Section 3.2

4. Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$.

Proof. (Baggett) Since $Z(G)$ is a subgroup of G, from Lagrange's Theorem we have that $|Z(G)| = 1, p, q,$ or pq. Suppose that $|Z(G)| \neq 1$. If $|Z(G)| = p$, then $|G/Z(G)| = \frac{pq}{p} = q$. Since the order of $G/Z(G)$ is prime, $G/Z(G)$ is cyclic. Similarly, if $|Z(G)| = q$, then $|G/Z(G)| = \frac{pq}{q} = p$. Since the order of $G/Z(G)$ is prime, $G/Z(G)$ is cyclic. If $|Z(G)| = pq$, then $|G/Z(G)| = \frac{pq}{pq} = 1$. Thus, $G/Z(G)$ is the trivial group and is therefore cyclic. In all three cases where $|Z(G)| \neq 1$, $G/Z(G)$ is cyclic. From Exercise 3.1.36, we can conclude that G is abelian. Thus, either G is abelian or $Z(G) = 1$. □

5. Let H be a subgroup of G and fix some element $g \in G$.

   (a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

   (b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.

Proof. (Mobley)

(A) We know that the identity is contained in gHg^{-1} and it is therefore nonempty. Pick $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$. Then $(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1}$ and the subset is closed under the operation. Next, $(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1}$ and the subset is closed under inverses. Thus, $gHg^{-1} \leq G$.

Let $\varphi : H \to gHg^{-1}$ be defined by $h \mapsto ghg^{-1}$. Pick two elements in gHg^{-1} such that $gh_1g^{-1} = gh_2g^{-1}$. Then by using cancellation laws, $h_1 = h_2$ and φ is one-to-one. Now if $ghg^{-1} \in gHg^{-1}$, then $\varphi(h) = ghg^{-1}$ and φ is surjective. Thus, H and gHg^{-1} have the same cardinality.

(B) H is the only subgroup of order n. But from the first part $|H| = |gHg^{-1}|$ for an arbitrary $g \in G$. Thus, $gHg^{-1} = H$ for all $g \in G$ and $H \trianglelefteq G$. □

8. Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

Proof. (Mobley) We will use Proposition 3 on page 55 of the text. Pick $g \in H \cap K$. Since $|H| = p$ and $|K| = q$ and $(p, q) = 1$, it follows that $g^p = 1$, $g^q = 1$ and $g^1 = 1$. Thus g must be the identity and $H \cap K = 1$. □

16. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^{\times}$ to prove *Fermat's Little Theorem:* if p is a prime then $a^p \equiv a(\text{mod} p)$ for all $a \in \mathbb{Z}$.

Proof. (Buchholz) Let $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$ and note that $|G| = p - 1$ where p is prime. Then choose $a \in G$ and let $|a| = k$. By Lagrange's Theorem $|a| \big| |G|$, so $k | p - 1$. Then $p - 1 = km$ for some $m \in \mathbb{Z}^+$, which implies that $p = km + 1$. Consider,

$$a^p = a^{km+1} = (a^k)^m a = (1^m)a \equiv a(\text{mod} p).$$

Hence $a^p \equiv a(\text{mod} p)$ for all $a \in \mathbb{Z}$.

□

22. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^{\times}$ to prove *Euler's Theorem:* $a^{\varphi(n)} \equiv 1(\text{mod})n$ for every integer a relatively prime to n, where φ denotes Euler's $\varphi-$function.

Proof. (Buchholz) Let $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$ and note that $|G| = \varphi(n)$. Then choose $a \in G$ where $(a, n) = 1$. Let $|a| = k$. By Lagrange's Theorem $|a|\big||G|$, so $k\big|\varphi(n)$. Then $\varphi(n) - 1 = km$ for some $m \in \mathbb{Z}^+$. Consider,

$$a^{\varphi(n)} = a^{km} = (a^k)^m = (1^m) \equiv 1(\text{mod} n).$$

Hence $a^{\varphi(n)} \equiv 1(\text{mod})n$ for all $a \in \mathbb{Z}$ which is relatively prime to n.

□

Section 3.3

3.3.1 LET F BE A FINITE FIELD OF ORDER q AND LET $n \in \mathbb{Z}^+$, THEN $|GL_n(F) : SL_n(F)| = q - 1$.

Proof. (Gillispie) Consider the function $\varphi : GL_n(F) \to F$ defined by

$$g \mapsto \det(g)$$

.

