Simple groups and the classification of finite groups

1 Finite groups of small order

How can we describe all finite groups? Before we address this question, let's write down a list of all the finite groups of small orders ≤ 15, up to isomorphism. We have seen almost all of these already. If G is abelian, it is easy to write down all possible G of a given order, using the Fundamental Theorem of Finite Abelian Groups: G must be isomorphic to a direct product of cyclic groups, and any isomorphism between two such direct products is a consequence of the Chinese Remainder Theorem. For example, if $\#(G) = n$ and n is a product of distinct primes then G is cyclic, and hence isomorphic to $\mathbb{Z}/n\mathbb{Z}$. The only cases where this doesn't happen for $n \leq 15$ are:

- $n = 4$ and $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
- $n = 8$ and $G \cong \mathbb{Z}/8\mathbb{Z}$, $G \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ or $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
- $n = 9$ and $G \cong \mathbb{Z}/9\mathbb{Z}$ or $G \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
- $n = 12$ and $G \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ or $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.

Note that, for $n = 16$, there are already 5 possibilities for G.

In case G is not abelian, there are many orders which can't arise. For example, if $\#(G) = p$, where p is a prime, then we have seen that G is abelian. We will show soon that, if $\#(G) = p^2$, where p is a prime, then G is abelian. Also, if $\#(G) = pq$, where p and q are distinct primes, say $p < q$, then G is abelian unless $q \equiv 1 \bmod p$, and in this case the nonabelian G can be described quite explicitly. Thus for example every group of order 15 is abelian, hence cyclic. The only possibilities then for nonabelian groups of order at most 15, up to isomorphism, are given by:

- $n = 6$ and $G \cong S_3 \cong D_3$.
- $n = 8$; $G \cong D_4$ or $G \cong Q$, the quaternion group.

- $n = 10$ and $G \cong D_5$.
- $n = 12$; $G \cong D_6$, $G \cong A_4$, or $G \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$, a certain group which we shall describe later. (Note: $S_3 \times (\mathbb{Z}/2\mathbb{Z})$ is also a nonabelian group of order 12, but in fact $S_3 \times (\mathbb{Z}/2\mathbb{Z}) \cong D_6$.)
- $n = 14$ and $G \cong D_7$.

Lest one conclude that the list seems manageable, we mention that for $n = 16$, there are already 5 non-isomorphic abelian groups of order 16 as well as 9 non-isomorphic nonabelian groups of order 16, and it is rather complicated to describe them all. In general, if n is divisible by a large power of a prime p, then it becomes very difficult to list all groups G with $\#(G) = n$ up to isomorphism.

2 Breaking up finite groups into simpler pieces

We begin with a discussion of quotient groups as a way to break a group up into simpler pieces. Suppose for simplicity that G is a finite group and that $H \triangleleft G$. If $H = \{1\}$, then $G/H \cong G$, and if $H = G$ then $G/H = \{G\}$ is the trivial group with one element. So we suppose that H is a nontrivial proper normal subgroup of G, i.e. that $H \neq \{1\}, G$. In this case $1 < \#(H) < \#(G)$, and hence $1 < \#(G/H) < \#(G)$ as well. We can think of this as saying that the subgroup H and quotient group G/H are simpler (smaller) groups and that G is somehow built out of the building blocks H and G/H.

In general, however, this process is quite complicated. For example, $\mathbb{Z}/4\mathbb{Z}$ has the nontrivial proper (normal) subgroup $\langle 2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$, and (as we have seen) the quotient group $\mathbb{Z}/4\mathbb{Z}/\langle 2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$ as well. This says that $\mathbb{Z}/4\mathbb{Z}$, the simplest group which has any proper nontrivial subgroup at all, is built out of two building blocks, each isomorphic to $\mathbb{Z}/2\mathbb{Z}$. However, if instead we look at $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, it has the subgroup $\{0\} \times \mathbb{Z}/2\mathbb{Z}$, also isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})/(\{0\} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ as well. So $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is also built up from two building blocks, each isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and there needs to be additional information in how they are put together in order to distinguish the end result $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ from $\mathbb{Z}/4\mathbb{Z}$. In general the issue of how to reconstruct G given the knowledge of H and G/H is called the *extension problem*, and it is generally agreed to be a hopeless problem as stated. If there is a subgroup K of G such that $\pi|K$ is an isomorphism, where $\pi \colon G \to G/H$ is the quotient homomorphism, then G can be described fairly concretely in terms of H and $G/H \cong K$ (as we shall see), but this situation turns out to be rather rare. In the special

case where H is an **abelian** subgroup of G, there is a mechanism (group cohomology) for listing the possibilities for G given H and the group G/H (and an extra piece of data which we shall describe later).

