# CONJUGACY CLASSES AND AUTOMORPHISMS

COLTON GRAINGER (MATH 6130 ALGEBRA)

## 6. Assignment due 2018-10-17

6.1. **[1, No. 4.2.9].** If $p$ is a prime and $G$ is a group of order $p^\alpha$ for some $\alpha \in \mathbf{N}$, then every subgroup of index $p$ is normal in $G$. Therefore every group of order $p^2$ has a normal subgroup of order $p$.

*Given.* A group $G$ of order $p^\alpha$ with $p$ prime and $\alpha \in \mathbf{N}$.

*To prove.* Every subgroup of index $p$ is normal in $G$.

*Proof à la carte.* (We proved this in class as an application of the third isomorphism theorem; it's also in the text as a corollary of Cayley's theorem.)

Suppose $H \leq G$ and $|G : H| = p$. Let $\pi_H$ be the permutation representation $\pi \colon G \to S_G$ afforded by left multiplication of the cosets of $H$ in $G$, let $K = \ker \pi_H$, and let $|H : K| = k$. Now $|G : K| = |G : H|\,|H : K| = pk$. Since $H$ has $p$ left cosets, $G/K$ is isomorphic to a subgroup of $S_p$ be the first isomorphism theorem. By Lagrange's theorem, $pk = |G/K|$ divides $p = |G/H|$. Thus $k$ divides $(p-1)!$ But all the prime divisors of $k$ are at least as large as $p$. With $p$ chosen minimally, we're forced to accept $k = 1$, so $K = H$, and therefore $H \lhd G$. □

*Given.* A group $G$ of order $p^2$.

*To prove.* There exists a subgroup $H$ of $G$ where $|H| = p$.

*Proof.* By Cauchy's theorem, there's an element of order $p$ in $G$, call it $x$. Now $|G : \langle x \rangle| = p^2/p = p$. By the result à la carte, $\langle x \rangle$ is normal in $G$. □

6.2. **[1, No. 4.2.11].** Let $G$ be a finite group and let $\pi \colon G \to S_G$ be the left regular representation. If $x$ is an element of $G$ of order $n$ and $|G| = mn$, then $\pi(x)$ is a product of $m$ $n$-cycles. Therefore $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $\frac{|G|}{|x|}$ is odd.

*Given.* A finite group $G$ of order $mn$, an element $x$ of order $n$, and the left regular representation $\pi \colon G \to S_G$, arising from the action of $G$ on itself by left multiplication.

*To prove.* The permutation $\pi(x)$ is a product of $m$ disjoint $n$-cycles.

*Proof.* Since $x$ has order $n$, the cyclic subgroup $\langle x \rangle$ has index $mn/n = m$ in $G$. Now choose $m$ representatives $\{g_i\}_{i=1}^m$ from the *right* cosets $\langle x \rangle \backslash G$. Observe that each coset $\langle x \rangle g_i$ is recovered by $n$ repeated left multiplications by $x$, that is,

$$\langle x \rangle g_i = \bigcup_{j \in \mathbf{Z}} x^j g_i = \bigsqcup_{j=1}^{n} x_j g_i \text{ for all } g_i.$$

We'll now argue $\pi(x)$ is a product of $m$ $n$-cycles by writing each element of $G$ in the form $\pi^j(x)(g_i) = x^j g_i$ and counting. Our goal is to recover $G$ as a disjoint union of the images of the representatives $p_1, \ldots, p_m$ under the action of $\pi^j(x)$ for $j = 1, \ldots, n$. So,

$$G = \bigsqcup_{i=1}^{m} \bigsqcup_{j=1}^{n} x^j g_i = \bigsqcup_{i=1}^{m} \bigsqcup_{j=1}^{n} \pi^j(x)(g_i).$$

We conclude that $\pi(x)$ is the product of $m$ $n$-cycles. □

*Date:* 2018-10-05.
*Compiled:* 2018-10-17.

*Corollary.* For a finite group $G$, a left regular representation $\pi\colon G \to S_G$, and an element $x \in G$, the permutation $\pi(x)$ is odd if and only if $|x|$ is even and $|G| / |x|$ is odd.

