)| = (p^2-1)(p^2-p)$. $|\mathrm{PGL}_2(K)| = p^3 - p$.

For $p = 5$, $|\mathrm{PGL}_2(\mathbb{F}_5)| = 120$ and $\mathrm{PGL}_2(\mathbb{F}_5)$ acts transitively on $\mathbb{P}^1(\mathbb{F}_5)$, where $|\mathbb{P}^1(\mathbb{F}_5)| = 6$.

♚ $\mathrm{Aut}(S_6) \cong S_6 \rtimes \mathbb{Z}_2$ and $\mathrm{Aut}(S_6) \ncong S_6 \times \mathbb{Z}_2$.

♛ **Proof:**

1. For $n \geqslant 5$, proper subgroup of A_n has index at least n. Consider action by left translation of A_n on cosets.

2. $[\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)] \leqslant 2$. Element in $\mathrm{Aut}(S_6)$ maps conjugacy class (viii) to (viii)(inner) or (ix)(not inner).

3. S_5 acts by conjugation on its 6 Sylow 5-subgroups induces homomorphism $\varphi : S_5 \to S_6$. φ maps commutators to commutators, so $\varphi(A_5) \subseteq A_6$. $\varphi(A_5) = \varphi(A_5) \cap A_6 \leqslant \varphi(S_5) \cap A_6 < A_6$.

From 1, $|\varphi(A_5)| = \dfrac{5!}{2} \leqslant |\varphi(S_5) \cap A_6| \leqslant \dfrac{1}{6} \cdot \dfrac{6!}{2}$, thus $\varphi(A_5) = \varphi(S_5) \cap A_6$. $\varphi : S_5 \to S_6$ preserves parity.

4. S_6 acts by left translation on $\varphi(S_5)$ yields an automorphism of S_6 which is not inner.

$[S_6 : \varphi(S_5)] = [S_6 : S_5] = 6$, action of S_6 on $\varphi(S_5)$ by left translation yields an isomorphism $\psi : S_6 \to S_6$.

Suppose $\psi((12))$ is a transposition, then for some coset $x\varphi(S_5)$, $(12)x\varphi(S_5) = x\varphi(S_5)$, $x^{-1}(12)x \in \varphi(S_5)$.

Suppose $\varphi(\sigma) = x^{-1}(12)x$, since $x^{-1}(12)x$ is transposition and $\varphi : S_5 \to S_6$ preserves parity, σ is transposition.

For six Sylow 5-subgroups $X_1, \ldots, X_6$ of S_5, $\sigma(X_i)\sigma^{-1} = X_{\varphi(\sigma)(i)}$. $\varphi(\sigma)$ is transposition, $\exists X_j$ s.t. $\sigma(X_j)\sigma^{-1} = X_j$.

Suppose $X_j = \langle (abcde) \rangle, \sigma(abcde)\sigma^{-1} = (abcde)^k$, then $\sigma(abcde)^k\sigma^{-1} = (abcde)^{k^2} = (abcde)$, $k = \pm 1$.

WLOG suppose σ fixes a, then $\sigma(abcde)\sigma^{-1} = (a, \sigma(b), \sigma(c), \sigma(d), \sigma(e)) = (abcde)^{\pm 1}$, $\sigma = \mathrm{id}$ or $\sigma = (be)(cd)$.

Contradiction. Thus $\psi((12))$ is not transposition, $\psi \in \mathrm{Aut}(S_6)$ is not inner. $[\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)] = 2$.

5. We have short exact sequence of groups: $1 \to S_6 \xrightarrow{f} \mathrm{Aut}(S_6) \xrightarrow{\pi} \mathbb{Z}_2 \to 1$, $\mathbb{Z}_2 = \{\pm 1, \times\}$.

$\psi : (12) \mapsto (15)(23)(46)$, $(13) \mapsto (14)(26)(35)$, $(14) \mapsto (13)(24)(56)$, $(15) \mapsto (12)(36)(45)$, $(16) \mapsto (16)(25)(34)$.

$\psi \in \mathrm{Aut}(S_6) \setminus \mathrm{Inn}(S_6)$ and $\psi^2 = \mathrm{id}$. $\mathbb{Z}_2 \cong \langle \psi \rangle \leqslant \mathrm{Aut}(S_6)$, so $\mathrm{Aut}(S_6) \cong S_6 \rtimes \mathbb{Z}_2$.

6. This sequence right splits, so there exists homomorphism $g : \mathbb{Z}_2 \to \mathrm{Aut}(S_6)$ s.t. $\pi \circ g = \mathrm{id}$.

Let $g(-1) = \psi \notin \mathrm{Inn}(S_6)$, then $g(1) = \psi^2 = \mathrm{id}$. $f : S_6 \to \mathrm{Inn}(S_6)$, $g : \mathbb{Z}_2 \to \langle \psi \rangle$.

Claim: $\langle \psi \rangle$ is not a normal subgroup of $\mathrm{Aut}(S_6)$, so $\mathrm{Aut}(S_6) \ncong S_6 \times \mathbb{Z}_2$.

For $\sigma \in S_6$, define $\gamma_\sigma \in \mathrm{Inn}(S_6)$ to be the conjugation of σ. It's sufficient to prove $\gamma_\sigma \psi \gamma_\sigma^{-1} \neq \psi$ for some $\sigma \in S_6$.