Let us give some more examples. For the group $G = \mathbb{Z}/6\mathbb{Z}$, we have the subgroup $H = \langle 2 \rangle \triangleleft \mathbb{Z}/6\mathbb{Z}$, with $H \cong \mathbb{Z}/3\mathbb{Z}$ and the quotient $(\mathbb{Z}/6\mathbb{Z})/\langle 2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. We could also have looked at the subgroup $\langle 3 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. In this case $\mathbb{Z}/6\mathbb{Z}/\langle 3 \rangle \cong \mathbb{Z}/3\mathbb{Z}$. Thus in this case we could have used the building blocks in either order. Working instead with S_3, there is the unique normal subgroup $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, and $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$. Here there is only one possible order. (We will also see later that there is a difference between how the building blocks for $\mathbb{Z}/6\mathbb{Z}$ or for S_3 fit together.)

For larger groups, we must continue this process. For example, for the quaternion group Q, we have the normal subgroup $\langle i \rangle$ (normal because it has index two), and the quotient group $Q/\langle i \rangle \cong \mathbb{Z}/2\mathbb{Z}$. This group can be further pulled apart as above, by looking at the subgroup $\langle -1 \rangle \leq \langle i \rangle$. Putting this together, we have a sequence

$$\{1\} \triangleleft \langle -1 \rangle \triangleleft \langle i \rangle \triangleleft Q,$$

where each subgroup is normal in the next one, and the quotients are all isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Of course, we could also have used the subgroups $\langle j \rangle$ or $\langle k \rangle$ in this picture instead of $\langle i \rangle$. Working with D_4, or $\mathbb{Z}/8\mathbb{Z}$, or $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, or $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, would give a very similar picture. For example, D_4 also has a cyclic normal subgroup of order 4, the subgroup $\langle (1234) \rangle$, and the quotient must also be isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Another example is S_4, where we could begin with the normal subgroup A_4, then use the normal subgroup H of A_4, where $H = \{1, (12)(34), (13)(24), (14)(23)\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and finally take a subgroup of H isomorphic to $\mathbb{Z}/2\mathbb{Z}$, say $K = \{1, (12)(34)\}$. The picture would then look like

$$\{1\} \triangleleft K \triangleleft H \triangleleft A_4 \triangleleft S_4,$$

with the successive quotients isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z}$.

In general, we would attempt the following strategy: begin with the group G, and look for a nontrivial proper normal subgroup $H \triangleleft G$, leading to building blocks H, G/H. Then, on the left hand side, look for a nontrivial proper normal subgroup $H' \triangleleft H$. On the right hand side, if we have found a nontrivial proper normal subgroup $J \triangleleft G/H$, then we can look at $K = \pi^{-1}(J) \triangleleft G$, where $\pi \colon G \to G/H$ is the quotient homomorphism. Note that $H \triangleleft K$ and that $K/H \cong J$ since $\pi|K \colon K \to J$ is surjective with kernel H.

The Third Isomorphism Theorem says that $G/K \cong (G/H)/J$. So the longer sequence of groups

$$\{1\} \triangleleft H \triangleleft K \triangleleft G$$

has the building blocks H, J, $G/K \cong (G/H)/K$. In general, we would consider a sequence

$$\{1\} \triangleleft G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G,$$

where each $G_i \triangleleft G_{i+1}$, but G_i is not necessarily a normal subgroup of G. If we can further pull apart the quotient G_{i+1}/G_i by finding a nontrivial proper normal subgroup $J \triangleleft (G_{i+1}/G_i)$, then the procedure outlined above tells us how to enlarge the sequence $\{G_i\}$ by adding an intermediate subgroup K with $G_i \triangleleft K \triangleleft G_{i+1}$. So we enlarge the sequence and continue. This procedure is called *refining* the sequence $\{G_i\}$. If G is finite and we only work with nontrivial proper subgroups, the orders of the G_{i+1}/G_i cannot decrease indefinitely, so this procedure must terminate.