*Proof.* With the lemma below, $\pi(x)$ is odd if and only if its cycle type contains an odd number of even integers, which occurs precisely when the disjoint cycle representation of $\pi(x)$ is a factorization containing an odd number of even length cycles. Well, borrowing notation from the proof above,

$$\text{the cycle type of } \pi(x) \text{ is } \underbrace{(n, n, \ldots, n)}_{m \text{ times}}.$$

So $\pi(x)$ is odd if and only if $|G| / |x| = m$ is odd and $|x| = n$ is even. □

**Lemma**. A permutation $\sigma \in S_G$ is odd if an only if an odd number of the $\tau_i$ in the disjoint cycle decomposition of $\sigma$ have even cycle length.

*Proof.* The sign of a permutation is a group homomorphism $\epsilon\colon S_G \to \{-1, 1\}$. Now for $\sigma \in S_G$ with disjoint cycle decomposition $\sigma = \tau_1\tau_2 \cdots \tau_m$, we have $\epsilon(\sigma) = -1$ if and only if $\epsilon(\tau_1)\epsilon(\tau_2)\cdots\epsilon(\tau_m) = -1$ if and only if an odd number of the $\tau_i$ are of even cycle length. □

6.3. **[1, No. 4.3.13].** The only finite group with exactly two conjugacy classes is isomorphic to the cyclic group $C_2$.

(That $C_2$ has two conjugacy classes is clear: they are the singletons $\{1\}$ and $\{-1\}$. We'll focus on uniqueness—showing that $C_2$ is (up to isomorphism) the *only* group with exactly two conjugacy classes.)

*Given.* A finite group $G$ with exactly two conjugacy classes.

*To prove.* $G$ is isomorphic to $C_2$.

*Proof.*[1] Consider the class equation

$$|G| = \frac{|G|}{|C_G(g_1)|} + \frac{|G|}{|C_G(g_2)|}.$$

By hypothesis $G \neq \{1\}$. It follows that each $C_G(g_i)$ contains at least two elements, 1 and $g_i$. Now let $n_1 = |C_G(g_1)|$ and $n_2 = |C_G(g_2)|$, and without loss of generality suppose $n_1 \le n_2$. To satisfy the class equation, we must have

$$1 = \frac{1}{n_1} + \frac{1}{n_2}.$$

Then $1 \le \frac{2}{n_2}$, so $n_1 \le 2$. Moreover $n_2 \le \frac{1}{1-\frac{1}{2}} = 2$. Therefore $n_1 = 2$ and $n_2 = 2$.

So for both of the representatives $g_i$ in $G$, we have $C_G(g) = 1, g$. Certainly one of the $g_i$ is the identity 1. The other is its own inverse, distinct from the identity.[2] Therefore $G \cong C_2$. □

6.4. **[1, No. 4.3.19].** Assume $H$ is a normal subgroup of $G$, $\mathscr{K}$ is a conjugacy class of $G$ contained in $H$ and $x \in \mathscr{K}$. We show $\mathscr{K}$ is a union of $k$ conjugacy classes of equal size in $H$, where $k = |G : HC_G(x)|$.

*Given.* $H \trianglelefteq G$, $\mathscr{K}$ a conjugacy class of $G$, $\mathscr{K} \subset H$.

*To prove*. For $x \in \mathscr{K}$, we have that $\mathscr{K}$ is a union of $k = |G : HC_G(x)|$ conjugacy classes in $H$.

*Proof.* $G$ acts transitively by conjugation on $\mathscr{K}$—for every pair of elements $a$ and $b$ in $\mathscr{K}$ is conjugate to the other in $G$. Now recall from the previous assignment [1, No. 4.1.9]:

> [When] $G$ acts transitively on the finite set $A$ and $H$ is a normal subgroup of $G$, with $\mathscr{O}_1, \mathscr{O}_2, \ldots, \mathscr{O}_k$ the distinct orbits of $H$ on $A$, we have that
>
> (a) $G$ is transitive on $\{\mathscr{O}_1, \ldots, \mathscr{O}_k\}$ and all orbits of $H$ on $A$ have the same cardinality.

