Chapter 6 Further Topics in Group Theory

6.1 p-groups, Nilpotent Groups, and Solvable Groups

6.1.1

Characteristicity of the Central Upper Series (6.1.1)

Dummit and Foote *Abstract Algebra*, section 6.1, exercise 1:

Prove $Z_i(G)$ char G for all i.

Proof: Lemma 1: $Z(G)$ char G for any group G. Proof: For any $x, y \in G$, $\varphi \in Aut(G)$ we have:

$$\varphi(x) \in Z(G) \Leftrightarrow \varphi(x)\varphi(y) = \varphi(x)\varphi(y)$$

$$\Leftrightarrow \varphi(xy) = \varphi(yx) \Leftrightarrow xy = yx \Leftrightarrow x \in Z(G) \quad \square$$

Lemma 2: For K char G and $\varphi \in Aut(G)$ and letting the bar notation denote passage into G/K, we have $\psi \in Aut(\bar{G})$ where $\psi : \bar{x} \mapsto \overline{\varphi(x)}$. Proof:
Well-defined:
$\bar{x} = \bar{y} \Rightarrow y^{-1}x \in K \Rightarrow \varphi(y^{-1}x) \in K \Rightarrow \overline{\varphi(x)} = \overline{\varphi(y)} \Rightarrow \psi(\bar{x}) = \psi(\bar{y})$.
Homomorphic: $\psi(\overline{xy}) = \overline{\varphi(xy)} = \varphi(x)\varphi(y) = \overline{\varphi(x)}\,\overline{\varphi(y)} = \psi(\bar{x})\psi(\bar{y})$.
Injective:

$$\psi(\bar{x}) = \psi(\bar{y}) \Rightarrow \overline{\varphi(x)} = \overline{\varphi(y)} \Rightarrow \overline{\varphi(y^{-1}x)} = 1$$

$$\Rightarrow \varphi(y^{-1}x) \in K \Rightarrow y^{-1}x \in K \Rightarrow \bar{x} = \bar{y}$$

.
Surjective: For any $\bar{x}$, let y be the preimage of x by φ. By way of construction, $\psi(\bar{y}) = \bar{x}$.$\square$

Returning to the main result, we shall proceed by induction. Clearly $Z_0(G)$ char G, so apply the inductive hypothesis on i. Let the overbar denote passage into G/Z_{i-1}. Since $\overline{Z_i(G)} = Z(\overline{G})$, by lemma 1 we have $\overline{Z_i(G)}$ char $\overline{G}$. Let φ be any automorphism of G, and let ψ be the automorphism of $\overline{G}$ afforded by φ. Complete the proof:
$x \in Z_i(G) \Leftrightarrow \bar{x} \in \overline{Z_i(G)} \Leftrightarrow \psi(\bar{x}) \in \overline{Z_i(G)} \Leftrightarrow \overline{\varphi(x)} \in \overline{Z_i(G)} \Leftrightarrow \varphi(x) \in Z_i(G)$
. $\square$

6.1.2

Normal Subgroups and Center of a Nilpotent Group (6.1.2a)

Dummit and Foote *Abstract Algebra*, section 6.1, exercise 2a:

Let G be finite and nilpotent, and $1 < H \trianglelefteq G$. Prove $H \cap Z(G) \neq 1$.

Proof: Let $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.

By theorem 3(4), we have $G \cong P_1 \times \dots \times P_r$. Associate H under this isomorphism, and for some nontrivial element in H choose a coordinate (the i^{th}) in which a nontrivial element resides; call the associated Sylow p_i-subgroup P_i. Due to the way by which direct products work, for any $x \in A$ we are able to identify some element in H with x in the i^{th} coordinate (*), where A is the group generated by the i^{th} coordinates of the elements of H. Since $H \trianglelefteq G$, we must have $A \trianglelefteq P_i$, since an arbitrary element of P_i associated within G may be used to conjugate the elements of H; if one of these conjugations results in an element in the i^{th} coordinate not contained in A, then since H is normal, this has contradicted the construction of A. Therefore, by theorem 1, choose a nontrivial element of $A \cap Z(P_i)$ and associate it with an element in H (*), and raise this to the power of $|G|/p_i^{\alpha_i}$. This returns an element of H that has the identity in every coordinate besides the i^{th}, and in the i^{th} an element within $Z(P_i)$ that is nontrivial by Lagrange. Therefore, this nontrivial element is within $Z(G) \cong Z(P_1) \times \dots \times Z(P_r)$ by 5.1.1. □

6.1.3

6.1.3. If G is finite prove that G is nilpotent if and only if it has a normal subgroup of each order dividing $|G|$, and is cyclic if and only if it has a unique subgroup of each order dividing $|G|$.

Proof. Suppose G is nilpotent so theorem 3 states $G \cong P_1 \times \cdots \times P_s$ for $P_i \in Syl_{p_i}$. But if $n \mid |G|$, then $n = p_1^{k_1} \cdots p_s^{k_s}$. Theorem 1 states each P_i has a normal subgroup, P_i', with order $p_i^{k_i}$. Thus $|P_1' \times \cdots \times P_s'| = n$ with the desired normality property.

Now suppose G has a normal subgroup of each order dividing $|G|$. Then each Sylow subgroup is normal in G, so theorem 3 states G is nilpotent.

If G is cyclic, then theorem 2.7 states it has a unique subgroup of each order dividing $|G|$.

If G has a unique subgroup of each order dividing $|G|$, then proposition 5 shows G is cyclic. □

3. Let $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, and $P_i \in \mathrm{Syl}_{p_i}(G)$.

Assume that G is nilpotent. Then $G = P_1 \times \cdots \times P_r$. If $d \mid |G|$, then $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$, with $0 \leq \beta_i \leq \alpha_i$. Since P_i is a p_i-group, there exists $Q_i \triangleleft P_i$ with $|Q_i| = p_i^{\beta_i}$. Since $P_i \triangleleft G$, and is a Sylow subgroup, we have in fact that $P_i \operatorname{char} G$, and hence $Q_i \triangleleft G$.

Thus, $Q_1 \times \cdots \times Q_r$ is a normal subgroup of G of order d.

Conversely, assume that for all $d \mid |G|$, there is a normal subgroup of order d. Taking $d = p_i^{\alpha_i}$, we get that all Sylow subgroups of G are normal, and hence G is nilpotent.

We already know that if G is cyclic, then there is exactly one subgroup of order d for each divisor of $|G|$.

So, assume now that there is exactly one subgroup of order d for each divisor of $|G|$. So, P_i is the unique subgroup of order $p_i^{\alpha_i}$, and hence $P_i \triangleleft G$ and G is nilpotent. So, it suffices now to show that P_i is cyclic.

Since G has a unique group of order p_i, then so does P_i. By Problem 5.5.20, P_i must be cyclic.

[Note that we could also use Proposition 5 here, if you don't want to quote a previous problem.]

6.1.4

6.1.4. Prove that a maximal subgroup of a finite nilpotent group has prime index.

Proof. Let $M < G$ be a maximal subgroup of G. Since G is nilpotent, $M \triangleleft G$. Since G/M is nilpotent, exercise 6.1.3 shows it has a normal subgroup of each order dividing $|G/M|$. If $\overline{P} \trianglelefteq G/M$ with $\left|\overline{P}\right| = p$ for p prime, then $M \leq P \leq G$ so $P = G$ by maximality of M. Therefore $[G : M] = p$. □

(5) Prove that a maximal subgroup of a [finite] nilpotent group has prime index.

Let M be a maximal subgroup of a finite nilpotent group G. Since G is a finite nilpotent group, every proper subgroup of G is a proper subgroup of its normalizer. This is by Theorem 3 in section 6.1 of Dummit and Foote. Thus M is a proper subgroup of $N_G(M)$. Since M is maximal, the only subgroup that properly contains it is G itself, so it must be that $N_G(M) = G$ and M is normal. Thus we have a quotient group G/M, of order equal to the index of M. If $[G : M]$ is not prime, then G/M has a nontrivial proper subgroup by, for instance, Cauchy's Theorem. By the Fourth Isomorphism Theorem, that subgroup of G/M is A/M for some subgroup A strictly between M and G, which contradicts the maximality of M. Therefore $[G : M]$ is prime.

The problem set didn't state that G must be finite, but Dummit and Foote state the problem with the additional hypothesis that the nilpotent group is finite. I have yet to think of a counterexample, but I suspect that this hypothesis is necessary. A maximal subgroup of an infinite group might not necessarily even have FINITE index, let alone a prime number.