What makes the procedure terminate? For an even more basic question, what happens when, for a given G, we can't get started at all, because G has no proper normal subgroups? For example, if p is a prime, then the group $\mathbb{Z}/p\mathbb{Z}$ has no nontrivial proper subgroups at all and hence no nontrivial proper normal subgroups. Let us make a definition:

Definition 2.1. Let G be a group (not necessarily finite), with G not the trivial group. Then G is *simple* if it has no nontrivial proper normal subgroups, i.e. G is simple if $G \neq \{1\}$ and if, for every $H \triangleleft G$, either $H = \{1\}$ or $H = G$.

For example, $\mathbb{Z}/p\mathbb{Z}$ is simple if p is prime. Optimistically, we might conjecture that, if a finite group G is simple, then conversely $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime number p. However, as we shall see, this turns out not to be the case. The discussion above says that, if G is a finite group, then we can find a sequence of subgroups G_i of G with the property that

$$\{1\} \triangleleft G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G,$$

and such that the quotient group G_{i+1}/G_i is simple for every i. Such a sequence is called a *composition series*. It is not unique, but a result called the *Jordan-Hölder theorem* says that the set of simple quotient groups G_{i+1}/G_i, together with how many times they appear, are independent of the choice of composition series.

We note that a nontrivial finite **abelian** group A is simple $\iff$ $A \cong \mathbb{Z}/p\mathbb{Z}$ for some prime number p. In fact, we have the following:

Lemma 2.2. *Let A be an abelian group (written additively), not necessarily finite. If $A \neq \{0\}$ and A is not isomorphic to $\mathbb{Z}/p\mathbb{Z}$, where p is a prime, then A has a nontrivial proper subgroup, necessarily normal.*

Proof. For an abelian group A, A has no proper nontrivial normal subgroups $\iff$ A has no proper nontrivial subgroups, since every subgroup of an abelian group is automatically normal. We have seen in the homework that this is equivalent to: $A \cong \mathbb{Z}/p\mathbb{Z}$ for some prime number p. □

Since every quotient of an abelian group is again abelian, this says that we can perform the procedure described earlier for a finite abelian group A and eventually reach a stage where there is a sequence of subgroups

$$\{0\} \lhd A_0 \lhd A_1 \lhd \cdots \lhd A_{k-1} \lhd A_k = A,$$

where A_{i+1}/A_i is a cyclic group of prime order.

In general, let G be a group, not necessarily abelian, and suppose that there exists a sequence

$$\{1\} \lhd G_0 \lhd G_1 \lhd \cdots \lhd G_{k-1} \lhd G_k = G,$$

where each $G_i \lhd G_{i+1}$ and G_{i+1}/G_i is abelian. Then applying the above results for abelian groups and by successively refining the sequence $\{G_i\}$ as described above we can in fact assume that each G_{i+1}/G_i is cyclic of prime order. In general, we make the following:

Definition 2.3. Let G be a group (not necessarily finite), with G not the trivial group. Then G is *solvable* if there exists a sequence

$$\{1\} \lhd G_0 \lhd G_1 \lhd \cdots \lhd G_{k-1} \lhd G_k = G,$$

where each $G_i \lhd G_{i+1}$ and G_{i+1}/G_i is abelian. By the above remarks, if G is finite, then G is solvable $\iff$ there exists a sequence as above such that G_{i+1}/G_i is cyclic of prime order.

(The term *solvable* comes from the theory of solving polynomial equations by radicals.)

3 Simple groups

What are the possibilities for finite simple groups other than $\mathbb{Z}/p\mathbb{Z}$? First, there is the following, which we shall prove later and which is connected with the insolvability of polynomial equations of degree 5 and higher by radicals:

Theorem 3.1. *For $n \geq 5$, the group A_n is simple.*

As outlined in the homework, this leads to the following:

Corollary 3.2. *For $n \geq 5$, if $H \triangleleft S_n$, then H is either $\{1\}$, A_n, or S_n.*

Thus, for $n \geq 5$, the group S_n has very few normal subgroups.

The theorem shows that there exists a simple group of order $n!/2$ for every $n \geq 5$, so of order 60, 360, 2520, ... It turns out that 60 is the smallest possible order of a simple group not isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and every simple group of order 60 is isomorphic to A_5. However, there are many other finite simple groups.

