Abstract Algebra. Math 6320. Bertram/Utah 2022-23.
Products and Automorphisms

Let $N \subset G$ be a normal subgroup, and view it as a short exact sequence:

$$(*)\ 1 \to N \xrightarrow{i} G \xrightarrow{q} G/N \to 1$$

with inclusion map $i(n) = n$ and quotient map $q(g) = gN$.

Remark. We'll use "1" instead of "0" to reflect the fact that the operation is multiplication, and we will only name the inclusion map when it is lends clarity.

Unlike the case with abelian groups or categories, there is a difference in this non-abelian setting between left splittings and right splittings of a sequence $(*)$. Recall that the sequence is left-split by a "backwards" (surjective) group homomorphism

$$\phi : G \to N \text{ such that } \phi \circ i = \mathrm{id}_N : N \to N$$

and it is right-split by a "backwards" (injective) group homomorphism

$$f : G/N \to G \text{ such that } q \circ f = \mathrm{id}_{G/N} : G/N \to G/N$$

Given a left splitting, the kernel $K = \ker(\phi)$ satisfies $N \cap K = \{e\}$ since:

$$i(n) \in i(N) \cap K \text{ implies } n = \phi(i(n)) = e$$

Thus, the map $q|_K : K \to G/N$ is injective. Now suppose $gN = q(g)$. Then:

(a) $q(g \cdot (i \circ \phi(g))^{-1}) = q(g)$ since $i(\phi(g))^{-1} \in N$, and

(b) $\phi(g \cdot (i \circ \phi(g))^{-1}) = \phi(g) \cdot (\phi \circ i)(\phi(g))^{-1} = e$ so $g \cdot (i \circ \phi(g))^{-1}) \in K$.

Thus $q|_K : K \to G/N$ is surjective, and an isomorphism. Its inverse:

$$f = (q|_K)^{-1} : G/N \to K \text{ is a right splitting of the sequence!}$$

Thus a left split sequence is **both** left and right split, $NK = G$, and:

$$(\phi, f \circ q) : G = NK \to N \times K \text{ is an isomorphism with inverse } (n,k) \mapsto nk$$

This is what one would expect from our work on abelian categories.

A right splitting, however, may not split the group G. Given a right splitting of $(*)$, let $H = \mathrm{im}(f) \subset G$. Then $N \cap H = \{e\}$ and $G = NH$, as with a left splitting, but in this case $G = NH$ is **not** (in general) isomorphic to $N \times H$. The failure to split will be measured by a group homomorphism.

Examples. The following sequence is right-split but not a product:

$$1 \to C_3 \to S_3 \to C_2 \to 1,\ C_2 \cong \{e, (1\ 2)\} \subset S_3$$

This generalizes to the (non-abelian!) *dihedral* groups with right-split sequences:

$$1 \to C_n \to D_{2n} \to C_2 \to 1;\ C_2 \cong \{e, r\} \text{ where } r \text{ is a reflection}$$

It also directly generalizes to the other symmetric groups via right-split sequences:

$$1 \to A_n \to S_n \to C_2 \to 1,\ C_2 \cong \{e, \tau\} \text{ for any transposition } \tau \in S_n$$

There are, of course, short exact sequences that do not have any splittings.

Examples. (a) Recall that the short exact sequence of abelian groups:

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

does not right-split (otherwise C_4 would be isomorphic to $C_2 \times C_2$).

(b) For a non-abelian example, consider the group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with quaternionic multiplication. Then Q_8 has three normal cyclic subgroups generated by each of i, j, k (or their negatives). But none of the resulting short exact sequences:

$$1 \to C_4 \to Q_8 \xrightarrow{q} C_2 \to 1$$

is right-split since the only C_2 subgroup of Q_8 is $\{\pm 1\}$, which is *contained* in every C_4 subgroup and therefore maps to $\{e\}$ under q in every short exact sequence.

Proposition 1. Given a right-split sequence $(*)$ and $H = f(G/N)$, the conjugation group homomorphism (of elements of N by elements of H):

$$c : H \to \ \mathrm{Aut}_{\mathcal{G}r}(N); \ c_h(n) = hnh^{-1}$$

exaplains how to multiply elements n_1h_1 and n_2h_2 in $NH = G$.