Note that by the properties of the determinate we know that $\varphi(e) = 1$ and if $g_1, g_2 \in GL_n(F)$, then $\det(g_1)\det(g_2) = \det(g_1g_2)$ and so φ is a group homomorphism.
Now if we let $s \in SL_n(F)$, by definition we know that $\varphi(s) = \det(s) = 1$, so $s \in Ker\varphi$ and $SL_n(F) \subset Ker\varphi$.
If we let $k \in Ker\varphi$, then we know that $1 = \varphi(k) = \det(k)$, which by definition means that $k \in SL_n(F)$, and so $SL_n(F) = Ker\varphi$.
By the first isomorphism theorem we mow have that $|GL_n(F) : SL_n(F)| = |\varphi(GL_n(F))|$.
If $g \in GL_n(F)$, then $\det(g) \in F - 0$ and so $\varphi(GL_N(F)) \subset F - \{0\}$. Now, if we let $f \in F$, I claim that the $n \times n$ matrix with all zeroes(in F) off the main diagonal, f in the upper-left hand position, and ones(in F) in every other main diagonal position has determinate f. By construction this matrix is in $GL_n(F)$, and so $F - \{0\} \subset \varphi(GL_n(F)$.
We have that $|GL_n(F) : SL_n(F)| = |\varphi(GL_n(F))| = |F - \{0\}| = q - 1$. As needed.

□

3. PROVE THAT IF H IS A NORMAL SUBGROUP OF G OF PRIME INDEX p THEN FOR ALL $K \leq G$ EITHER

i. $K \leq H$ OR
ii. $G = HK$ AND $|K : K \bigcap H| = p$.

Proof. (Hazlett) Suppose $K \not\leq H$. Then $H \subset K$. Hence we can deduce that $|G : HK| = 1$ since $|G : H| = p$, a prime. So $HK = G$. Then by the Second Isomorphism Theorem we have $HK/H \cong K/H \cap K$. Consequently $G/H \cong K/H \cap K$. Therefore $|K : K \bigcap H| = p$. □

3.3.7 LET M AND N BE NORMAL SUBGROUPS OF G S.T. $MN = G$, THEN $G/(N \cap M) \cong (G/M) \times (G/N)$.

Proof. (Gillispie) Define $\varphi : G \to G/M \times G/N$ by $g \mapsto gM, gN$.

Note that $\varphi(e_G) = e_GM, e_GN = M, N$ which is the identity in $G/M \times G/N$.

Let $g_1, g_2 \in G$. Because $G = MN$, there exist $m_1, m_2 \in M$ and $n_1, n_2 \in N$ s.t. $g_1 = m_1n_1$and $g_2 = m_2n_2$

$$\begin{aligned}
\varphi(g_1g_2) &= g_1g_2M, g_1g_2N \\
&= (g_1M, g_1N)(g_2M, g_2N) \\
&= \varphi(g_1)\varphi(g_2)
\end{aligned}$$

And so φ is a homomorphism.

Consider the kernel of φ. Let $k \in Ker\varphi$, that is $kM, kN = M, N$ by proposition 3.1.4 we have then that $k \in M$ and $k \in N$, so $k \in M \cap N$.
Now let $g \in M \cap N$, notice that $\varphi(g) = (gM, gN) = (M, N)$ again by proposition 3.1.4, and so $Ker\varphi = M \cap N$.

I claim now that φ is surjective, and thus by the first isomorphism theorem $G/M \times G/N \cong G/M \cap N$.

Let $(pM, qN) \in G/M \times G/N$, since $p, q \in G = MN$ and by proposition 3.2.6 $MN = NM$, there exist $m_1, m_2 \in M$ and $n_1, n_2 \in N$ s.t. $p = m_1n_1$ and $q = n_2m_2$. By Theorem 3.1.6

$$\begin{aligned}
\varphi(n_1m_2) &= (n_1m_2M, n_1m_2N) \\
&= (n_1M, Nn_1m_2) \\
&= (n_1m_1M, Nm_2) \\
&= (pM, Nn_2m_2) \\
&= (pM., Nq) \\
&= (pM, qN)
\end{aligned}$$

So, φ is surjective onto $G/M \times G/N$, and by the first isomorphism theorem $G/M \cap N = G/Ker\varphi \cong \varphi(G) = G/M \times G/N$. □

Section 3.4

2. Exhibit all 3 composition series for for Q_8 and all 7 composition series for D_8. List the composition factors in each case.