Example 3.3. For every prime number p, there is a group $PSL_2(\mathbb{Z}/p\mathbb{Z})$ which is simple for $p \geq 5$. Begin with $GL_2(\mathbb{Z}/p\mathbb{Z})$, the group of 2×2 matrices with coefficients in $\mathbb{Z}/p\mathbb{Z}$ and with nonzero determinant. Thus

$$GL_2(\mathbb{Z}/p\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/p\mathbb{Z}, \det A = ad - bc \neq 0 \right\}.$$

Elements of $GL_2(\mathbb{Z}/p\mathbb{Z})$ are multiplied by the usual formulas for multiplying matrices, using the operations of addition and multiplication in $\mathbb{Z}/p\mathbb{Z}$. The usual formulas for the inverse of a 2×2 matrix show that, if $\det A \neq 0$, then A has an inverse and conversely. Thus $GL_2(\mathbb{Z}/p\mathbb{Z})$ is a group, but it is not simple: By the usual properties of det, the function

$$\det \colon GL_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^*$$

is a surjective homomorphism, whose kernel by definition is the normal subgroup $SL_2(\mathbb{Z}/p\mathbb{Z})$. The group $SL_2(\mathbb{Z}/p\mathbb{Z})$ is also not simple, because it has a center $\{\pm I\}$, which as we have seen is always a normal subgroup of $SL_2(\mathbb{Z}/p\mathbb{Z})$. Set $PSL_2(\mathbb{Z}/p\mathbb{Z}) = SL_2(\mathbb{Z}/p\mathbb{Z})/\{\pm I\}$ For $p = 2$, $-I = I$ and $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, so that $PSL_2(\mathbb{Z}/2\mathbb{Z}) = SL_2(\mathbb{Z}/2\mathbb{Z}) = GL_2(\mathbb{Z}/2\mathbb{Z})$. One can show that in this case $PSL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$. For $p > 2$, it is not hard to show that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ has order $\frac{1}{2}p(p^2 - 1)$. Thus, $\#(PSL_2(\mathbb{Z}/3\mathbb{Z})) = 12$, and in fact $PSL_2(\mathbb{Z}/3\mathbb{Z}) \cong A_4$. For $p = 5$, $PSL_2(\mathbb{Z}/5\mathbb{Z})$ has order 60 and in fact it is isomorphic to A_5. But for $p = 7$, $PSL_2(\mathbb{Z}/7\mathbb{Z})$ has order 168 and hence it is not isomorphic to A_n for any n. In fact, by comparing orders, it is easy to see that, for all $p \geq 7$, $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is not isomorphic to A_n for any n. One can then show:

Theorem 3.4. *$PSL_2(\mathbb{Z}/p\mathbb{Z})$ is simple for all $p \geq 5$.*

What can one say about finite simple groups which are not cyclic? Burnside proved around 1900 that, if G is a finite simple group which is not cyclic, then $\#(G)$ is divisible by at least 3 primes. Feit and Thompson proved in 1965 that a finite simple group which is not cyclic has even order. The proof runs to over 250 pages. The complete classification of finite simple groups was felt to have been completed around 1983, and ran to several thousand pages of widely scattered journal articles, but later it was noticed that some details needed to elaborated, which ran to another thousand or so pages. This step was only completed in 2004. The answer is that, every finite simple group is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p, or to A_n for some $n \geq 5$, or to one of 16 infinite series of groups most of which in some sense are a generalization of the groups $PSL_2(\mathbb{Z}/p\mathbb{Z})$ (finite groups of Lie type and their generalizations), or to one of 26 so-called "sporadic simple groups." The largest of the sporadic simple groups was finally constructed in 1981 and is called the *Fischer-Griess monster group* (or briefly the monster), although its existence had been conjectured for some time. It has order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \sim 8 \times 10^{53},$$

and in a certain sense it contains almost all of the other sporadic simple groups within it. The monster group has very unexpected connections with number theory (modular forms) and mathematical physics (vertex operator algebras).