Proof. Recall that conjugation by h is a group homomorphism:

$c_h(e) = heh^{-1} = e$ and $c_h(n_1n_2) = h(n_1n_2)h^{-1} = (hn_1h^{-1})(hn_2h^{-1}) = c_h(n_1)c_h(n_2)$

and overall, conjugation c is a group homomorphism from H:

$$c_{h_1h_2}(n) = (h_1h_2)n(h_1h_2)^{-1} = h_1(h_2nh_2^{-1})h_1^{-1} = (c_{h_1} \circ c_{h_2})(n)$$

and in particular, $c_h \circ c_{h^{-1}} = c_e = \mathrm{id}_N$ so each c_h is a group automorphism of N. From this, we get $hnh^{-1} = c_h(n)$ and $hn = c_h(n) \cdot h$, and the multiplication:

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2)h_2 = (n_1c_{h_1}(n_2))(h_1h_2) \quad \square$$

Corollary. If $H \subset G$ is *normal* for a right-split sequence $(*)$, then:

$$c_h(n) = n \text{ for all } h \text{ and } n, \text{ i.e. } G = NH = N \times H$$

Proof. If $H \subset G$ is normal, it gives a short exact sequence:

$$(**) \ 1 \to H \to G \to G/H \to 1$$

that is left-split by the right splitting $G/N \xrightarrow{\sim} H$ of $(*)$, so it is also right-split! Turning this around, $(*)$ is left-split by the right splitting of $(**)$ and then, as we've seen already, $G = NH = N \times H$ and $c_h(n) = n$ in this split group. $\square$

We have a converse to Proposition 1,

Proposition 2. Groups N, H and a group homomorphism $\phi : H \to \mathrm{Aut}_{\mathcal{G}r}(N)$ define a "twisted" multiplication on the Cartesian product $H \times N$ via:

$$(n_1h_1)(n_2h_2) = (n_1 \cdot \phi_{h_1}(n_2))(h_1h_2)$$

This group, denoted by $N \rtimes_\phi H$ (or just $N \rtimes H$) fits in a right-split sequence:

$$1 \to N \to N \rtimes H \to H \to 1$$

for which $c_h(n) = \phi_h(n)$.

Proof. One shows that the multiplication is associative (exercise). Then:

$$(n_1e)(n_2e) = (n_1n_2)e \text{ and } (eh_1)(eh_2) = e(h_1h_2)$$

shows that N, H are subgroups of $N \rtimes H$, and $1 \to N \to N \rtimes H \to H \to 1$ is a short exact (right-split) sequence via the group homomorphism $(nh) \mapsto h$. Moreover, since the product $(n_1n_2)(h_1h_2) = (n_1c_{h_1}(n_2))(h_1h_2)$ it follows that $\phi_h = c_h$ for all $h \in H$. Thus the homomorphism ϕ converts to conjugation in $N \rtimes H$! $\square$

In the previous section we used the Sylow Theorems to find normal subgroups. We can also use them to classify groups of various orders.

Application. If G has "complementary" subgroups $N, H \subset G$ satisfying:

$$N \cap H = \{e\}, \quad HN = G \text{ and } N \text{ is normal}$$

then G is a semi-direct product $N \rtimes H$ for some homomorphism $\phi : H \to \mathrm{Aut}_{\mathcal{G}r}(N)$. If $H = K$ is also normal, then $\phi = \mathrm{id}$, and $G = N \times H$.

Proposition 3. If $|G| = pq$ for primes $p < q$ and:

(i) p does not divide $q-1$, then $G = C_q \times C_p = C_{pq}$ is cyclic.

(ii) p does divide $q-1$, then G is a semi-direct product $G = C_q \rtimes C_p$.

Proof. By the Sylow theorems $C_q = N \subset G$ (the q-Sylow subgroup) is normal and $C_p = H \subset G$ is a p-Sylow subgroup, which is normal in case (i), so $G = C_q \times C_p$. But it may not be normal in (ii), so we only conclude that G is a semi-direct product.

So in case (ii), how many isomorphism classes of semi-direct products are there? To understand this, we need to begin to understand the groups of automorphisms:

$$\mathrm{Aut}_{\mathcal{G}r}(N) \text{ of an arbitrary group } N$$

We start with essentially the only easy case:

Proposition 4. If $N = C_n$ is cyclic, then $\mathrm{Aut}_{\mathcal{G}r}(N) \cong ((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$.