[1]Keith Conrad [2] presents a general case for any finite number of conjugacy classes. Vipul Naik does so too here: `https://groupprops.subwiki.org/wiki/There_are_finitely_many_finite_groups_with_bounded_number_of_conjugacy_classes`.

[2]Why is the other forced to be its own inverse? This argument is awfully myopic.

Therefore, in our specific case, $G$ acts transitively on the orbits of the conjugation action of $H$ on $\mathscr{K}$. If these orbits of $H$ on $\mathscr{K}$ are denoted $\mathscr{O}_1, \ldots, \mathscr{O}_k$, then $|\mathscr{O}_1| = \cdots = |\mathscr{O}_k|$.

We now want to show that the number of such orbits $k = |G : HC_G(x)|$. Perhaps relabelling indices, let $x \in \mathscr{O}_1 \subset \mathscr{K}$. Citing again [1, No. 4.1.9], we have:

(b) If $a \in \mathscr{O}_1$, then $|\mathscr{O}_1| = |H : H \cap \mathrm{Stab}_G(a)|$. Furthermore, $k = |G : H\mathrm{Stab}_G(a)|$.

In our specific case, both $G$ and $H$ act on $\mathscr{K}$ by conjugation. We thus recognize $\mathrm{Stab}_G(a) = C_G(a)$ for points $a$ in $\mathscr{K}$. That $k = |G : HC_G(x)|$ is immediate. For clarity of argument, however, we'll find $k$ directly from the diamond isomorphism theorem, ignoring[3] the result [1, No. 4.1.9] (b) .

Onwards! Consider the centralizer of $x$ in $G$ and $C_G(x)$ and $H \trianglelefteq G$. Now by the diamond isomorphism theorem we have the lattice

$$\begin{tikzcd}
 & HC_G(x) \arrow[dl, dash] \arrow[dr, equal] & \\
C_G(x) \arrow[dr, equal] & & H \arrow[dl, dash] \\
 & C_H(x) &
\end{tikzcd}$$

where we've observed that $C_H(x) = \{h \in H : hx = xh\} = \{g \in G : g \in H \text{ and } gx = xg\} = H \cap C_G(x)$ for the bottom node. As a consequence of the diamond isomorphism theorem,

$$\frac{HC_G(x)}{H} \cong \frac{C_G(x)}{C_H(x)} \quad \text{therefore} \quad |HC_G(x)| = \frac{|C_G(x)|\,|H|}{|C_H(x)|}.$$

By orbit stabilizer for the action of $G$ and $H$ on $\mathscr{K}$,

$$|\mathscr{K}| = \frac{|G|}{|C_G(x)|} \quad \text{and, zooming in to action of } H, \quad |\mathscr{O}_1| = \frac{|H|}{|C_H(x)|}.$$

Noting $\mathscr{K}$ is the union of disjoint orbits $\mathscr{O}_i$ of the same size, we find $k = \frac{|\mathscr{K}|}{|\mathscr{O}_1|}$ as follows

$$\begin{aligned}
k &= |\mathscr{K}| \cdot \frac{1}{|\mathscr{O}_1|} \\
&= \frac{|G|}{|C_G(x)|} \cdot \frac{|C_H(x)|}{|H|} \\
&= \frac{|G|}{|HC_G(x)|} \\
&= |G : HC_G(x)|\,.
\end{aligned}$$

Therefore $\mathscr{K}$ is the union of $|G : HC_G(x)|$ equally sized orbits of $H$. □

**Corollary.** A conjugacy class in $S_n$ that consists of even permutations is either a single conjugacy class under the action of $A_n$ or is a union of two classes of the same size in $A_n$.

*Proof.* Say that $\mathscr{K}$ is a conjugacy class of $S_n$ that consists of only even permutations. We recognize $A_n$ is normal in $S_n$, so the hypotheses of the previous result are satisfied our specific case. Thus, $\mathscr{K}$ is the union $|A_n C_G(x)|$ equally sized orbits of $A_n$ acting by conjugation on $\mathscr{K}$. Since

$$\frac{n!}{2} = |A_n| \leq |A_n C_G(x)|$$

we must have the index of $A_n C_G(x)$ in $S_n$ either 1 or 2. □

[3] I had to revise it anyways.