   (Schamel) Q_8 :

$$\begin{gathered}
\langle 1 \rangle \lhd \langle -1 \rangle \lhd \langle i \rangle \lhd Q_8 \\
\langle 1 \rangle \lhd \langle -1 \rangle \lhd \langle j \rangle \lhd Q_8 \\
\langle 1 \rangle \lhd \langle -1 \rangle \lhd \langle j \rangle \lhd Q_8
\end{gathered}$$

   D_8 :

$$\begin{gathered}
\langle 1 \rangle \lhd \langle s \rangle \lhd \left\langle s, r^2 \right\rangle \lhd D_8 \\
\langle 1 \rangle \lhd \left\langle sr^2 \right\rangle \lhd \left\langle s, r^2 \right\rangle \lhd D_8 \\
\langle 1 \rangle \lhd \left\langle r^2 \right\rangle \lhd \left\langle s, r^2 \right\rangle \lhd D_8 \\
\langle 1 \rangle \lhd \left\langle r^2 \right\rangle \lhd \langle r \rangle \lhd D_8 \\
\langle 1 \rangle \lhd \left\langle r^2 \right\rangle \lhd \left\langle sr, r^2 \right\rangle \lhd D_8 \\
\langle 1 \rangle \lhd \langle sr \rangle \lhd \left\langle sr, r^2 \right\rangle \lhd D_8 \\
\langle 1 \rangle \lhd \left\langle sr^3 \right\rangle \lhd \left\langle sr, r^2 \right\rangle \lhd D_8
\end{gathered}$$

   In both groups and all composition series, the index between sucessive terms is always 2. Thus, for both groups, each composition series has 3 composition factors, all isomorphic to C_2.

5. Prove that subgroups and quotient groups of a solvable group are solvable.

   Proof. (Bastille) Let G be a solvable group, and let $N \leq G$. Since G is solvable, there exists a chain of subgroups of G satisfying:

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

where G_{i+1}/G_i is Abelian for $i = 0, 1, \cdots, s-1$.

We will show that N is solvable by considering a chain of $G_i \cap N$. Let $i \in \{0, 1, \cdots, s-1\}$.

Since $G_i \trianglelefteq G_{i+1}$, $G_i \subseteq G_{i+1}$. Hence if $g \in G_i \cap N$ then $g \in N$ and $g \in G_i \subseteq G_{i+1}$, so $g \in G_{i+1} \cap N$. Furthermore, the intersection of two subgroups is a subgroup, hence $G_i \cap N \leq G_{i+1} \cap N$. We also note that if $g \in G_{i+1} \cap N$ and $h \in G_i \cap N$, then $ghg^{-1} \in N$ by closure under . of N (because $g, h \in N$), and $ghg^{-1} \in G_i$ since $g \in G_{i+1}, h \in G_i$ and $G_i \trianglelefteq G_{i+1}$. Thus, for all $g \in G_{i+1} \cap N$, and for all $h \in G_i \cap N$, $ghg^{-1} \in G_i \cap N$, and so $G_i \cap N \trianglelefteq G_{i+1} \cap N$.

Now we need to show that $G_{i+1} \cap N/G_i \cap N$ is Abelian. In Exercise 3.1.40, we showed that $\bar{x}, \bar{y} \in G_{i+1}/G_i$ commute if and only if $x^{-1}y^{-1}xy \in G_i$. So in particular, since G_{i+1}/G_i is indeed Abelian, if $x, y \in G_{i+1} \cap N \subseteq G_{i+1}$ then $x^{-1}y^{-1}xy \in G_i$. But since $x, y \in N$, by closure under inverses and ., $x^{-1}y^{-1}xy \in N$. Hence $x^{-1}y^{-1}xy \in G_i \cap N$. Thus by Exercise 3.1.40, $\bar{x}, \bar{y}$ commute in $G_{i+1} \cap N/G_i \cap N$ (well-defined) so $G_{i+1} \cap N/G_i \cap N$ is Abelian.