Proof. Let $g \in C_n$ be a generator. Then a group automorphism $f : C_n \to C_n$ is entirely determined by $f(g) = g^k$, and to be invertible, we need $\gcd(k, n) = 1$, i.e. we need $k \in (\mathbb{Z}/n\mathbb{Z})^*$. But then the composition of $f_1(g) = g^{k_1}$ and $f_2(g) = g^{k_2}$ is:

$$f_1(f_2(g)) = f_1(g^{k_2}) = (g^{k_2})^{k_1} = g^{k_1 k_2}$$

and so composition (of automorphisms) corresponds to multiplication in $(\mathbb{Z}/n\mathbb{Z})^*$.

Thus a semidirect product $C_n \rtimes H$ corresponds to a homomorphism:

$$\phi : H \to (\mathbb{Z}/n\mathbb{Z})^*$$

Recall also that if $n = p$ is **prime**, then $(\mathbb{Z}/n\mathbb{Z})^* = C_{p-1}$ is cyclic.

Definition. The dihedral group D_{2n} is the semi-direct product:

$$1 \to C_n \to D_{2n} \to C_2 \to 1$$

given by $\phi(h) = -1$, i.e. $\phi_h(g) = g^{-1}$ for $g \in C_n$ and the non-trivial $h \in C_2$.

Corollary. If $|G| = 2q$, then G is either the cyclic group or the dihedral group.

Proof. The q-Sylow subgroup $C_q \subset G$ is unique and normal and any of the 2-Sylow subgroups $C_2 \subset G$ is complementary to C_q in the sense of the application. So G is a semi-direct product $C_q \rtimes C_2$. Since $(\mathbb{Z}/q\mathbb{Z})^* = C_{q-1}$ has only one element of order two, it follows that the only non-trivial homomorphism $\phi : C_2 \to (\mathbb{Z}/q\mathbb{Z})^*$ is the map $\phi(h) = q-1$, i.e. $\phi_h(g) = g^{q-1} = g^{-1}$, which gives the dihedral group. $\square$

In particular, we have now classified all groups of order:

$$2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 15, 17, 19, 22, 23, 25, 26, 29$$

leaving us to deal with (among groups of order < 30):

$$8, 12, 16, 18, 20, 24, 27, 28$$

When $|G| = 28$, **both** the 7-Sylow subgroup and 2-Sylow subgroups are normal, so $G = C_7 \times C_4 = C_{28}$ or $G = C_7 \times C_2 \times C_2$ (depending on the 2-Sylow subgroup).

Of the rest of the orders, we know that:

$$|G| = 18 = 9 \cdot 2 \text{ implies that } G = N \rtimes C_2 \text{ for } |N| = 9$$
$$|G| = 20 = 5 \cdot 4 \text{ implies that } G = C_5 \rtimes H \text{ for } |H| = 4$$
$$|G| = 21 = 7 \cdot 3 \text{ implies that } G = C_7 \rtimes C_3$$

We handle the case $|G| = 21$ first with a strengthening of Proposition 3.

Proposition 5. In the setting of Proposition 3(b), G is either:

$$C_q \times C_p \text{ or it is isomorphic to a single semi-direct product } C_q \rtimes C_p$$

Proof. If p divides $q - 1$, then the equation $x^p \equiv 1 \pmod q$ has exactly p solutions, including the trivial solution $x = 1$ (by Fermat's Little Theorem). If we let $h \in H = C_p$ and $g \in C_q$ be generators, this gives p semi-direct products:

$$\phi^r : H \to (\mathbb{Z}/q\mathbb{Z})^*;\ \phi^r(h) = r \text{ for roots } r \text{ of the equation } x^p \equiv 1 \pmod q$$

Since p is prime, there is a "primitive" p-th root ρ of the equation and all other roots are of the form $r = \rho^i$ for $i = 1, ..., p$. This translates to:

$$\phi^\rho(h^i) = \rho^i = r = \phi^r(h)$$

so ϕ^r and ϕ^ρ are related by the "change of variables" $h \leftrightarrow h^i$ replacing one generator h by the other generator h^i (as long as $i \neq p$). Since the choice of generator of H was arbitrary, it follows that the semi-direct product groups are isomorphic.