6.5. **[1, No. 4.3.23].** If $M$ is a maximal subgroup of $G$ then either $N_G(M) = M$ or $N_G(M) = G$. Therefore, if $M$ is a maximal subgroup of $G$ that is not normal in $G$ then the number of nonidentity elements of $G$ that are contained in conjugates of $M$ is at most $(|M| - 1) \cdot |G : M|$.

*Given.* A maximal subgroup $M$ of $G$.

*To prove.* Either $N_G(M) = M$ or $N_G(M) = G$. Also, the number of non-identity elements of $G$ that are contained contained in conjugates of $M$ is at most $(|M| - 1) \cdot |G : M|$.

*Proof.* Since $M \leq N_G(M) \leq G$ and $M$ is maximal in $G$, either $N_G(M) = M$ or $N_G(M) = G$. Now to put an upper bound on the number of nonidentity elements of $G$ contained in conjugates of $M$, assuming $M$ is *not* normal in $G$. The key idea is to note that conjugation is an automorphism of $G$, so any conjugate $gMg^{-1}$ is isomorphic to $M$. Since the identity is only conjugate to itself, the number of non-identity elements in each conjugate $gMg^{-1}$ is $|M| - 1$. We can partition $G$ into $|G : M|$ disjoint left cosets of $M$, but we can't partition $G$ into conjugates of $M$, for conjugation fixes the identity element. So we have at most $(|M| - 1)$ non-identity elements of $M$ to work with. Since the index of $M$ in $G$ is $|G : M|$, we conclude there are at most $(|M| - 1)\,|G : M|$ distinct non-identity elements of $G$ in conjugates of $M$. □

6.6. **[1, No. 4.3.24].** Assume $H$ is a proper subgroup of the finite group $G$. Then $G$ is not the union of the conjugates of any proper subgroup, i.e.,

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

*Proof.* If $G$ is a proper subgroup of $G$, then $H \leq M$ for some maximal subgroup $M \leq G$. By [1, p. 4.3.23],

$$\begin{aligned} \left| \bigcup_{g \in G} gHg^{-1} \right| &\leq (|M| - 1)\,|G : M| \\ &= |G| \cdot \frac{|M| - 1}{|M|} \\ &< |G|\,. \end{aligned}$$

We conclude that $G$ is not the union of conjugates of the proper subgroup $H$. □

6.7. **The size of each conjugacy class in $S_n$ [1, No. 4.3.33].** Let $\sigma$ be a permutation in $S_n$ and let $m_1, \ldots, m_s$ be *distinct* integers that appear in the cycle type of $\sigma$ (including 1-cycles). For each $i \in \{1, 2, \ldots, s\}$ assume $\sigma$ has $k_i$ cycles of length $m_i$ (so that $\sum_{i=1}^{s} k_i m_i = n$). Then the number of conjugates of $\sigma$ is

$$\frac{n!}{(k_1!m_1^{k_1})(k_2!m_2^{k_2}) \cdots (k_s!m_s^{k_s})}.$$

*Proof.* Suppose $\sigma \in S_n$ is as described above. Place out parentheses according to the cycle type of $\sigma$. There are $n!$ ordered arrangements of exactly $n$ distinct indices without repetition into the parentheses.[4]

Now cyclic permutations of indices in a set of parentheses are equivalent, so for each $m_i$ cycle in $\sigma$ we mod out the $n!$ arrangements by $m_i^{k_i}$, the number of cyclic permutations of indices affecting equivalent arrangements of the indices in the $m_i$ cycles.

Furthermore, permutations of the order in which order disjoint cycles are listed in the cycle decomposition of $\sigma$ are equivalent, so for each $k_i$, we mod out $n!/\left(\prod_{i=1}^{s} m_i^{k_i}\right)$ by the possible reorderings $k_i!$ for each $k_i$ that's the number of $m_i$-length cycles appearing in the decomposition of $\sigma$.