4 Proof that A_n is simple

Finally we prove Theorem 3.1, that A_n is simple for $n \geq 5$. We begin with the following lemma:

Lemma 4.1. *Suppose that $n \geq 5$ and that H is a normal subgroup of A_n. If H contains a 3-cycle, then $H = A_n$.*

Proof. We have seen in the homework that A_n is generated by the set of 3-cycles. So we will show that, if a normal subgroup H of A_n contains a 3-cycle, then H contains all 3-cycles and hence $H = A_n$.

Suppose that $(a, b, c) \in H$ is a 3-cycle. Let (d, e, f) be any 3-cycle. We claim that there exists a $\rho \in A_n$ such that $\rho \cdot (a, b, c) \cdot \rho^{-1} = (d, e, f)$. Since H is normal, this implies that $(d, e, f) \in H$, hence that H contains all 3-cycles and thus that $H = A_n$.

To find ρ, choose $\sigma \in S_n$ such that $\sigma(a) = d$, $\sigma(b) = e$, $\sigma(c) = f$, and σ defines some bijection from $\{1, 2, \ldots, n\} - \{a, b, c\}$ to $\{1, 2, \ldots, n\} - \{d, e, f\}$,

which is clearly possible since both sets have $n-3$ elements. Note that $\sigma \cdot (a,b,c) \cdot \sigma^{-1} = (\sigma(a), \sigma(b), \sigma(c)) = (d,e,f)$. If σ is even, we can just take $\rho = \sigma \in A_n$, and then $\rho \cdot (a,b,c) \cdot \rho^{-1} = (d,e,f)$. If σ is odd, since $n \geq 5$, we can choose two distinct elements $x, y \in \{1,2,\ldots,n\} - \{a,b,c\}$. (This is the only place where we use $n \geq 5$.) Then set $\rho = \sigma \cdot (x,y)$. Since σ is odd, ρ is even and hence $\rho \in A_n$. Also, $\rho(a) = \sigma \cdot (x,y)(a) = \sigma(a) = d$, and likewise $\rho(b) = e$, $\rho(c) = f$. Thus $\rho \cdot (a,b,c) \cdot \rho^{-1} = (\rho(a), \rho(b), \rho(c)) = (d,e,f)$ as desired. □

The next step is:

Lemma 4.2. *A_5 is simple.*

Proof. By the previous lemma, we must show that, if $H \triangleleft A_5$ and $H \neq \{1\}$, then H contains a 3-cycle. Now every element of A_5 is an even permutation in S_5 and hence is either the identity, a 3-cycle, a product of two disjoint transpositions, or a 5-cycle. Since $H \neq \{1\}$, H contains either a 3-cycle, a product of two disjoint transpositions, or a 5-cycle. If H already contains a 3-cycle, we are done. If H contains a product $(a,b)(c,d)$ of two disjoint transpositions, then there exists an $e \in \{1,2,3,4,5\}$ with $e \neq a,b,c,d$. Then $\sigma = (a,b)(d,e) \in A_5$ and

$$\sigma \cdot (a,b)(c,d) \cdot \sigma^{-1} = (a,b)(c,e) \in H$$

since H is normal. Hence $(a,b)(c,d) \cdot (a,b)(c,e) \in H$ since H is closed under multiplication. But

$$(a,b)(c,d)(a,b)(c,e) = (c,d)(c,e) = (c,e,d) \in H.$$

Hence again H contains a 3-cycle. Finally, if H contains a 5-cycle (a,b,c,d,e), let $\sigma = (a,b)(c,d) \in A_5$. Then

$$\sigma \cdot (a,b,c,d,e) \cdot \sigma^{-1} = (b,a,d,c,e) \in H,$$

and hence $(a,b,c,d,e) \cdot (b,a,d,c,e) \in H$. But $(a,b,c,d,e) \cdot (b,a,d,c,e) = (a,e,c) \in H$, so that once again H contains a 3-cycle. So in all cases H contains a 3-cycle and hence $H = A_5$. □

We now complete the proof of the simplicity of A_n. The proof is by induction on n, starting with the case $n = 5$, which is the statement of the previous lemma. Suppose inductively that $n \geq 6$ and that we have proved

that A_{n-1} is simple, and let $H \triangleleft A_n$ with $H \neq \{1\}$. Recall that we have the subgroup $H_n \leq S_n$ defined by

$$H_n = \{\sigma \in S_n : \sigma(n) = n\}.$$

Then $H_n \cong S_{n-1}$ and $H_n \cap A_n \cong A_{n-1}$ and hence is simple as well. If we can show that $H \cap (H_n \cap A_n) \neq \{1\}$, then $H \cap (H_n \cap A_n)$ is a normal subgroup of $H_n \cap A_n$, not equal to $\{1\}$, and hence it is all of $H_n \cap A_n$. In particular, H must contain a 3-cycle, hence $H = A_n$.