Therefore we have the following chain of subgroups (with possibly several $\{1\}$ sets on the left, and several N's on the right):

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{s-1} \trianglelefteq H_s = N$$

where $H_i = G_i \cap N$ for all $i = 0, 1, \cdots, s$ and H_{i+1}/H_i is Abelian for all $i = 0, 1, \cdots, s-1$. Therefore by definition, N is solvable.

Now for quotient groups, let H be a normal subgroup of G. If $H = G$, then trivially we have the chain $1 = 1H/H \trianglelefteq G/H = 1$ and $(G/H)/(H/H)$ is Abelian (it contains again only the trivial group), and so G/H is solvable. Now assume that $H \triangleleft G$. We will construct a chain using $(G_iH)/H$. Let $i \in \{0, 1, \cdots, s-1\}$.

By the Second Isomorphism Theorem, since $G_i \leq G = N_G(H)$, then $G_iH \leq G$, and $H \trianglelefteq G_iH$. We also have $G_iH \leq G_{i+1}H$ (since if $y = gh \in G_iH$ then $g \in G_i \subseteq G_{i+1}$ so $gh \in G_{i+1}H$). Hence we obtain the following chain:

$$H = G_0H \leq G_1H \leq G_2H \leq \cdots \leq G_{s-1}H \leq G_sH = GH = G.$$

We now show that $G_iH \trianglelefteq G_{i+1}H$. Let $y = bh_1 \in G_{i+1}H$ and let $x = ah_2 \in G_iH$. Then,

$$\begin{aligned}
yxy^{-1} &= bh_1ah_2h_1^{-1}b^{-1} = bh_1(b^{-1}b)a(b^{-1}b)h_2h_1^{-1}b^{-1} \\
&= \underbrace{(bh_1b^{-1})}_{\in H}(bab^{-1})\underbrace{(bh_2h_1^{-1}b^{-1})}_{\in H} \quad \text{since } H \trianglelefteq G \text{ and } b \in G_{i+1} \subseteq G \\
&= h_3\underbrace{bab^{-1}}_{\in G_i}h_4 \quad \text{since } G_i \trianglelefteq G_{i+1} \text{ so set } bab^{-1} = a_1 \\
&= \underbrace{h_3a_1}_{\in HG_i = G_iH} h_4 \quad \text{since they are subgroups, so } h_3a_1 = a_2h_5 \text{ for some } a_2 \in G_i, h_5 \in H \\
&= a_2h_5h_4 = a_2h_6 \in G_iH.
\end{aligned}$$

Therefore G_iH is normal in $G_{i+1}H$. Hence by the Fourth Isomorphism Theorem, we have:

$$1 = (G_0H)/H \trianglelefteq (G_1H)/H \trianglelefteq \cdots \trianglelefteq (G_{s-1}H)/H \trianglelefteq G/H.$$

We now need only show that $((G_{i+1}H)/H) / ((G_iH)/H)$ is Abelian. By the Third Isomorphism Theorem, this is equivalent to showing $(G_{i+1}H)/(G_iH)$ is Abelian since $((G_{i+1}H)/H) / ((G_iH)/H) \cong (G_{i+1}H)/(G_iH)$. We reprise a similar argument: since G_{i+1}/G_i is Abelian, for any $x, y \in G_{i+1}$, $x^{-1}y^{-1}xy \in G_i$. Now consider $(G_{i+1}H)/(G_iH)$. Let $z_1, z_2 \in G_{i+1}H$. Then there exist $x, y \in G_{i+1}$

and $h_1, h_2 \in H$ such that $z_1 = xh_1, z_2 = yh_2$. We must show that $z_1^{-1}z_2^{-1}z_1z_2 \in G_iH$. Observe that:

$$\begin{aligned} z_1^{-1}z_2^{-1}z_1z_2 &= h_1^{-1}x^{-1}h_2^{-1}y^{-1}xh_1yh_2 = h_1^{-1}x^{-1}h_2^{-1}(xx^{-1})y^{-1}x(yy^{-1})h_1yh_2 \\ &= h_1^{-1}\underbrace{((x^{-1})h_2^{-1}(x^{-1})^{-1})}_{\in H}x^{-1}y^{-1}xy\underbrace{(y^{-1}h_1(y^{-1})^{-1})}_{\in H}h_2 \quad \text{since } H \trianglelefteq G \text{ and } x^{-1}, y^{-1} \in G \\ &= h_1^{-1}h_3\underbrace{x^{-1}y^{-1}xy}_{\in G_i}h_4h_2 \quad \text{since } G_{i+1}/G_i \text{ is Abelian} \\ &= \underbrace{h_5g_1}_{\in HG_i = G_iH} h_6 = g_2h_7h_6 = g_2h_8 \in G_iH. \end{aligned}$$