Therefore, the number of distinct conjugates of $\sigma$ in $S_n$ is given by

$$n/\left(\prod_{i=1}^{s} k_i!m_i^{k_i}\right) = \frac{n!}{(k_1!m_1^{k_1})(k_2!m_2^{k_2}) \cdots (k_s!m_s^{k_s})}.$$

[4]Being polite: We assume the parentheses are not nested, we require there are $n$ total positions in between all the pairs, and we also assume that the parentheses are open and closed ecumenically.

**Examples.** If $n \geq m$ then the number of $m$-cycles in $S_n$ is given by

$$\frac{n(n-1)(n-2)\ldots(n-m+1)}{m}.$$

If $n \geq 4$ then the number of permutations in $S_n$ that are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$. The later will come into use as a base case for determining the order of the conjugacy classes of elements with order 2 in $S_n$

6.8. **[1, No. 4.4.3].** Under any automorphism of $D_8$, $r$ has at most 2 possible images and $s$ has at most 4 possible images. Thence $|\mathrm{Aut}(D_8)| \leq 8$.

*Demonstration.* Suppose $\varphi$ is an automorphism of $D_8$. Now $\varphi$ preserves some structural group properties, e.g., elements of an order are mapped to elements of the same order. Hence

$$r \mapsto r \text{ or } r^3, \text{ which are elements of order 4.}$$

Note we cannot have $s \mapsto r^2$ for then

$$\varphi(\underbrace{rs}_{|rs|=2}) \neq \varphi(r)\varphi(s) = \underbrace{r^3 \text{ or } r}_{\text{order } 4}.$$

Therefore, by order considerations

$$s \mapsto s, rs, r^2 s, r^3 s.$$

Now $\varphi$ is determined by the images of the generators $r$ and $s$. Observe the are at most $2 \cdot 4$ distinct choices for these images. Hence $|\mathrm{Aut}(D_8)| \leq 8$. □

6.9. **[1, No. 4.4.8].** Suppose $G$ is a group with subgroups $H$ and $K$ where $H \leq K$.

(b) If $H$ is characteristic in $K$ and $K$ is characteristic in $G$, then $H$ is characteristic in $G$. Thence the *Viergruppe* $V_4$ is characteristic in $S_4$.

*Proof.* For each $\varphi \in \mathrm{Aut}(G)$, observe $\varphi|_K$ is automorphism of $K$. Note $\varphi|_K(H) = H$ because $H \mathrm{char} K$. Extending back to $\varphi$, we have $\varphi(H) = H$, as desired to show $H \mathrm{char} G$. □

In the specific case of $V_4$ characteristic in $A_4$, characteristic in $S_4$, transitivity implies $V_4$ is characteristic in $S_4$.

To show the first two relations, say $\varphi \in \mathrm{Aut}(G)$. Note $V_4 = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$. The automorphism $\varphi$ maps conjugate elements to eachother. By the lattice isomorphism theorem, $V_4 = \varphi(V_4) = \langle \varphi((1\,2)(3\,4)), \varphi((1\,3)(2\,4)) \rangle$. For the second relation, suppose $\psi \in \mathrm{Aut}(S_4)$. By order considerations, $\psi$ must map any two distinct 3-cycles in $A_4$ to other distinct 3-cycles in $A_4$. Therefore $\psi(A_4) = \langle \psi((i_1 i_2 i_3)), \psi((j_1 j_2 j_3)) \rangle = A_4$, since 3-cycles generate $A_4$.

We have seen $V_4$ is characteristic in $A_4$ is characteristic in $S_4$. Hence $V_4$ is characteristic in $S_4$.

(c) If $H$ is normal in $K$ and $K$ is characteristic in $G$, then $H$ need not be normal in $G$.

Consider $H = \langle (1\,2)(3\,4) \rangle$, $K = V_4$, and $G = A_4$. Since $V_4$ is abelian, $H$ is normal in $V_4$. Yet for $\sigma = (1\,2\,3) \in A_4$, conjugation by $\sigma$ of $H$ produces the element $(1\,3)(2\,4) \notin H$. So $H \ntrianglelefteq A_4$.