4. Let M be a maximal subgroup of G. By Proposition 7, we have that $M \triangleleft G$, and hence we can consider $\bar{G} = G/M$.

Let p be a prime divisor of $|G/M|$ [which exists since $M \neq G$]. Then there exists an element $\bar{x} \in \bar{G}$ of order p, and hence $\bar{H} \stackrel{\text{def}}{=} \langle \bar{x} \rangle$ is such that $1 < \bar{H} \leq \bar{G}$, and $\left|\bar{H}\right| = p$. By correspondence, there exists $H \leq G$ such that $M < H \leq G$, and since M is maximal, we have that $H = G$. Therefore, $\bar{G} = \bar{H}$, and $p = \left|\bar{G}\right| = |G : H|$.

6.1.5

6.1.6

(4) Show that if $G/Z(G)$ is nilpotent then G is nilpotent

Suppose that the quotient group $Q = G/Z(G)$ is nilpotent of class c. We show that G is nilpotent of class $c+1$ using the upper central series. First, we prove by induction that $Z_i(Q) = Z_{i+1}(G)/Z(G)$. The case $i = 0$ is true by virtue of $Z_0(Q) = \{1\} = Z(G)/Z(G) = Z_1(G)/Z(G)$ since $Z_1(G) = Z(G)$ by definition. The case $i = 1$ says that $Z(Q) = Z_2(G)/Z(G)$, which means $Z(G/Z(G)) = Z_2/Z_1(G)$. The latter is true because, by definition, $Z_2(G)$ is the subgroup of G such that $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) = Z(G/Z(G))$.

Now suppose, as an induction hypothesis, that $Z_i(Q) = Z_{i+1}(G)/Z(G)$. We have to show that $Z_{i+1}(Q) = Z_{i+2}(G)/Z(G)$. By definition, $Z_{i+1}(Q)$ is the subgroup of Q such that $Z_{i+1}(Q)/Z_i(Q) = Z(Q/Z_i(Q))$. Now we calculate that,

$$\begin{aligned}
[Z_{i+2}(G)/Z(G)]/Z_i(Q) &= [Z_{i+2}(G)/Z(G)]/[Z_{i+1}(G)/Z(G)] \\
&\cong Z_{i+2}(G)/Z_{i+1}(G) \\
&= Z(G/Z_{i+1}(G)) \\
&\cong Z([G/Z(G)]/[Z_{i+1}(G)/Z(G)]) \\
&= Z(Q/Z_i(Q))
\end{aligned}$$

where we have used the induction hypothesis on the first line, applied the Third Isomorphism Theorem to cancel the $Z(G)$ terms going from the first line to the second line, noted the defining property of $Z_{i+2}(G)$ in passing from the second to the third line, applied the Third Isomorphism Theorem again to reintroduce the $Z(G)$ terms in the fourth line, and finally used the induction hypothesis again. Since we applied the Third Isomorphism Theorem in one direction and then again in the reverse direction, we actually have equality between the first and last terms in this sequence of manipulations. We have verified that $Z_{i+2}(G)/Z(G)$ satisfies the defining property of $Z_{i+1}(Q)$, so as required, $Z_{i+1}(Q) = Z_{i+2}(G)/Z(G)$. The induction is complete.

Since Q is nilpotent of class c, $G/Z(G) = Q = Z_c(Q) = Z_{c+1}(G)/Z(G)$, so $G = Z_{c+1}(G)$ and G is nilpotent of class at most $c+1$. Its nilpotence class is in fact exactly $c+1$. Indeed, if $Z_i(G) = G$, then $Z_{i-1}(Q) = Z_i(G)/Z(G) = G/Z(G) = Q$, but since c is the smallest index i such that $Z_i(Q) = Q$, $c \leq i-1$, so $i \geq c+1$.

Another strategy is to use the lower central series. $Q = G/Z(G)$ is nilpotent, so for some c, $Q^c = \{1\}$, which means that any "iterated commutator" of $c+1$ elements $g_1Z(G)$, ..., $g_{c+1}Z(G)$ is the identity $Z(G)$ in the quotient group. Equivalently, the iterated commutator of the elements $g_1, \ldots, g_{c+1}$ in G be some element $z \in Z(G)$. Here, by iterated commutator, I have in mind something like this (if $c+1 = 4$): $[[[g_1, g_2], g_3], g_4]$. The $c+1$, rather than c, is because we need TWO elements to take one commutator, so three elements to take commutators twice as in $[[g_1, g_2], g_3]$, and so on. Anyway, that c-tuple commutator works out to some element z in the center, so if we take the commutator of z with one more element $g_{c+2} \in G$, since z commutes with everything, we get $[z, g_{c+2}] = 1$. Thus the iterated commutator of any $c+2$ elements of G is trivial, which means that the lower central series of G will eventually reach $\{1\}$. More precisely, $G^{c+1} = \{1\}$, so G is nilpotent of class $c+1$.

Dummit and Foote *Abstract Algebra*, section 6.1, exercise 6:

If $G/Z(G)$ is nilpotent, prove G is nilpotent.

Proof: Lemma 1: For φ an isomorphism, we have $\varphi(Z(G)) = Z(\varphi(G))$. Proof: For any $x, y \in G$, we observe

$$\varphi(x) \in \varphi(Z(G)) \Leftrightarrow x \in Z(G) \Leftrightarrow xy = yx \Leftrightarrow \varphi(xy) = \varphi(yx) \Leftrightarrow$$
$$\varphi(x)\varphi(y) = \varphi(y)\varphi(x) \Leftrightarrow \varphi(x) \in Z(\varphi(G)) \quad \square$$

Now, let the overbar denote passage into $G/Z(G)$.

Inductively prove that $Z_n(\overline{G}) = \overline{Z_{n+1}(G)}$ for all nonnegative n. When $n = 0$, we have $Z_0(\overline{G}) = Z(G)/Z(G) = Z_1(G)/Z(G) = \overline{Z_1(G)}$, so now validate the inductive step: Let $\varphi : G/Z_n(G) \to \overline{G}/\overline{Z_n(G)}$ be an isomorphism by $\varphi(gZ_n(G)) = \bar{g}\overline{Z_n(G)}$ (the inverse of the natural isomorphism by the Third Isomorphism Theorem), and we have:
$Z_n(\overline{G})/\overline{Z_{n-1}(G)} = Z(\overline{G}/\overline{Z_{n-1}(G)}) \Rightarrow$
$Z_n(\overline{G})/\overline{Z_n(G)} = Z(\overline{G}/\overline{Z_n(G)}) \Rightarrow$
$Z_n(\overline{G})/\overline{Z_n(G)} = Z(\varphi(G/Z_n(G))) \Rightarrow$
$Z_n(\overline{G})/\overline{Z_n(G)} = \varphi(Z(G/Z_n(G))) \Rightarrow$
$Z_n(\overline{G})/\overline{Z_n(G)} = \varphi(Z_{n+1}(G)/Z_n(G)) \Rightarrow$
$Z_n(\overline{G})/\overline{Z_n(G)} = \overline{Z_{n+1}(G)}/\overline{Z_n(G)}$.
Since $Z_{n+1}(G)$ contains $Z_n(G)$ contains $Z(G)$, we have $\overline{Z_{n+1}(G)}$ contains $\overline{Z_n(G)}$. Further, $Z_n(\overline{G})$ contains $\overline{Z_n(G)} = Z_{n-1}(\overline{G})$. The Lattice Isomorphism Theorem describes a bijection between the subgroups of a parent group containing the normal subgroup and the subgroups of the quotient group, so we are left with $Z_n(\overline{G}) = \overline{Z_{n+1}(G)}$.

Now, set $n = m$ where $Z_m(\overline{G}) = \overline{G}$ and we have $Z_m(\overline{G}) = \overline{Z_{m+1}(G)} = \overline{G}$, so similarly as above $Z_{m+1}(G) = G$, therefore G is nilpotent (and $\overline{Z_m(G)} = Z_{m-1}(\overline{G}) \neq \overline{G}$ so $Z_m(G) \neq G$, therefore G is of class $m+1$ when G is nontrivial). $\square$

6.1.7

§6.1 #7: *Subgroups and quotient groups of nilpotent groups are nilpotent.*

Proof. Let G be a nilpotent group and let H be a subgroup of G. We first show $H^i \leqslant G^i$ for all i. Since $H^0 = H \leqslant G = G^0$, this holds for $i = 0$. If $H^i \leqslant G^i$ for some i, then

$$H^{i+1} = [H^i, H] \leqslant [G^i, G] = G^{i+1},$$

and so the result follows for all i by induction. Since G is nilpotent, $G^n = \langle 1 \rangle$ for some n and $H^n \leqslant G^n$. Hence $H^n = \langle 1 \rangle$, and so H is nilpotent.