Since $H \subseteq A_n$, $H \cap (H_n \cap A_n) = H \cap H_n$, and it suffices to prove that this subgroup is not $\{1\}$, i.e. that there exists a $\sigma \in H$ with $\sigma \neq 1$ and $\sigma(n) = n$. Since by assumption $H \neq \{1\}$, there exists a $\sigma \in H$ with $\sigma \neq 1$. If $\sigma(n) = n$, we are done: $\sigma \in H \cap H_n$. Otherwise $\sigma(n) = i$ with $i \neq n$.

First suppose that $\sigma(i) = j$ with $j \neq n$ (note that $\sigma(i) \neq i$ since $\sigma(n) = i$). Thus when we write σ as a product of disjoint cycles, one of the cycles looks like $(n, i, j, \dots)$. Choose some $k \neq n, i, j$. The element (j, k) is odd, but since $n \geq 6$, there exist $a, b \in \{1, 2, \dots, n\}$ with a, b distinct elements not equal to n, i, j, k, and $\rho = (j, k)(a, b)$ is even. Then $\rho \cdot \sigma \cdot \rho^{-1} \in H$ since H is normal, and hence $\tau = \sigma^{-1} \cdot \rho \cdot \sigma \cdot \rho^{-1} \in H$ since H is closed under taking inverses and products. Now $\rho(n) = n$ by construction, and hence

$$\tau(n) = \sigma^{-1} \cdot \rho \cdot \sigma \cdot \rho^{-1}(n) = \sigma^{-1} \cdot \rho \cdot \sigma(n) = \sigma^{-1} \cdot \rho(i) = \sigma^{-1}(i) = n.$$

Thus $\tau \in H \cap H_n$. Finally, we claim that $\tau \neq 1$. To see this, note that

$$\tau(i) = \sigma^{-1} \cdot \rho \cdot \sigma \cdot \rho^{-1}(i) = \sigma^{-1} \cdot \rho \cdot \sigma(i) = \sigma^{-1} \cdot \rho(j) = \sigma^{-1}(k).$$

We cannot have $\sigma^{-1}(k) = i$, for otherwise $\sigma(i) = k$, but also $\sigma(i) = j \neq k$, which is impossible. Hence $\tau(i) \neq i$, so that $\tau \neq 1$.

The remaining case is where $\sigma(n) = i$ with $i \neq n$ and $\sigma(i) = n$. This case is similar in spirit to the previous case. Since σ is even, $\sigma \neq (n, i)$, and so there exists a $j \neq n, i$ with $\sigma(j) = k \neq n, i$. (Think of writing σ as a product of disjoint cycles of lengths at least two: one such looks like (n, i) and there must be another which begins $(j, k, \dots)$.) Again using $n \geq 6$, there exist ℓ, m which are distinct and not equal to any of n, i, j, k. Let $\rho = (j, \ell, m)$. Then $\rho \in A_n$ since ρ is a 3-cycle, and, setting $\tau = \sigma^{-1} \cdot \rho \cdot \sigma \cdot \rho^{-1}$, $\tau \in H$ as before. But

$$\tau(n) = \sigma^{-1} \cdot \rho \cdot \sigma \cdot \rho^{-1}(n) = \sigma^{-1} \cdot \rho \cdot \sigma(n) = \sigma^{-1} \cdot \rho(i) = \sigma^{-1}(i) = n;$$
$$\tau(\ell) = \sigma^{-1} \cdot \rho \cdot \sigma \cdot \rho^{-1}(\ell) = \sigma^{-1} \cdot \rho \cdot \sigma(j) = \sigma^{-1} \cdot \rho(k) = \sigma^{-1}(k) = j.$$

The first equation says that $\tau \in H \cap H_n$, and the second says that $\tau(\ell) = j \neq \ell$, so that $\tau \neq 1$. Hence in both cases $H \cap H_n \neq \{1\}$ and we are done. $\square$