6.10. **[1, No. 4.4.18].** For $n \neq 6$ every automorphism of $S_n$ is inner. Fix an integer $n \geq 2$ with $n \neq 6$.

(a) The automorphism group of a group $G$ permutes the conjugacy classes of $G$, i.e., for each $\sigma \in \mathrm{Aut}(G)$ and each conjugacy class $\mathscr{K}$ of $G$ the set $\sigma(\mathscr{K})$ is also a conjugacy class of $G$.

*Given.* A group $G$, its automorphism group $\mathrm{Aut}(G)$, and the collection $\Omega = \{\mathscr{K} : \text{ conjugacy classes in } G\}$.

*To prove.* If $\sigma \in \mathrm{Aut}(G)$ and $\mathscr{K} \in \Omega$, then $\sigma(\mathscr{K}) \in \Omega$.

*Proof.* Suppose $a$ and $b$ are conjugate elements in $G$. Then for some $g \in G$, $a = gbg^{-1}$. Consider the image under automorphism, $\sigma(a) = \sigma(g)\sigma(b)\sigma(g)^{-1}$. So $\sigma(a)$ and $\sigma(b)$ are conjugate.

Pairwise conjugacy of the points in the image of $\mathscr{K}$ under $\sigma$ implies $\sigma(\mathscr{K}) \subset \mathscr{F} \in \Omega$. Now to show $\mathscr{F} \subset \sigma(\mathscr{K})$. Let $c \in \mathscr{F}$. Then $\sigma(a) = hch^{-1}$ for some $h \in G$. Applying the inverse automorphism $\sigma^{-1}$, we see $a$ is conjugate to $\sigma^{-1}(c)$, thus $\sigma^{-1}(c) \in \mathscr{K}$. Thus $\sigma^{-1}(\mathscr{F}) \subset \mathscr{K}$. Applying $\sigma$, we conclude $\mathscr{F} \subset \sigma(\mathscr{K})$.

(b) Let $\mathscr{K}$ be the conjugacy class of transpositions in $S_n$ and let $\mathscr{K}'$ be the conjugacy class of any element of order 2 in $S_n$ that is not a transposition. Then $|\mathscr{K}| \neq |\mathscr{K}'|$. Furthermore, any automorphism of $S_n$ sends transpositions to transpositions.

If $n < 4$ the only elements of order 2 are transpositions. Therefore $\mathscr{K}' = \varnothing$. So suppose $n \geq 4$. Elements of order 2 in $S_n$ that are not transpositions are products of $k$ many disjoint 2-cycles. We observe $2 \leq 2 \leq \lceil n \rceil$.

We now show $|\mathscr{K}| \neq |\mathscr{K}'|$ for all $n, k$ with the exception of $(n, k) = (6, 3)$, for which there are 15 elements in both the conjugacy class $\mathscr{K}$ of transpositions and in the class $\mathscr{K}' = \{\text{products of 3 disjoint 2-cycles}\}$.

We generate a heatmap plot of the value $|\mathscr{K}'| - |\mathscr{K}|$, where both are defined:

```
dim = 10
A = np.full([dim,dim], float('nan'))
for n in np.arange(2,b):
    for k in np.arange(2,int(n/2.0)+1):
        A[n,k] = -(n*(n-1)/2) + np.math.factorial(n)/(np.math.factorial(k)*2**k)
```