Now let $N \trianglelefteq G$ and let $\pi : G \to G/N$ be the canonical homomorphism. By Problem #I above, $(G/N)^i = \pi(G)^i = \pi(G^i)$ for all i. Again, since G is nilpotent, $G^n = \langle 1 \rangle$, and so

$$(G/N)^n = \pi(G^n) = \pi(\langle 1 \rangle) = \langle 1N \rangle = \langle 1_{G/N} \rangle.$$

Hence G/N is nilpotent. □

7. Let $H \leq G$. We will prove that $Z_i(G) \cap H \leq Z_i(H)$, by induction on i. It is trivial for $i = 0$, so assume that $Z_{i-1}(G) \cap H \leq Z_{i-1}(H)$, and let $x \in Z_i(G) \cap H$. Then, for all $g \in G$, $gxg^{-1}x^{-1} \in Z_{i-1}(G)$ [since $Z_i(G)/Z_{i-1}(G)$ is the center of $G/Z_{i-1}(G)$, and hence commutative]. In particular, for all $h \in H$, we have $hxh^{-1}x^{-1} \in Z_{i-1}(G) \cap H \leq Z_{i-1}(H)$ [since $x \in H$]. Thus, $x \in Z_i(H)$ [since $xZ_{i-1}(H) \in Z(H/Z_{i-1}(H)) = Z_i(H)$].

Since G is nilpotent, there is c such that $Z_c(G) = G$, and therefore, $H = G \cap H = Z_c(G) \cap H \leq Z_c(H) \leq H$. Therefore $Z_c(H) = H$ [and so the nilpotency class of H is less than or equal to the nilpotency class of G].

Assume now that $H \triangleleft G$ and let $\pi : G \to \bar{G} \stackrel{\text{def}}{=} G/H$. We will prove that $\pi(Z_i(G)) \leq Z_i(\bar{G})$ by induction on i. The case $i = 0$ is again trivial, so assume that $\pi(Z_{i-1}(G)) \leq Z_{i-1}(\bar{G})$, and let $x \in Z_i(G)$. Then, $xgx^{-1}g^{-1} \in Z_i(G)$ for all $g \in G$. Thus $\pi(xgx^{-1}g^{-1}) = \pi(x)\pi(g)\pi(x)^{-1}\pi(g) \in \pi(Z_{i-1}(G)) \leq Z_{i-1}(\bar{G})$. Since π is onto, this means that $\pi(x) \in Z_i(\bar{G})$, and hence $\pi(Z_i(G)) \leq Z_i(\bar{G})$.

Since $\bar{G} = \pi(G) = \pi(Z_c(G)) \leq Z_c(\bar{G}) \leq \bar{G}$, we have that $Z_c(\bar{G}) = \bar{G}$ [and so the nilpotency class of G/H is less than or equal to the nilpotency class of G].

Let $G = D_6 = \langle r, s \rangle$, and $H = \langle r \rangle$. Then $|G : H| = 2$ and hence $H \triangleleft G$. We have that both H and G/H are abelian [in fact cyclic of prime order], and therefore nilpotent. On the other hand, $Z(D_6) = 1$, and so D_6 is not nilpotent.

6.1.8

6.1.8. Prove that if p is a prime and P is a non-abelian group of order p^3 then $|Z(P)| = p$ and $P/Z(P) \cong Z_p \times Z_p$.

Proof. Since $|P| = p^3$ we know P is nilpotent. Since P is a p-group $Z(P) \neq 1$, since P is non-abelian, $Z(P) \neq P$. Thus $|Z(P)| \in \{p, p^2\}$. If $|Z(P)| = p^2$, then $P/Z(P)$ is cyclic contradicting P being non-abelian. Thus $|Z(P)| = p$. Since $P/Z(P)$ is not cyclic, we must have $P/Z(P) \cong Z_p \times Z_p$. □

6.1.9

9. Let $a, b \in G$, with $(|a|, |b|) = 1$. Thus, $|a| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, and $|b| = q_1^{\beta_1} \cdots q_s^{\beta_s}$, with $p_i \neq q_j$ for all i and j.

Since G is nilpotent, we have that

$$G = P_1 \times \cdots \times P_r \times Q_1 \times \cdots \times Q_s \times R, \tag{3}$$

where $P_i \in \mathrm{Syl}_{p_i}(G)$, $Q_j \in \mathrm{Syl}_{q_j}(G)$, and R is the direct product of all Sylow subgroups for primes different from the p_i's and q_j's.

Let $H \stackrel{\text{def}}{=} \langle a \rangle$. Then $H \leq G$, and it is solvable [by Problem 7]. Thus, $H = \tilde{P}_1 \times \cdots \times \tilde{P}_r$, where $\tilde{P}_i \in \mathrm{Syl}_{p_i}(H)$. So, since $P_i \lhd G$, we have that $\tilde{P}_i = P_i \cap H \leq P_i$. Thus, $a \in P_1 \times \cdots \times P_r$.

In the same way, one sees that $b \in Q_1 \times \cdots \times Q_s$. But then, by (3), a and b commute.

Conversely, assume that for all $a, b \in G$ [with $|G| < \infty$] such that $(|a|, |b|) = 1$, we have that $ab = ba$. Let $p_1, \cdots, p_k$ be the prime divisors of $|G|$ and $P_i \in \mathrm{Syl}_{p_i}(G)$.

We claim that $G = P_1 \cdots P_k$. Indeed, since for all $x \in P_1$ and $y \in P_2$, we have $yxy^{-1} = x$ [since the orders are relatively prime], and so $P_2 \leq C_G(P_1) \leq N_G(P_2)$ and $P_1 P_2 \leq G$. In the same way, we can prove that $P_3 \in N_G(P_1 P_2)$ [since $|P_1 P_2| = p_1 p_2$ is relatively prime to p_3], and hence $P_1 P_2 P_3 \leq G$, and continue inductively to obtain that $P_1 \cdots P_k \leq G$. But, since they must have the same order, we must have equality.

But then each P_i is normal, since for all $x \in G$, we have that $x = x_1 x_2$, where $x_2 \in P_i$ and $x_1 \in P_1 \cdots P_{i-1} P_{i+1} \cdots P_k$. Since $|x_1|$ is relatively prime to p_i, we have that $x_1 \in C_G(P_i) \leq N_G(P_i)$, and hence $x P_i x^{-1} = x_1 x_2 P x_2^{-1} x_1^{-1} = x_1 P_i x_i^{-1} = P_i$.

Thus, every Sylow subgroup is normal, and hence G is nilpotent.

6.1.10

10. Suppose that $p \mid n$, where p is an odd prime. Let $x = r^{n/p}$. Then $|x| = p$. Also, $xs = r^{n/p}s = sr^{-n/p} = sx^{-1}$. But, if $x = x^{-1}$, then $2 \mid |x| = p$, which cannot happen. Thus, $xs \neq sx$, and $(|s|, |x|) = (2, p) = 1$. So, D_{2n} is not nilpotent in this case.

If $n = 2^k$, then $|D_{2n}| = 2^{k+1}$. Thus, D_{2n} is a 2-group, and hence nilpotent.

6.1.11

6.1.12

6.1.12. Find the upper and lower central series for A_4 and S_4.

Solution. The upper central series of A_4 is $Z_i(A_4) = 1$ and of S_4 is $Z_i(S_4) = 1$ for all i since the center of S_4 is trivial.

Since $s^{-1}a^{-1}sa$ is an even permutation, $S_4^1 \leq A_4$. But if $\alpha \in A_4$, we can choose $s \in S_4$ such that $s^{-1}a^{-1}s = \alpha a$ so that $\alpha \in S_4^1$. The same argument shows $S_4^2 = A_4$. Since $S_4^1 = A_4$ and $S_4^2 = A_4$, we have found the lower central series for S_4.