Thus, there are exactly two groups of order 21 (and 55 and 57...).

The Case $|G| = 20$**.** $H = C_4$ or $C_2 \times C_2$ (and $N = C_5$), and there are five groups.

(a) Let $H = C_4$. We mimic the argument in the proof of Proposition 5 with the equation $x^4 \equiv 1 \pmod 5$, and define homomorphisms ϕ^r as above for the roots of the equation in $(\mathbb{Z}/5\mathbb{Z})^*$. But now only:

$$\phi^2(h) = 2 \text{ and } \ \phi^3(h) = 3 = \phi^2(h^3) \text{ (for a given generator } h \text{ of } C_4)$$

are related by a change of variables, since h^2 is not a generator of $H = C_4$. Thus there are three semi-direct products, giving groups:

$$C_5 \times C_4 = C_{20},\ C_5 \rtimes_{\phi^2} C_4 \text{ and } C_5 \rtimes_{\phi^4} C_4$$

Thus we get a cyclic group and two "mystery groups."

(b) If $H = C_2 \times C_2$ (the Klein group), generated by $h_1 = (h, e)$ and $h_2 = (e, h)$, then this accounts for four homomorphisms ϕ (including the trivial one) with:

$$\phi_{h_1}(g) = g \text{ or } g^{-1} \text{ and } \phi_{h_2}(g) = g \text{ or } g^{-1}$$

but as before, some of these give isomorphic semi-direct products when the given choice of generators for H are replaced by others. In fact, we are left with only two semi-direct products (up to change of variables): $\phi_{h_i}(g) = g$ (trivial product), and $\phi_{h_1}(g) = g, \phi_{h_2}(g) = g^{-1}$ resulting in $C_5 \times H = C_{10} \times C_2$ and $D_{10} \times C_2 = D_{20}$.

Remark. The first mystery group from (a) isn't all that mysterious. Letting:

$$g = (1\ 2\ 3\ 4\ 5) \text{ and } h = (2\ 3\ 5\ 4) \text{ gives us } hgh^{-1} = (1\ 3\ 5\ 2\ 4) = g^2$$

which is enough to pin down $G = C_5 \rtimes_{\phi^2} C_4$ as this very concrete subgroup of S_5. The second mystery group is a "dicyclic" group...a close cousin of the group Q_8.

The Case $|G| = 18$. Here $N = C_9$ or $C_3 \times C_3$ and $H = C_2$.

(a) If $N = C_9$, then G is either a product and C_{18} or else it is a semi-direct product and D_{18} since $\mathrm{Aut}(C_9) \cong C_6$ has a single element of order two.

(b) If $N = C_3 \times C_3$, then either G is the product, or else it is a semidirect product coming from an element of order two in $\mathrm{Aut}(C_3 \times C_3)$, and we are therefore tasked with finding elements of order two in this group and deciding when they differ by a change of variables. We'll take this up in a bit.

Let's tackle 12 and 24 "modulo semi-direct products of Sylow subgroups"

The Case $|G| = 12 = 2^2 \cdot 3 = 3 \cdot 4$. There are five groups here, too.

We claim that G has either a normal 2-Sylow subgroup N, and therefore is:

$$C_4 \rtimes C_3 \ (= C_4 \times C_3) \text{ or } (C_2 \times C_2) \rtimes C_3$$

(A_4 is in this collection) or else G has a normal 3-Sylow subgroup and is:

$$C_3 \rtimes C_4 \text{ (another dicyclic group) or } C_3 \rtimes (C_2 \times C_2)$$

(D_{12} is in this collection) and we've already seen that G is one (or both) of these.

The Case $|G| = 24 = 2^3 \cdot 3 = 3 \cdot 8$.

There **is** a group G with $|G| = 24$ and no normal Sylow subgroups. Namely,

$$G = S_4$$

with the three dihedral 2-Sylow subgroups and the eight 3-Sylow cyclic subgroups. Thus in general, we cannot assume that one of the Sylow subgroups is normal, even when G fails to be a simple group.