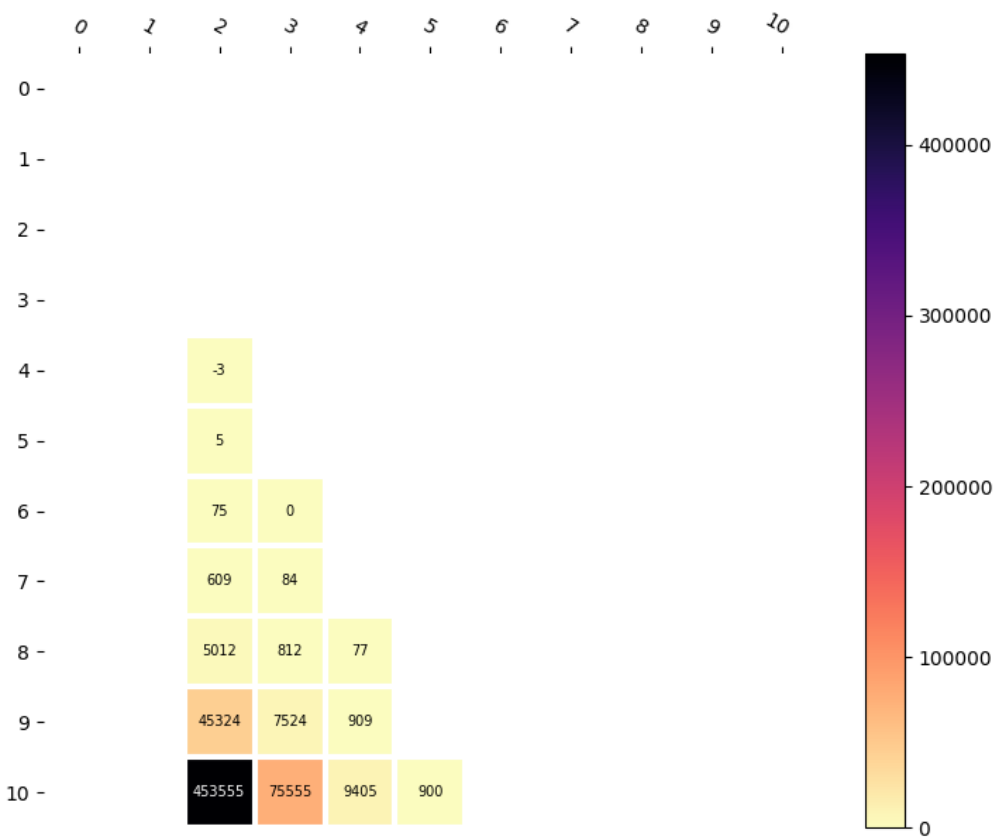


Figure 1. heat

By previous exercise, we have

$$|\mathscr{K}| = \frac{n(n-1)}{2} \quad \text{and} \quad \left|\mathscr{K}'\right| = \frac{n!}{k!2^k}.$$

The heatmap provides a base case, and it's clear that $|\mathscr{K}'|$ strictly dominates $|\mathscr{K}|$ for, say, $n \geq 9$ and $k \geq 4$.

Since $\sigma$ must preserve the order of both conjugacy classes and elements in them, we see that $\sigma$ stabilizes the set $\mathscr{K}$ of transpositions, as desired.

(c) For each $\sigma \in \mathrm{Aut}\,(S_n)$ we have

$$\sigma\colon (1\,2) \mapsto (a\,b_2), \qquad \sigma\colon (1\,3) \mapsto (a\,b_3), \quad \ldots, \quad \sigma\colon (1\,n) \mapsto (a\,b_n)$$

for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, 2, \ldots, n\}$.

Say $(1\;j) \mapsto (a\,b)$ and $(1\;j) \mapsto (c\,d)$. Then $(i\;j)(1\;i)(i\;j) = (1\;j)$. If $\{a, b\}$ and $\{c, d\}$ are disjoint, there's no $\sigma \in S_n$ such that

$$\sigma(a\,b)\sigma = (c\,d),$$

a contradiction. So $\{a, b\}$ and $\{c, d\}$ meet. Since $\sigma$ is injective, the only available conclusion is apparent:

$$\sigma\colon (1\,2) \mapsto (a\,b_2), \qquad \sigma\colon (1\,3) \mapsto (a\,b_3), \quad \ldots, \quad \sigma\colon (1\,n) \mapsto (a\,b_n)$$

for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, 2, \ldots, n\}$.