Now $N = \{1, (12)(34), (13)(24), (14)(23)\}$ is the only proper normal subgroup of A_4. Thus $A_4^i = N$ for all i so this is the lower central series for A_4. □

29 (10 points) Dummit-Foote, 6.1 #12

Let $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$. Then $K \triangleleft S_4$ and hence $K \triangleleft A_4$. Let $H = \{\mathrm{id}, (123), (132)\} \simeq C_3$. We have $A_4 = K \rtimes H$. We can check that conjugating by any hk is never a trivial automorphism of A_4, hence $Z(A_4) = \{\mathrm{id}\}$. We already know that $Z(S_4) = \{\mathrm{id}\}$. Thus:

$$\text{the upper central series of both } S_4 \text{ and } A_4 \text{ is :} \qquad \{\mathrm{id}\} \leq \{\mathrm{id}\} \leq \{\mathrm{id}\} \leq \cdots$$

Since $K \triangleleft A_4$, we have $[A_4 : A_4] \leq K$. Now, let $h = (123)$ and let $k_1 = (12)(34)$, $k_2 = (13)(24)$ and $k_3 = (14)(23)$. We can check that $[h : k_i] = k_{i+1}$.
Thus $[H : K] = K$ and, using $K \geq [A_4 : A_4] \geq [A_4 : K] \geq [H : K] = K$, we conclude that the

$$\text{lower central series of } \ A_4 \text{ is :} \qquad A_4 \geq K \geq K \geq \cdots$$

Let $L = \{\mathrm{id}, (12)\} < S_4$, then $S_4 = A_4 \rtimes L$. Since $A_4 \triangleleft S_4$ we have $A_4 \geq [S_4 : A_4] \geq [A_4 : A_4] = K$. Thus we know that $[S_4 : A_4]$ is either K or A_4. The calculation $[(12) : (123)] = (123)$ shows $[S_4 : A_4] = A_4$. Moreover, for any pair of groups $H \leq G$: G/H is an abelian group $\Leftrightarrow H \geq [G : G]$. (Aside: A subgroup of G which contains $[G : G]$ is always normal). In the present case this shows $[S_4 : S_4] \leq A_4$. Therefore $A_4 \geq [S_4 : S_4] \geq [S_4 : A_4] = A_4$ and thus the

$$\text{lower central series of } \ S_4 \text{ is :} \qquad S_4 \geq A_4 \geq A_4 \geq A_4 \geq \cdots$$

12. We have that $Z(A_4) = Z(S_4) = 1$, and hence both have trivial upper central series.

Since S_4/A_4 is abelian [since the order is 2], we have that $S_4' \leq A_4$. The only normal subgroup of A_4 different from 1 and A_4 is $K \stackrel{\text{def}}{=} \langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle \cong V_4$ [and it is also normal in S_4]. Since S_4 is not commutative, we then either $S_4' = A_4$ or $S_4' = K$. Now S_4/K has order 6, so either $S_4/K \cong Z_6$ or $S_4/K \cong S_3$. But since no element of S_4 has order multiple of 6, no element of S_4/K can have order 6, and $S_4/K \cong S_3$ [not abelian]. Therefore, $S_4' = A_4$.

We claim that $S_4^2 = [S_4, A_4] = A_4$. Indeed, we have that $S_4^2 \lhd S_4' = A_4$, so either S_4^2 is 1, K, or S_4. Suffices then to show that there is a 3-cycle in S_4^2. But:

$$[(1\,2), (1\,2\,3)] = (1\,2)(1\,2\,3)(1\,2)(1\,3\,2) = (1\,2)(2\,3) = (1\,2\,3) \in S_4^2.$$

Hence, the lower central series of S_4 is just $A_4 \lhd S_4$.

Now, for A_4: since A_4/K is abelian, $A_4' \leq K$. Since no subgroup of K is normal in A_4, we have that A_4' is either 1 or K. But, since A_4 is not abelian, we must have $A_4' = K$. Now $A_4^2 \leq K$ is also normal in A_4 [since it's characteristic], so it must either 1 or K. But

$$\begin{aligned}[(1\,2\,3), (1\,2)(3\,4)] &= (1\,2\,3)(1\,2)(3\,4)(1\,3\,2)(1\,2)(3\,4) \\ &= (1\,3)(2\,4))(1\,2)(3\,4) = \\ &= (1\,4)(2\,3) \neq 1.\end{aligned}$$

So, $A_4^2 = K$ and we have that the lower central series for A_4 is just $K \lhd A_4$.

27. (Dummit-Foote, 6.1 #12) For any group G where $Z(G) = 1$, the Upper Central Series of G has $Z_i(G) = 1$ for all i. Since $Z(A_4) = 1 = Z(S_4)$, we have trivial Upper Central Series for both of these groups.

To compute the Lower Central Series of A_4, note that the only non-trivial normal subgroup of A_4, $K = \{1, (12)(34), (13)(24), (14)(23)\}$, has index 3 and thus the quotient A_4/K is abelian. Hence $[A_4, A_4] = K$. To compute $[A_4, K]$, note that

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

hence every product of disjoint two cycles is in $[A_4, K]$, thus $[A_4, K] = K$. It follows that

$$A_4 \geq K \geq K \geq \dots$$

is the Lower Central Series for A_4.

To compute the Lower Central Series of S_4, note that the commutator of the elements $(a\ b)$ and $(a\ b\ c)$ is $(a\ b\ c)$. As A_4 is generated by 3-cycles, we have $A_4 \leq [S_4, S_4]$. Since the quotient S_4/A_4 is abelian, we must have $[S_4, S_4] = A_4$. Now $(a\ b\ c) \in A_4$, so the above commutator is actually an element of $[S_4, A_4]$. Thus $A_4 = [S_4, A_4]$, and it follows easily that

$$S_4 \geq A_4 \geq A_4 \geq \dots$$

is the Lower Central Series for S_4.

6.1.13

(Dummit-Foote, 6.1 #13) Since S_n and A_n have trivial centers for $n \geq 5$, they have $Z_i = 1$ for all i, as above.

Now A_n is simple for $n \geq 5$, hence $[A_n, A_n] = 1$ or $[A_n, A_n] = A_n$. As A_n is non-abelian, we must have $[A_n, A_n] = A_n$, hence the Lower Central Series of A_n is

$$A_n = A_n = \dots.$$

For $n \geq 5$, the only non-trivial normal subgroup of S_n is A_n, and the quotient is order two and hence abelian. Thus $[S_n, S_n] = A_n$. Now $[S_n, A_n]$ must contain $[A_n, A_n] = A_n$, hence $[S_n, A_n] = A_n$. Thus the Lower Central Series for S_n is

$$S_n \geq A_n \geq A_n \geq \dots.$$

6.1.14

§6.1 #14: *If G is a group, then G^i is a characteristic subgroup of G for all i.*

Proof. If φ is any automorphism of G, then by Problem #I above, $\varphi(G^i) = \varphi(G)^i = G^i$. Hence G^i is a characteristic subgroup of G. □

6.1.15

6.1.16

(1) Prove that the additive group $\mathbb{Q}$ has no maximal subgroups.

This proof uses the notion of a divisible abelian group. An abelian group A (written additively) is divisible if and only if, for any non-zero integer n and any $a \in A$, there is always an x such that $a = n \cdot x$, where $n \cdot x = x + x + x + \ldots + x$ n times for $n > 0$ (the empty sum is 0) and $(-n) \cdot x = -(n \cdot x)$. In other words, you can divide by any integer n, hence the name. Sometimes people require divisible groups to be non-trivial as part of the definition. The basic example of a divisible abelian group, and the one that is relevant here, is $\mathbb{Q}$. It's divisible because you can take $x = a/n$ if a is a given rational number and $n \neq 0$ a given integer.

A quotient of a divisible group is also divisible. To prove this, suppose D is a divisible group and H is a subgroup of D. To show the quotient D/H is divisible, write the cosets additively and take an equation $a+H = n\cdot(x+H)$ to be solved for $x+H$ given a coset $a+H$ and an integer $n < 0$. Since D is divisible, we can find an x such that $a = n\cdot x$, and it follows that $n\cdot(x+H) = (x+H)+(x+H)+\ldots+(x+H) = (x+x+\ldots+x+H) = n\cdot x+H = a+H$, as required. The case $n < 0$ is the same with a couple of minus signs. So D/H is divisible.

The finite divisible groups are all trivial. Indeed, suppose A is a non-trivial finite abelian group. Then $\#A \cdot x = 0$ for all $x \in A$ because the order of x divides the order of A. Thus, given a non-zero $a \in A$, it is impossible to solve the equation $a = n \cdot x$ for x if $n = \#A$, so A is not divisible.

The concept of divisibility will surface again when you study things called "injective modules" in chapter 10 of Dummit and Foote.