Therefore $(G_{i+1}H)/(G_iH)$ is Abelian and so is $((G_{i+1}H)/H)\,/\,((G_iH)/H)$. Thus, G/H is solvable. Hence we find that subgroups and quotient groups of solvable groups are solvable. $\square$

6. Prove part (1) of the Jordan-Holder Theorem by induction on $|G|$: Every finite group G with $|G| > 1$ has a composition series.

   Proof. (Schamel) If $|G| = 2$ then $G \cong C_2$. Since 1 is normal in G and $G/1 \cong G$, which is simple, we conclude that $1 = N_1 \lhd N_2 = G$ is a composition series for G.

   Suppose $|G| = n > 2$ and that every group of strictly smaller order has a composition series. Note that $1 \lhd G$, so G has at least one normal subgroup. Let H be a proper normal subgroup of G of maximal order (that is, there is no proper normal subgroup of G of larger order). We will show that G/H is simple. To the contrary, suppose G/H is not simple. Then there is a normal subgroup $K/H \lhd G/H$ such that K/H is neither the trivial subgroup nor all of G/H. But then, by the Fourth Isomorphism Theorem, $\exists K \lhd G$ and $|G : K| = |G/H : K/H| > 1$ and hence $K \neq G$, but $H \leq K$ and $|K : H| = |K/H : 1| = |K/H| > 1$. Thus H is does not have maximal order amongst the proper normal subgroups of G, a contradiction. We conclude G/H is simple. By our induction hypothesis, H has a composition series: $1 = N_1 \lhd \cdots \lhd N_k = H$ where N_{i+1}/N_i is simple for all i. Then $1 = N_1 \lhd \cdots \lhd N_k = H \lhd G$ is a composition series for G. This inductive construction allows us to conclude that every finite group of order 2 or more has a composition series. $\square$

Section 3.5

3. Prove that S_n is generated by $\{(i \;\; i+1) \mid 1 \leq i \leq n-1\}$.

   Proof. (Baggett) Let $A = \langle\{(i \;\; i+1) \mid 1 \leq i \leq n-1\}\rangle$. Since S_n is closed under products, $A \leq S_n$. Because any permutation in S_n can be expressed as a product of transpositions, we need only show that all transpositions are generated by A. Take $(a \;\; b)$ where $1 \leq a < b \leq n$. Then
   $(b-1 \;\; b)...(a+2 \;\; a+3)[(a \;\; a+1)(a+1 \;\; a+2)(a \;\; a+1)](a+2 \;\; a+3)...(b-1 \;\; b)$
   $= (b-1 \;\; b)...(a+2 \;\; a+3)(a \;\; a+2)(a+2 \;\; a+3)...(b-1 \;\; b)$
   $= (b-1 \;\; b)...(a \;\; a+3)...(b-1 \;\; b)$
   .
   .
   .
   $= (a \;\; b)$.
   Thus, $(a \;\; b) \in A$ for any transposition $(a \;\; b)$. Therefore, $A = S_n$. $\square$

4. Show that $S_n = \langle (1\,2), (1\,2\,3\ldots n)\rangle$ for all $n \geq 2$.

Proof. (Lawless) We have just shown that S_n is generated by the set of transpositions of the form $(i \quad i{+}1)$. We will show we can generate these elements as products of elements from $\{(1\,2), (1\,2\,3\ldots n)\}$.