Automorphisms

We've seen that the automorphism group of a cyclic group is abelian. Namely:

$$\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

When $n = p$ is prime, this is a cyclic group, but what is it when n is not prime? Paralleling the computation of the Euler "totient" function:

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$$

we see that if $n = \prod {p_i}^{k_i}$ is the prime factorization of n, then:

$$C_n = \prod C_{p_i^{k_i}} \text{ and } \mathrm{Aut}(C_n) = \prod \ \mathrm{Aut}(C_{p_i^{k_i}}) = \prod (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$$

since an automorphism respects the product decomposition.

We know further that the totient function factors:

$$\phi(p^k) = p^{k-1}(p-1)$$

and then by a theorem of Gauss (deeper than anything we've done so far):

$$(\mathbb{Z}/p^k\mathbb{Z})^* = C_{\phi(p^k)} \text{ (for all powers of an odd prime)}$$

When $p = 2$, this isn't the case, since, for example:

$$(\mathbb{Z}/8\mathbb{Z})^* = C_2 \times C_2 \text{ is the Klein group}$$

Note that $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic if n has at least two odd prime factors, e.g.

$$(\mathbb{Z}/55\mathbb{Z})^* = (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^* = C_4 \times C_{10} = C_2 \times C_{20}$$

In our classifications above, we've also encountered:

$$\mathrm{Aut}(C_2 \times C_2) \text{ and } \mathrm{Aut}(C_3 \times C_3)$$

The automorphism groups of these are not even abelian groups!

Proposition 6. The automorphism groups of $(C_p)^n$ are the general linear groups:

$$\mathrm{GL}(n, \mathbb{F}_p)$$

of invertible $n \times n$ matrices with entries in the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proof. Let g generate C_p and let g_i generate the ith factor of the product C_p^n. Then a group homomorphism $f : C_p^n \to C_p^n$ is given by:

$$f(g_i) = \prod g_j^{a_{ij}} \text{ for } a_{ij} \in \mathbb{F}_p$$

and $A = (a_{ij})$ converts the group homomorphism to a matrix, with composition of homomorphisms corresponding to multiplication of matrices. Thus, in particular, the invertible matrices correspond to the automorphisms of the group C_p^n. $\square$

Extended Examples. The six elements of $\mathrm{Aut}(C_2 \times C_2) = \mathrm{GL}(2, \mathbb{F}_2)$ are:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ (the identity)}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ (order two)}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ (order three)}$$

This group is therefore isomorphic to S_3. One can use this knowledge, for example, to show that A_4 is the *only* semi-direct product of the form $(C_2 \times C_2) \rtimes C_3$ since the two elements of order three in $\mathrm{GL}(2, \mathbb{F}_2)$ are conjugate.

There are 48 elements of $\mathrm{Aut}(C_3 \times C_3) = \mathrm{GL}(2, \mathbb{F}_3)$ (see below). We can whittle this group down twice by taking the kernel of the determinant map:

$$1 \to \mathrm{SL}(2, \mathbb{F}_3) \to \mathrm{GL}(2, \mathbb{F}_3) \stackrel{det}{\to} (\mathbb{F}_3)^* = \mathrm{GL}(1, \mathbb{F}_3) \to 1$$

and then noticing that $\mathrm{SL}(2, \mathbb{F}_3)$ has a *center* equal to $\pm I_2$, giving us:

$$1 \to Z(\mathrm{SL}(2, \mathbb{F}_3)) \to \mathrm{SL}(2, \mathbb{F}_3) \to \mathrm{PSL}(2, \mathbb{F}_3) \to 1$$

where $\mathrm{PSL}(2, \mathbb{F}_3)$, the *projective special linear group*, is thought of as the matrices of determinant one modulo $\pm I_2$. There are $12 = 48/4$ elements of this group:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ (all of order two: the Klein group!)}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \text{ (two pair of order three elements)}$$

$$\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \text{ (two pair of order three elements)}$$

This is the alternating group A_4.

Proposition 7. There are:

(a) $(p^2-1)(p^2-p) = (p+1)p(p-1)^2$ elements in the group $\mathrm{GL}(2,\mathbb{F}_p)$, and

(b) $(p+1)\cdot\binom{p}{2}$ elements in the group $\mathrm{PSL}(2,\mathbb{F}_p) = \mathrm{SL}(2,\mathbb{F}_p)/\pm I_2$.