Now suppose, for a contradiction, that M is a maximal subgroup of $\mathbb{Q}$. Since $\mathbb{Q}$ is abelian, M is normal and we have a quotient group $\mathbb{Q}/M$. Since M is maximal, there are no intermediate subgroups between M and $\mathbb{Q}$. By the Fourth Isomorphism Theorem, there are thus no non-trivial proper subgroups of $\mathbb{Q}/M$. It follows that $\mathbb{Q}/M$ is cyclic. Indeed, if not, since $M \neq \mathbb{Q}$, there is a non-zero $x \in \mathbb{Q}/M$, and supposing $\mathbb{Q}/M$ is not cyclic, $\langle x\rangle \neq \mathbb{Q}/M$, so $\langle x\rangle$ is a non-trivial proper subgroup of $\mathbb{Q}/M$. But there are no such subgroups! Contradiction. Therefore $\mathbb{Q}/M$ is cyclic. Being a quotient of the divisible group $\mathbb{Q}$, $\mathbb{Q}/M$ is divisible. It must therefore be an infinite cyclic group because, otherwise, it would be a nontrivial finite divisible group, and there are no such groups. So $\mathbb{Q}/M$ is an infinite cyclic group, say $\langle x\rangle$. But infinite cyclic groups have lots of subgroups! For instance, $\langle x^2\rangle$ is a non-trivial proper subgroup of $\langle x\rangle = \mathbb{Q}/M$ So we have a contradiction. Therefore $\mathbb{Q}$ has no maximal subgroups.

6.1.17

6.1.18

See the next prob for one solution.

6.1.19

(2) Prove that there is no group whose commutator subgroup is S_4 (see the hint for problem 6.1.19).

This proof uses the following fact from a previous exercise, which was incorrectly stated (at least in my edition of the book): if G'/G'' and G''/G''' are both cyclic, then $G'' = G'''$. The hint stated this with the conclusion that $G'' = \{1\}$, which is what you get when you assume without loss of generality that $G''' = \{1\}$. To reduce the general case to this one, you just have to replace everything by its quotient by G'''.

To prove this bizarre lemma, observe that G/G'' acts on G''/G''' by $(xG'') * yG''' = xyx^{-1}G'''$ for $x \in G$ and $y \in G''$. We are defining this action using representatives for

the cosets, so we have to check that it is well-defined. Let's say that we use different representatives $\xi = xg$ for some $g \in G''$ and $\eta = yh$ for some $h \in G'''$. We must check that we get the same result for the action, meaning that $xyx^{-1}G''' = \xi\eta\xi^{-1}G'''$. Equivalently, $\xi\eta\xi^{-1}xyx^{-1} \in G'''$. To check that the latter holds, substitute the formulas for ξ and η to get $\xi\eta\xi^{-1}xyx^{-1} = xgh^{-1}y^{-1}g^{-1}x^{-1}xyx^{-1} = xgh^{-1}y^{-1}g^{-1}yx^{-1} = xgh^{-1}y^{-1}g^{-1}ygg^{-1}x^{-1} = (xg)(h^{-1}[y,g])(xg)^{-1}$. Now we're in the clear. Indeed, y and g are in G'', so their commutator $[y,g]$ is in G''' by definition. Since h is also in G''', $h^{-1}[y,g]$ is in G''' because G''' is a subgroup. Finally, because G''' is a normal subgroup, $(xg)(h^{-1}[y,g])(xg)^{-1}$ is in G'''. Thus the action is well-defined.

The action of a fixed $xG'' \in G/G''$ is an automorphism of G''/G'''. Indeed, it is a homomorphism from G''/G''' to itself because $(xG'') * (yG''' \cdot zG''') = (xG'') * yzG''' = xyzx^{-1}G''' = xyx^{-1}xzx^{-1}G''' = xyx^{-1}G''' \cdot xzx^{-1}G''' = (xG'') * yG''' \cdot (xG'') * zG'''$, which is the homomorphism condition. It maps G''/G''' to itself because $xyx^{-1} \in G''$ whenever $y \in G''$ since G'' is normal. The map is invertible because, as you can check, the action of $x^{-1}G''$ functions as a two-sided inverse. So we have a mapping, say ϕ, from G/G'' to $\mathrm{Aut}(G''/G''')$. This mapping is a homomorphism basically because $x(\xi y\xi^{-1})x^{-1} = (x\xi)y(x\xi)^{-1}$.

By hypothesis, G''/G''' is a cyclic group, so its automorphism group is abelian. Indeed, an automorphism of a cyclic group is completely determined by which other generator it sends a fixed generator to. The infinite cyclic group $\mathbb{Z}$ has just two generators, 1 or -1, so $\mathrm{Aut}(\mathbb{Z})$ is a cyclic group of order 2. A generator of a finite cyclic group $\mathbb{Z}/n\mathbb{Z}$ corresponds to a unit in the ring $\mathbb{Z}/n\mathbb{Z}$, so the automorphism group here is isomorphic to the unit group of $\mathbb{Z}/n\mathbb{Z}$, which is abelian because that ring is commutative. If you just want to see why these automorphism groups are abelian, note that if t is a generator for the given cyclic group (written multiplicatively), any two automorphisms σ and τ are given by $\sigma(t) = t^a$ and $\tau(t) = t^b$ for some integers a and b such that t^a and t^b are also generators. Then $\sigma\tau(t) = \sigma(t^b) = (\sigma(t))^b = (t^a)^b = t^{ba} = (t^b)^a = (\tau(t))^a = \tau(t^a) = \tau\sigma(t)$, so $\sigma\tau = \tau\sigma$ and $\mathrm{Aut}(\langle t\rangle)$ is abelian.

Any homomorphism ϕ from a group Γ to an abelian group A "factors through" the "abelianization" Γ/Γ'. This means there is a homomorphism ψ from Γ/Γ' to A such that $\phi = \psi \circ \pi$ where π is the usual map from Γ to a quotient of Γ. The terminology is suggestive: we have literally factored the map ϕ into a product (i.e. composition) of two maps. The map ψ is easy to guess: $\psi(\gamma\Gamma') = \phi(\gamma)$ is the only thing that could possibly work, and it is well defined because A is abelian.

We can apply this factoring property with $\Gamma = G/G''$, $A = \mathrm{Aut}(G''/G''')$, and the homomorphism $\phi : G/G'' \to \mathrm{Aut}(G''/G''')$ from above. Here, the abelianization is $\Gamma/\Gamma' = (G/G'')/(G/G'')'$. We have $(G/G'')' = G'/G''$ because its elements are computed by taking products of commutators of elements of G and collapsing G'' to the identity, and those are precisely the elements of G'/G''. Thus, by the Third Isomorphism Theorem, the abelianization is $\Gamma/\Gamma' = (G/G'')/(G/G'')' = (G/G'')/(G'/G'') \cong G/G'$. Via this factored map, the abelianization G/G' acts trivially by conjugation on G''/G'''.

Finally, to show that $G'' = G'''$, the inclusion $G''' \subseteq G''$ is automatic, and for the other inclusion, we show that every generator of G'' is in G'''. These generators are $x^{-1}y^{-1}xy$ with x and y in G'. Suppose the cyclic group G'/G'' is generated by gG'', where $g \in G'$. Then we have $x = g^m a$ and $y = g^n b$ for some integers m and n, where a and b are elements of G''. Picking a generator hG''', where $h \in G''$, for the cyclic group G''/G''', we have other

integers k and l such that $a = h^k c$ and $b = h^l d$ for some c and d in G''''. This implies that $x^{-1}y^{-1}xy = a^{-1}g^{-m}b^{-1}h^{-n}g^m a h^n b = c^{-1}h^{-k}g^{-m}d^{-1}h^{-l}h^{-n}g^m h^k c h^n h^l d$. We had the abelianization G/G' acting trivially on G''/G'''' by conjugation, so since $g^m \in G'$ and $d^{-1}h^{-l}h^{-n} \in G''$, we have $g^{-m}d^{-1}h^{-l}h^{-n}g^m = d^{-1}h^{-l}h^{-m}$ and we effectively ignore the g^m terms as we continue with our commutator computation: $x^{-1}y^{-1}xy = c^{-1}h^{-k}g^{-m}d^{-1}h^{-l}h^{-n}g^m h^k c h^n h^l d = c^{-1}h^{-k}d^{-1}h^{-l}h^{-n}h^k c h^n h^l d = [ch^k, h^n h^l d]$, a commutator of the elements $ch^k \in G''$ and $h^n h^l d \in G''$ (subgroup!). Thus $x^{-1}y^{-1}xy$ is a commutator of things in G'', so it belongs to G'''' for any x, $y \in G'$. It follows that $G'' \subseteq G''''$, so $G'' = G''''$, as required.