(d) Therefore $(1\,2), (1\,3), \ldots, (1\,n)$ generate $S_n$. Furthermore $S_n$ is uniquely determined by its action on these elements. Then by (c), $S_n$ has at *most* $n!$ automorphisms. We conclude that $\mathrm{Aut}\,(S_n) = \mathrm{Inn}(S_n)$ for $n \neq 6$.

In class we showed that $S_n$ is generated by simple transpositions. These in turn are generated by the set of transpositions including the index 1, e.g., $(i\;j) = (1\;j)(1\;i)(1\;j)$. Since there are precisely $n!$ arrangements of $1, 2, 3, \ldots, n$ mapping bijectively to $a, b_2, b_3, \ldots, b_n$, we see that $|\mathrm{Aut}\,(S_n)| \leq |S_n|$. But also $|S_n| = |\mathrm{Inn} S_n| \leq |\mathrm{Aut}\,(S_n)|$. Therefore $|\mathrm{Inn} S_n| = \mathrm{Aut}\,(S_n)$. $\square$

6.11. **[1, No. 4.4.20].** For any finite group $P$, let $d(P)$ be the minimum[5] number of generators of $P$. Let $m(P)$ be the maximum of the integers $d(A)$ as $A$ runs[6] over all *abelian* subgroups of $P$. Define the *Thompson subgroup* of $P$ as

$$J(P) = \langle A : A \text{ is an abelian subgroup of } P \text{ with } d(A) = m(P)\rangle.$$

(a) $J(P)$ is a characteristic subgroup of $P$.

(b) For each of the following groups $P$, we exhaustively list all abelian subgroups $A$ of $P$ that satisfy $d(A) = m(P)$.

- $Q_8$
- $D_8$
- $D_{16}$
- $QD_{16}$ (the quasidihedral group of order 16)

[5]For example, $d(P) = 1$ if and only if $P$ is a nontrivial cyclic group and $d(Q_8) = 2$.
[6]For example, $m(Q_8) = 1$ and $m(D_8) = 2$.

6.12. **Classification of simple groups of size less than 60.** If a simple group has order less than 60, then it is abelian.

*Given.* The set $\mathscr{S}$ of all groups $G$ such that $1 \leq |G| \leq 59$.

*To show.* Exhaustively, that each group $G$ in $\mathscr{S}$ is abelian or not simple.

*Demonstration.*

- The trivial group $\{1\}$ is not simple, by definition of simple as having no *nontrivial* proper normal subgroup.
- By Lagrange's theorem, groups of prime order are cyclic, therefore abelian.
- By the class equation, groups of prime power order $p^\alpha$ for $p$ prime and $\alpha \in \mathbf{Z}_{\geq 0}$ have non-trivial centers.
  - Either center of the group is the group itself and the group is abelian, or
  - or the center of the group is a (normal) nontrivial proper subgroup, in which case the group is not simple.
- By the lemma below, groups of order $pq$ (where $p$ and $q$ are primes) are not simple.
- By the lemma below, groups of order $p^2q$ (where $p$ and $q$ are primes) are not simple.
- What orders of groups in $\mathscr{S}$ remain to be discussed?

| order | prime factorization |
|---|---|
| 24 | $2^3 \cdot 3$ |
| 30 | $2 \cdot 3 \cdot 5$ |
| 36 | $2^2 \cdot 3^2$ |
| 40 | $2^2 \cdot 3^2$ |
| 42 | $2 \cdot 3 \cdot 7$ |
| 48 | $2^4 \cdot 3$ |
| 60 | $2^2 \cdot 3 \cdot 7$ |

**Lemma.** Groups of order $pq$ (where $p$ and $q$ are primes) are not simple. Moreover, groups of order $p^2q$ are also not simple.

*Given.* Primes $p$ and $q$ (WLOG $p < q$), a group $G$ of order $pq$, a group $K$ of order $p^2q$.

*To prove.* Both $G$ and $K$ posses normal nontrivial proper subgroups.

*Proof.*

## 7. References

[1] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed. Hardcover; Prentice Hall, 2004 [Online]. Available: `http://www.worldcat.org/isbn/0471433349`

[2] K. Conrad, "Conjugation" [Online]. Available: `http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/conjclass.pdf`