For $\sigma = (12)$, $\gamma_\sigma \psi((12)) = (12)(15)(23)(46)(12) = (13)(25)(46)$, $\psi \gamma_\sigma((12)) = \psi((12)) = (15)(23)(46)$. $\gamma_\sigma \psi \neq \psi \gamma_\sigma$.

Therefore, $\mathrm{Aut}(S_6) \cong S_6 \rtimes \mathbb{Z}_2$, $\mathrm{Aut}(S_6) \ncong S_6 \times \mathbb{Z}_2$. $\square$

Conjugacy classes in S_6:

Conjugacy class	cycle type	order	sign	#	Conjugacy class	cycle type	order	sign	#
(i)	(123456)	6	-	120	(ii)	(123)(45)	6	-	120
(iii)	(12345)	5	+	144	(iv)	(1234)	4	-	90
(v)	(1234)(56)	4	+	90	(vi)	(123)	3	+	40
(vii)	(123)(456)	3	+	40	(viii)	(12)	2	-	15
(ix)	(12)(34)(56)	2	-	15	(x)	(12)(34)	2	+	45
(xi)	(1)	1	+	1					

♚ For Sylow 5-subgroup P of S_5, normalizer $N(P)$ has 20 elements.

♛ **Proof:**

For $P = \langle(abcde)\rangle$, 4-cycle $(bced)$ normalizes P. $|N(P)| \geqslant |\langle(abcde)\rangle| \cdot |\langle(bced)\rangle| = 20$ and $N(P) \nsubseteq A_5$.

If G is proper subgroup of A_5, then $|G| \leqslant \dfrac{|A_5|}{5} = 12$. If $|N(P)| > 20$, then $|N(P) \cap A_5| > 12$. Contradiction. $\square$

♞ Recall the construction of homomorphism $\varphi : S_5 \to S_6$ and isomorphism $\psi : S_6 \to S_6 \in \mathrm{Aut}(S_6) \setminus \mathrm{Inn}(S_6)$ before.

S_5 has six Sylow 5-subgroups, namely $X = \{X_1, X_2, X_3, X_4, X_5, X_6\}$.

S_5 acts on X by conjugation and induces $\varphi : S_5 \to S_6$. For $\sigma \in S_5, \sigma X_i \sigma^{-1} = X_{\varphi(\sigma)(i)}$.

$\varphi(S_5)$ is of index 6 in S_6, $S_6/\varphi(S_5) = \{y_1\varphi(S_5), y_2\varphi(S_5), y_3\varphi(S_5), y_4\varphi(S_5), y_5\varphi(S_5), y_6\varphi(S_5)\}$.

S_6 acts on $S_6/\varphi(S_5)$ by left translation and induces $\psi : S_6 \to S_6$. For $\rho \in S_6, \rho \cdot y_i\varphi(S_5) = y_{\psi(\rho)(i)}\varphi(S_5)$.

Properties of outer automorphism ψ defined before:

♚ 1. Outer automorphism ψ swaps 3-cycles (vi) and permutations of type $(abc)(def)$ (vii).

♛ If α, β are 3-cycles and $\psi(\alpha) = \beta$, $\alpha \cdot y_i\varphi(S_5) = y_{\beta(i)}\varphi(S_5)$.

3-cycle β has fixed points, there exists i_0 s.t. $\alpha \cdot y_{i_0}\varphi(S_5) = y_{i_0}\varphi(S_5)$. $y_{i_0}^{-1}\alpha y_{i_0} \in \varphi(S_5)$, $\gamma := \varphi^{-1}(y_{i_0}^{-1}\alpha y_{i_0})$ is 3-cycle.

$\varphi(\gamma)$ is 3-cycle and has fixed points, recall $\gamma X_i \gamma^{-1} = X_{\varphi(\gamma)(i)}$, there exists j_0 s.t. $\gamma X_{j_0} \gamma^{-1} = X_{j_0}$. 3-cycle $\gamma \in N(X_{j_0})$.

From claim before, $|N(X_{j_0})| = 20$, $N(X_{j_0})$ doesn't contain element of order 3. Contradiction.

♚ 2. Outer automorphism ψ swaps 6-cycles (i) and permutations of type $(abc)(de)$ (ii).

♛ If ψ maps conjugacy class of permutations of type $(abc)(de)$ to itself, the same reason yields normalizer of a Sylow 5-subgroup of S_5 containing an element of order 6. Contradiction.

♚ 3. Outer automorphism ψ preserves 4-cycles (iv) and permutations of type $(abcd)(ef)$ (v).

♛ Permutations of type $(abcd)$ are odd while permutations of type $(abcd)(ef)$ are even.

A_6 is characteristic subgroup of S_6, so $\psi \in \mathrm{Aut}(S_6)$ preserves parity, i.e. $\forall \tau \in S_6$, τ and $\psi(\tau)$ have the same sign.

In conclusion, any outer automorphism of S_6 swaps conjugacy classes (i) and (ii), swaps (vi) and (vii) and swaps (viii) and (ix) and preserves the others, i.e. swaps permutations of type $(abcdef)$ and $(abc)(de)$, (abc) and $(abc)(def)$, (ab) and $(ab)(cd)(ef)$ while preserving the others.