Assuming the result from that previous exercise, suppose, for a contradiction, that G is a group with $G' = S_4$. Then $G'' = (G')' = S_4' = A_4$. As for the last step: the corresponding statement is true for all S_n, not just S_4. For a sketch of the proof, note first that the commutator subgroup has to be contained in the alternating group. Indeed, we have the sign homomorphism sgn: $S_n \to \{\pm 1\}$, and since $(\pm 1)^{-1} = \pm 1$, the fact that $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}$ guarantees that any permutation has the same sign as its inverse. This implies that any commutator in S_4 is an even permutation: $\mathrm{sgn}(\sigma\tau\sigma^{-1}\tau^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\mathrm{sgn}(\sigma^{-1})\mathrm{sgn}(\tau^{-1})$ $= \mathrm{sgn}(\sigma)^2\mathrm{sgn}(\tau)^2 = 1$. So the commutator subgroups is contained in the alternating subgroup. For the other inclusion, any even permutation is a product of an even number of transpositions, which you then have to write as a product of commutators (or maybe just a single commutator!). Anyway, $G'' = S_4' = A_4$. Similarly, $G'''' = (G'')' = A_4'$. Note that the commutator subgroup is always normal (even more: it's a characteristic subgroup, i.e., it's fixed by all automorphisms), so A_4' must be some normal subgroup of A_4. The only normal subgroups of A_4 are $\{1\}$, A_4, and a subgroup of order 4 isomorphic to the Klein 4-group, which is the symmetry group of a rectangle (not a square). The commutator subgroup is not $\{1\}$ because A_4 is not abelian. It isn't A_4 because, for instance, a 3-cycle cannot be written as a product of commutators of even transpositions, so some elements are not in the commutator subgroup. The only possibility is that A_4' is that normal subgroup of order 4. Now we are ready for our contradiction. $G'/G'' = S_4/A_4 \cong \{\pm 1\}$ is a group of order 2, a prime number, hence cyclic. We established that $G'''' = A_4'$ has order 4, so $G''/G'''' = A_4/A_4'$ is a group of order $12/4 = 3$, a prime number, so this group is also cyclic. Both those quotient groups are cyclic, so by the result I stated for you at the beginning, $G'' = G''''$. This is a contradiction: $A_4 = A_4'$, but we already said that A_4 is not its own commuator subgroup. Therefore there is no group whose commutator subgroup is S_4.

6.1.20

6.1.21

21. First note that if M is a maximal subgroup of G, then for all $\phi \in \mathrm{Aut}(G)$, $\phi(M)$ is also maximal. [Indeed, if $\phi(M) < H < G$, then $M < \phi^{-1}(H) < G$, since $\phi^{-1} \in \mathrm{Aut}(G)$, and hence it's bijective.] Also, given any $M < G$ maximal, then $\phi^{-1}(M)$ is also maximal [by the above remark], and so $M = \phi(\phi^{-1}(M))$. Hence, for all $\phi \in M$,

$$\{M \ : \ M \text{ is a max. subgroup of } G\} = \{\phi(M) \ : \ M \text{ is a max. subgroup of } G\}.$$

Now, observe that if $\phi \in \mathrm{Aut}(G)$ then $y \in \bigcap_{M \text{ max.}} \phi(M)$ if, and only if, for all M, there exists $x \in M$ such that $y = \phi(x)$. But, since ϕ is injective, this happens if, and only if, $x \in \bigcap_{M \text{ max.}} M$. Hence, $\bigcap_{M \text{ max.}} \phi(M) = \phi\left(\bigcap_{M \text{ max.}} M\right)$

So, for all $\phi \in \mathrm{Aut}(G)$, we have

$$\Phi(G) = \bigcap_{M \text{ max.}} M = \bigcap_{M \text{ max.}} \phi(M) = \phi\left(\bigcap_{M \text{ max.}} M\right) = \phi(\Phi(G)).$$

Proof: Let $\mathcal{M} = \{\dots, H_i, \dots\}$ be the (potentially infinite, even uncountable) set of maximal subgroups of G, and I be its indexing set.

Lemma 1: For any $\varphi \in Aut(G)$, we have φ permutes the elements of $\mathcal{M}$. Proof: Pick an arbitrary $H_i \in \mathcal{M}$. If $\varphi(H_i)$ is not a maximal subgroup of G, then observe $\varphi(H_i) < K < G$. We have $H_i = \varphi^{-1}(\varphi(H_i)) < \varphi^{-1}(K)$, the last term of which is properly contained in G (else $K = \varphi(G) = G$), therefore $H_i < \varphi^{-1}(K) < G$, a contradiction. Therefore $\varphi(H_i)$ is a maximal subgroup, and this action of φ on $\mathcal{M}$ is well defined, injective by nature, and surjective since $\varphi^{-1}(H_i)$ will map to H_i. □

Lemma 2: $\varphi(\bigcap_{i\in I} H_i) = \bigcap_{i\in I} \varphi(H_i)$ for any isomorphism φ of G, with $H_i \leq G$ for all $i \in I$. Proof:

$$\varphi(x) \in \varphi(\bigcap_{i\in I} H_i) \Leftrightarrow x \in \bigcap_{i\in I} H_i \Leftrightarrow \forall i \in I[x \in H_i] \Leftrightarrow$$

$$\forall i \in I[\varphi(x) \in \varphi(H_i)] \Leftrightarrow \varphi(x) \in \bigcap_{i\in I} \varphi(H_i) \quad \square$$

(21) Let π denote the permutation of the indices of the elements of $\mathcal{M}$ by $\varphi \in Aut(G)$ by lemma 1. We have

$$\varphi(\Phi(G)) = \varphi(\bigcap_{i\in I} H_i) = \bigcap_{i\in I} \varphi(H_i) = \bigcap_{i\in I} H_{\pi(i)} = \bigcap_{i\in I} H_i = \Phi(G)$$

since $\pi(I) = I$. □

6.1.22

(22) (With aid from Project Crazy Project) (Assuming G is finite) Lemma 3: Let $A \leq C \leq G$ and $B \leq G$. Then $A(B \cap C) = AB \cap C$. Proof: ($\subseteq$) $x \in A(B \cap C) \Rightarrow x = ad$ for some $a \in A$ and $d \in B \cap C$, so that $ad \in AB$ and $ad \in C$, ergo $x \in AB \cap C$. ($\supseteq$) $x \in AB \cap C \Rightarrow x = ab \wedge x \in C$, so that $b = a^{-1}x \in C$ and now $b \in B \cap C$, hence $x \in A(B \cap C)$. $\square$

Lemma 4: $\Phi(G)H < G$ for any $H < G$. Proof: Quickly done, this is a consequence of exercise 24. Proving it otherwise is a simple feat nonetheless. $\square$

Now, we have $\Phi(N) \operatorname{char} N \trianglelefteq G \Rightarrow \Phi(N) \trianglelefteq G$, so that $\Phi(N)K$ is a subgroup for any $K \leq G$. Observe the implications:

$$\Phi(N) \nleq \Phi(G) \Rightarrow \exists i \in I[\Phi(N) \nleq H_i] \Rightarrow N \nleq H_i \Rightarrow H_i \cap N < N \Rightarrow$$

$$\Phi(N)(H_i \cap N) < N \Rightarrow \Phi(N)H_i \cap N < N \Rightarrow G \cap N < N \Rightarrow N < N$$

We proceed to constructing a counterexample when $N \ntrianglelefteq G$. This lemma will be useful for the next exercise as well: Lemma 5: $\Phi(S_n) = \Phi(A_n) = 1$ when $n \geq 5$. Proof: $\Phi(A_n) \triangleleft A_n$, so we must have $\Phi(A_n) = 1$. As computed in 4.6.2, the only proper normal subgroups of S_n are A_n and 1. Since A_n is a maximal subgroup and not the only one (place $\langle\ (12)\ \rangle$ in a maximal subgroup, for instance), we must have $\Phi(S_n) = 1$. $\square$

Now, associate Q_8 with its isomorphic image in S_8. By order considerations, it is not equal to S_8, A_8, or 1, so it is nonnormal. We can see $\Phi(Q_8) = \langle\ -1\ \rangle$ is nontrivial, and by the above lemma $\Phi(S_8)$ is trivial, so the containment doesn't hold. $\square$

6.1.23

(23) The groups of order 3 and 2 by Cauchy are maximal by their orders, and have trivial intersection, so $\Phi(S_3) = 1$. By 3.5.8, $\langle\ (12)(34),\ (13)(24)\ \rangle$ and $\langle\ (123)\ \rangle$ are maximal subgroups, and have trivial intersection, therefore $\Phi(A_4) = 1$.