Pick an arbitrary i with $1 \leq i \leq n-1$. Then $(1\,2\,\ldots\,n)^{n-i+1}$ gives us:

$$\begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ n-i+2 & n-i+3 & \cdots & 1 & 2 & \cdots & n-i+1 \end{pmatrix}$$

Composing this with $(1\,2)$ to this gives us:

$$\begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ n-i+2 & n-i+3 & \cdots & 2 & 1 & \cdots & n-i+1 \end{pmatrix}$$

Finally, composing this with $(1\,2\,\cdots\,n)^{i-1}$ gives us:

$$\begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ 1 & 2 & \cdots & i+1 & i & \cdots & n \end{pmatrix}$$

Therefore, $(i \quad i+1) = (1\,2\,\cdots\,n)^{i-1}(1\,2)(1\,2\,\cdots\,n)^{n-i+1}$. Thus $S_n = \langle (1\,2), (1\,2\,3\ldots n)\rangle$.

□

6. Show that $\langle (13), (1234)\rangle$ is a proper subgroup of S_4. What is the isomorphism type of this group?

Proof (Granade). Recall that $D_8 = \left\langle r, s | r^4 = s^2 = 1, rs = sr^{-1}\right\rangle$. If we show that these relations hold for $s = (13)$ and $r = (1234)$, then we will have that $\langle (13), (1234)\rangle \cong D_8$. Then, since $|D_8| = 8 < 4!$, we will have that $\langle (13), (1234)\rangle$ is a proper subgroup of S_4. Following this plan, note that $|(13)| = 2$ and $|(1234)| = 4$. Then, $(13)(1234) = (12)(34)$, while $(4321)(13) = (12)(34)$. Thus, all three relations hold, and we are done. □

10. Find a composition series for A_4. Deduce that A_4 is solvable.

Proof (Granade). We claim that the following is a composition series for A_4:

$$\{1\} \leq \langle (12)(34)\rangle \leq K_4 \leq A_4$$

To show this, we must demonstrate that $\langle (12)(34)\rangle \lhd K_4$, $K_4 \lhd A_4$, and that $K_4 / \langle (12)(34)\rangle$ and A_4/K_4 are simple.

Note that $K_4 = \{(12)(34), (13)(24), (14)(23), (1)\} \subseteq A_4$. Then, since K_4 is a group, $K_4 \leq A_4$. Moreover, since conjugation in S_4 (and hence $A_4 \leq S_4$) preserves cycle decomposition structure, and since K_4 contains all elements of A_4 that are the product of two disjoint transpositions, we have that $\sigma K_4 \sigma^{-1} = K_4$ and thus that $K_4 \lhd A_4$. To see that A_4/K_4 is simple, note that $|A_4/K_4| = [A_4 : K_4] = |A_4| / |K_4| = 12/4 = 3$. But then, since 3 is prime, $A_4/K_4 \cong C_3$, which is simple.

Next, note that since K_4 is Abelian, all subgroups are also normal. In particular, $\langle (12)(34)\rangle \lhd K_4$. To see that $K_4/\langle (12)(34)\rangle$ is simple, note that $|K_4/\langle (12)(34)\rangle| = |K_4| / |\langle (12)(34)\rangle| = |K_4| / |(12)(34)| = 4/\mathrm{lcm}(2,2) = 4/2 = 2$. Thus, $K_4/\langle (12)(34)\rangle \cong C_2$, which is simple.

We have therefore shown that each subgroup inclusion is normal, and that each factor is simple. We conclude that the given series is in fact a composition series for A_4. □

Note that the proof also gives that A_4 is solvable, since $A_4/K_4 \cong C_3$, $\langle (12)(34)\rangle$ are both isomorphic to cyclic groups, which are Abelian.

15. Prove that if x and y are distinct 3-cycles in S_4 with $x \neq y^{-1}$, then the subgroup of S_4 generated by x and y is A_4.

Proof. (Bastille) Note that $H := \langle x \rangle = \{1, x, x^{-1}\}$ and $K := \langle y \rangle = \{1, y, y^{-1}\}$. We verify that any finite product of x, y and their powers will give an even permutation since x and y are both even, so $\langle x, y \rangle \leq A_4$. We have by assumption $x \neq y, y^{-1}$ hence $x^{-1} \neq y^{-1}, y$. Therefore $H \cap K = 1$. Hence we have:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 9.$$

But by definition, $HK \subseteq \langle x, y \rangle$. Hence $9 \leq |\langle x, y \rangle| \leq |A_4| = 12$. By Lagrange's Theorem, we must have $|\langle x, y \rangle| \,\Big|\, A_4$. Hence $|\langle x, y \rangle| = 12$ and $\langle x, y \rangle = A_4$. $\square$