Proof. Thinking of the columns of $A \in \mathrm{GL}(2,\mathbb{F}_p)$ as vectors in $\mathbb{F}_p \times \mathbb{F}_p$, there are p^2-1 possibilities for the first column (every vector other than zero) and, given the first column, there are p^2-p possibilities for the second column (every vector not in the line spanned by the first vector is fair game). This gives (a). Then $\mathrm{SL}(2,\mathbb{F}_p)$ is the kernel of the determinant map to $\mathbb{F}_p^*$, which gives (b). $\square$

Note that the next two numbers are:

$$|\mathrm{PSL}(2,\mathbb{F}_5)| = 60 \text{ and } |\mathrm{PSL}(2,\mathbb{F}_7)| = 168$$

and these groups (and all of the groups $\mathrm{PSL}(n,\mathbb{F}_p)$ for $p \geq 5$) are simple!

Before we leave the topic of automorphisms, consider some automorphism groups of non-abelian groups. Here we have the conjugation homomorphism:

Definition. The **inner** automorphism group $\mathrm{Inn}(G)$ is the image of:

$$c : G \to \mathrm{Aut}_{\mathcal{G}r}(G);\; c_g(h) = ghg^{-1}$$

Remark. Recall that the kernel of conjugation is the center $Z(G)$.

Proposition 8. The inner automorphisms form a *normal* subgroup of $\mathrm{Aut}(G)$.

Proof. For $f \in \mathrm{Aut}(G)$ and inner automorphism $c_g \in \mathrm{Inn}(G)$,

$$(f \circ c_g \circ f^{-1})(h) = f(c_g(f^{-1}(h))) = f(gf^{-1}(h)g^{-1}) = f(g)hf(g)^{-1} = c_{f(g)}(h)$$

is another inner automorphism. $\square$

Definition. The **outer automorphisms** are the elements of the quotient group

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

Of course if G is abelian, there are no inner automorphisms and therefore the outer automorphisms carry all the information. But the situation is reversed for symmetric groups. All the automorphisms of S_n are inner (with one exception).

Proposition 9. For the symmetric groups S_n with $n \geq 3$,

(a) $Z(S_n) = \{e\}$, so $\mathrm{Inn}(S_n) = S_n$, and

(b) $\mathrm{Out}(S_n) = \{e\}$ unless $n = 6$, in which case $\mathrm{Out}(S_6) = \mathbb{Z}/2\mathbb{Z}$.

Proof. We've seen that if $f : [n] \to [n]$ is a permutation, then

$$f \circ (a_1\ a_2\ \cdots a_m) \circ f^{-1} = (f(a_1)\ f(a_2)\ \cdots\ f(a_m))$$

From this it is clear that the center is trivial when $n \geq 3$.

For (b), consider that the symmetric group is generated by transpositions, in fact by transpositions of the form: $(a_1\ a_2)$, $(a_2\ a_3), \cdots,\ (a_{n-1}\ a_n)$ for distinct a_i. If $\phi \in \mathrm{Aut}(S_n)$ takes transpositions to transpositions, then there is a *pair* of lists $a_1, ..., a_n$ and $b_1, ..., b_n$ so that $\phi(a_i\ a_{i+1}) = (b_i\ b_{i+1})$ for all i. But this determines the automorphism ϕ (since these are generators). Moreover, such an automorphism is *necessarily inner*, achieved as: $\phi = c_f$ with $f(a_i) = b_i$.

So why should an automorphism take transpositions to transpositions? Because an automorphism necessarily takes *conjugacy classes* of elements of a given order to *conjugacy classes* of elements of the same order.

Among all the symmetric groups S_n for $n \geq 3$, there is only one time that a conjugacy class of elements of order two has the same size as the conjugacy class of transpositions, namely when $n = 6$ and:

$$|(**)| = \binom{6}{2} \text{ and } |(**)(**)(**)| = \binom{6}{2} \cdot \binom{4}{2} / 3!$$

and there is indeed an outer automorphism of C_6 that exchanges them. When composed with itself, however, this unique (non-trivial) outer automorphism reverts to an inner automorphism.