For $\Phi(S_4)$, take an arbitrary subgroup M of order 12 in S_4. By Cauchy, M has an element of order 3, which must be a 3-cycle. Since conjugation of M by elements of S_4 are automorphisms of M (since $M \trianglelefteq S_4$ by order), we have that M contains all 3-cycles, and is thus equal to A_4. Now, $\langle\ (12), (123)\ \rangle$ can only contain elements of S_3 due to its generators fixing 4, and indeed it does generate at least and thus exactly 6 elements. Therefore it is maximal since otherwise it is contained in a group of order 12, which must be A_4 by above, a contradiction since A_4 doesn't contain a subgroup of order 6 by 3.5.8. By this, $\Phi(S_4)$ is either of order 1 or 3, and not the latter since $\Phi(S_4) \trianglelefteq S_4$ would imply $\Phi(S_4)$ contains every 3-cycle.

By the lemma, $\Phi(A_5) = \Phi(S_5) = 1$. $\square$

6.1.24

(24) (Assuming G is finite)($\subseteq$) Let $x \in \Phi(G)$, and for any $H < G$, place H in a maximal subgroup H^*. We have $x \in H^*$, therefore $\langle x, H \rangle \leq \langle x, H^* \rangle = H^* < G$. ($\supseteq$) Let x be a nongenerator, so that for any maximal subgroup H^*, we must have $\langle x, H^* \rangle = H^*$, so that $x \in H^*$. $\square$

6.1.25

(25) Let P be an arbitrary Sylow subgroup of $\Phi(G)$. By Frattini, we have $\Phi(G)N_G(P) = G$. Since $\Phi(G)N_G(P)$ is clearly not a proper subgroup, we must have $N_G(P)$ is not a proper subgroup by lemma 4, which is to say $N_G(P) = G$ and now $P \trianglelefteq G$, and in particular $P \trianglelefteq \Phi(G)$, so that $\Phi(G)$ is nilpotent by theorem 3(3). $\square$

§6.1 #25: *If G is a finite group, then $\Phi(G)$ is nilpotent.*

Proof. We know that $\Phi(G) \trianglelefteq G$, so if P is a Sylow p-subgroup of $\Phi(G)$ for any prime p, then $G = \Phi(G)N_G(P)$ by the Frattini Argument. Since $\Phi(G)$ is the set of nongenerators of G, this implies $G = N_G(P)$. Hence every Sylow subgroup of $\Phi(G)$ is normal in G, so is certainly also normal in $\Phi(G)$, and $\Phi(G)$ is nilpotent by NGT. $\square$

25. Note that since G is finite, G has maximal subgroups, and each one of these are, by definition, different from G itself. So $\Phi(G) \neq G$.

Let $P \in \mathrm{Syl}_p(\Phi(G))$. Since $\Phi(G) \operatorname{char} G$, we have that $\Phi(G) \triangleleft G$. Then, by Frattini's argument, we have that $G = \Phi(G)N_G(P)$.

Now, if $N \stackrel{\text{def}}{=} N_G(P) \neq G$, then, there exists M maximal such that $N < M < G$, and hence $\Phi(G), N \leq M$. But then, $G = \Phi(G)N \leq M < G$, which cannot happen.

Thus, $G = N = N_G(P)$, i.e., $P \triangleleft G$. Therefore, $P \triangleleft \Phi(G)$. So, every Sylow subgroup of $\Phi(G)$ is normal, and hence $\Phi(G)$ is nilpotent.

6.1.26

§6.1 #26(a): *If P is a finite p-group for some prime p, then $\bar{P} = P/\Phi(P)$ is an elementary abelian p-group.*

Proof. Since P is a finite p-group, P is nilpotent. Hence $P' \leqslant \Phi(P)$ by NGT, and so $\bar{P}$ is abelian. Of course, $\bar{P}$ is a quotient of a p-group so is a p-group.

If M is a maximal subgroup of P, then $M \trianglelefteq P$ and $|P : M| = p$ by either NGT or Sylow's Theorem. Thus P/M is of order p and so for $x \in P$, $x^p M = (xM)^p = M$ in P/M. Hence $x^p \in M$ for all $x \in P$. Since this holds for every maximal subgroup, we have $x^p \in \Phi(P)$ and so $(x\Phi(P))^p = \Phi(P) = 1_{\bar{P}}$ for all $x\Phi(P) \in \bar{P}$. Hence $\bar{P}$ is elementary abelian. $\square$

Dummit and Foote *Abstract Algebra*, section 6.1, exercise 26a-b:

(a) Let the overbar denote passage into $P/\Phi(P)$. Prove $\overline{P}$ is an elementary abelian p-group. [Prove $P' \leq \Phi(P)$ and $x^p \in \Phi(P)$ for any $x \in P$]

(b) Prove that if P/N is elementary abelian, then $\Phi(P) \leq N$.

Proof: (a) Note that p-groups are nilpotent, so that every maximal subgroup of P is normal and of prime index by 6.1.4, so that the quotient group of P over any maximal subgroup is abelian, so that by an extension of 5.4.14, P' is contained within the intersection of all maximal subgroups, which is to say $P' \leq \Phi(P)$. Similarly, since the quotient groups are of prime order, we have $\bar{x}^p$ is trivial for any $x \in P$, which is to say $x^p \in \Phi(P)$. □

(b) Lemma 1: $\Phi(Z_p^t) = 1$ for any prime p and nonnegative integer t. Proof: Let $(x_1, \ldots, x_r, \ldots, x_t)$ be any nontrivial element with a nontrivial coordinate designated by x_r. We have $\langle e_1, \ldots, e_{r-1}, e_{r+1}, \ldots, e_t \rangle$ is a subgroup of order p^{t-1} that is maximal by its index, and this particular subgroup doesn't contain $(x_1, \ldots, x_r, \ldots, x_t)$. Since the nontrivial element was arbitrary, we have $\Phi(Z_p^t) = 1$. □

Since P/N is elementary abelian, we have the intersection of its maximal subgroups is the identity, which is to say (by the Lattice Isomorphism Theorem) that the intersection of the set of maximal subgroups of P containing N is contained in N. By definition, N is contained within the intersection of the set of maximal subgroups of P containing N, so there is an equality. Since $\Phi(P)$ is contained in all maximal subgroups of P, we have $\Phi(P) \leq N$.

In other words, if $\varphi : P \to E$ is any homomorphism of P into an elementary abelian group E, then φ factors through $\Phi(P)$.

$$\begin{array}{ccc} P & \xrightarrow{\pi} & P/\Phi(P) \\ & \searrow \varphi & \downarrow \psi \\ & & E \end{array}$$

□

6.1.27

6.1.28

6.1.29

6.1.30

6.1.31

Dummit and Foote *Abstract Algebra*, section 6.1, exercise 31:

A group M is called a minimal normal subgroup of G when $M \trianglelefteq G$ and every proper nontrivial subgroup of M is nonnormal in G. Prove that when G is finite and solvable, any minimal subgroup M is an elementary abelian p-group for some prime p. [Examine M's characteristic subgroups M' and $\langle\, x^p \mid x \in P \,\rangle$]

Proof: Let M^p denote $\langle\, x^p \mid x \in P \,\rangle$. If M is trivial, the case holds, so assume $M \neq 1$.

Lemma 1: $G^n \operatorname{char} G$ for any finitely generated group G and $n \in \mathbb{Z}$. Proof:

$x \in G^n \Leftrightarrow x = y_1^n \dots y_r^n \Leftrightarrow \varphi(x) = \varphi(y_1^n \dots y_r^n) = \varphi(y_1)^n \dots \varphi(y_r)^n \Leftrightarrow \varphi(x) \in G^n$ □

Since any characteristic subgroup of M is concomitantly normal in G, we must not have any proper nontrivial characteristic subgroups of M. Assume $M' = M$; since subgroups of a solvable group are solvable by Proposition 10(1), and yet the derived chain of M terminates before reaching the identity, we have a contradiction. So assume $M' = 1$, and now M is abelian.

Suppose $M^p = 1$ for some prime p. Then all the generators of M^p are trivial, which is to say $x^p = 1$ for all $x \in M$ and now M is elementary abelian. So assume that $M^p = M$ for any prime p. Inductively prove that $M^n = M$ for all $n \in \mathbb{Z}^+$, an absurd conclusion for $M^{|M|} = M$. The case is clear when $n = 1$, so proceed to the inductive step. The case is assumed true for prime n, so we have prime q dividing $n \neq q$. We have $(M^{n/q})^q = M$ by induction, revealing that for any element of the abelian M we have a representation of the form
$(m_{1,1}^{n/q} \dots m_{1,r_1}^{n/q})^q (m_{2,1}^{n/q} \dots m_{2,r_2}^{n/q})^q \dots (m_{s,1}^{n/q} \dots m_{s,r_s}^{n/q})^q =$
$m_{1,1}^n \dots m_{1,r_1}^n m_{2,1}^n \dots m_{2,r_2}^n \dots m_{s,1}^n \dots m_{s,r_s}^n \in M^n$. □

6.1.32

6.1.33

Proof: Let the overbar denote passage into G/M. If $p \in \pi$, then by induction there is a Hall π-subgroup of $\overline{G}$ of order n/p^a, so that its preimage in G is of order n, and is thus a Hall π-subgroup. Furthermore, if any Hall π-subgroup H does not contain M, then $H \cap M \neq M$, so that p divides $|M : H \cap M|$, so that by the Second Isomorphism Theorem p divides $|HM : H|$, which implies p divides $|G : HM| \cdot |HM : H| = |G : H|$, a contradiction. Now, for any two Hall π-subgroups H_1 and H_2, we have $\overline{H_1}$ and $\overline{H_2}$ are Hall π-subgroups of $\overline{G}$, and by induction they are conjugate, so that $\bar{g}\overline{H_1}\bar{g}^{-1} = \overline{gH_1g^{-1}} = \overline{H_2}$. Since $|gH_1g^{-1}| = n$ we have gH_1g^{-1} is a Hall π-subgroup, and now both these groups contain M so that $gH_1g^{-1} = H_2$.

Therefore assume $p \notin \pi$. Taking the Hall π-subgroup $\overline{H}$ of $\overline{G}$ and taking its preimage HM of order p^an, we can be assured that if $HM < G$, then by induction we can recognize Hall π-subgroups of HM for the existence condition. For any two Hall π-subgroups H_1 and H_2 of G, since $H_1 \cap M = H_2 \cap M = 1$, we have Hall π-subgroups $\overline{H_1}$ and $\overline{H_2}$ of $\overline{G}$, so that $\bar{g}\overline{H_1}\bar{g}^{-1} = \overline{H_2}$ by induction, and now $gH_1g^{-1}M = gH_1Mg^{-1} = H_2M$, so that $gH_1g^{-1} \leq H_2M$. This reveals H_1 is conjugate to some Hall π-subgroup of H_2M, and by induction this one is conjugate to H_2, so that finally H_1 is conjugate to H_2.

So assume $HM = G$ and $|G| = p^an$. If G is a p-group the proposition is evident, so we can take a minimal normal subgroup $\overline{N}$ (of order q^b with $q \neq p$) of $\overline{G}$, and observe $Q \in Syl_q(N)$. If $Q \trianglelefteq G$, then we can argue with Q in place of M as above. Therefore assume $N_G(Q) < G$. Since $\overline{N} \trianglelefteq \overline{G} \Rightarrow N \trianglelefteq G$, we can apply Frattini's Argument to N. Notice:

$$|G| = p^an = \frac{|N| \cdot |N_G(Q)|}{|N \cap N_G(Q)|} = \frac{p^aq^b \cdot |N_G(Q)|}{|N \cap N_G(Q)|}$$

Since $Q \leq N$ and $Q \leq N_G(Q)$, we have q^b divides $|N \cap N_G(Q)|$. Therefore, letting $n = q^{\alpha_0}p_1^{\alpha_1}\dots p_r^{\alpha_r}$, we observe that q^{α_0} and $p_i^{\alpha_i}$ divides $|N_G(Q)|$ for all i, ensuring that n divides $|N_G(Q)|$ and now by induction there exist Hall π-subgroups of G. Establish conjugacy: Take an arbitrary Hall π-subgroup T of G. Since $MT = G$ and $M \leq N$, we have:

$$\frac{|N| \cdot |T|}{|N \cap T|} = |G| \Rightarrow \frac{p^aq^b \cdot n}{|N \cap T|} = p^an \Rightarrow |N \cap T| = q^b = |Q|$$

So that $N \cap T$ is a Sylow q-subgroup of N and is thus conjugate to Q; let $g(N \cap T)g^{-1} = Q$. Since clearly $T \leq N_G(N \cap T)$, we have $gTg^{-1} \leq gN_G(N \cap T)g^{-1} = N_G(g(N \cap T)g^{-1}) = N_G(Q)$, so that every Hall π-subgroup of G is conjugate to some Hall π-subgroup of $N_G(Q)$, whose Hall π-subgroups are inductively assumed to be conjugate to each other. $\square$

6.1.34

6.1.35

6.1.36

6.1.37

6.1.38

6.2 Applications in Groups of Medium Order 201

6.2.1

6.2.2

6.2.2

$|S_3 \times S_3| = 36$ so a Sylow 2-subgroup has order 4.
Let a=(12) and b=(1,3) and e is the identity element of S_3.
$P = \{(e,e),(e,a),(a,e),(a,a)\}$
$Q = \{(e,e),(e,b),(b,e),(b,b)\}$
$S = \{(e,e),(e,a),(b,e),(b,a)\}$
then it is obvious that P, Q, S are Sylow 2-subgroups and $P \cap Q = \{(e,e)\}$ while $P \cap S = \{(e,e),(e,a)\}$. QED

6.2.3

4. Exercise 6.2.3. Prove that if $|G| = 380$, then G is not simple.

   First we write 380 as a product of prime powers, namely $2^2 * 5 * 19$. Suppose by way of contradiction G is a simple group of order 380. The number of Sylow 19-subgroups is congruent to 1 mod 19 and divides 20, hence is 1 or 20. But 1 is ruled out because then G would have a normal subgroup of order 19, which would contradict the hypothesis that G is simple. Therefore G has 20 Sylow 19-subgroups. Next we consider the Sylow 5-subgroups. The number is congruent to 1 mod 5 and divides $4 * 19$. Thus there are 1 or 76 Sylow 5-subgroups.

   Now we count elements. If P and Q are distinct Sylow 19-subgroups, then $P \cap Q \neq P$ and $P \cap Q \leqslant P$. Since $|P \cap Q|$ divides $|P| = 19$ by Lagrange's theorem, we deduce that

$P \cap Q = 1$. It follows that G has at least $20 * 18 = 360$ elements of order 19. Similarly two distinct Sylow 5-subgroups intersect trivially and we deduce that G has at least $76 * 4 = 304$ elements of order 5. We conclude that G has at least $360 + 304 = 664 >$ 380 elements, which is a contradiction. Therefore there is no simple group of order 380.

6.2.3
$380 = 19 \times 2^2 \times 5$
Suppose G is simple then $n_{19} = 19k + 1$, dividing 20 and $k > 0$. So $n_{19} = 20$ and since 19 is a prime, 2 subgroups of order 19 intersect trivially and, hence, there are $20 \times (19 - 1) = 360$ elements of order 19.
Now $n_5 = 5k + 1 > 1$ so $n_5 \geq 6$ so by an analogous argument, there are at least $6 \times (5 - 1) = 24$ elements of order 5. So G has at least $360 + 24 = 384$ distinct elements, a contradiction. So G is not simple. QED

6.2.4

$80 = 2^4 \times 5$
Suppose G is simple then $n_5 = 5k + 1$, dividing 16 and $k > 0$. So $n_5 = 16$ and since 5 is a prime, 2 subgroups of order 5 intersect trivially and, hence, there are $16 \times (5 - 1) = 64$ elements of order 5.
So there are at most 15 elements of order divisible by 2. Since a Sylow 2-subgroup has exactly 15 elements of order divisible by 2, there is only one Sylow 2-subgroup. That implies the Sylow 2-subgroup is a proper normal subgroup in G, a contradiction. So G is not simple. QED
$351 = 3^3 \times 13$
Suppose G is simple then $n_{13} = 13k + 1$, dividing by 27 and $k > 0$. So $n_3 = 27$ and since 13 is a prime, 2 subgroups of order 13 intersect trivially and, hence, there are $27 \times (13 - 1) = 324$ elements of order 13.
So there are at most 26 elements of order divisible by 3. Since a Sylow 3-subgroup has exactly 26 elements of order divisible by 3, there is only one Sylow 3-subgroup. That implies the Sylow 3-subgroup is a proper normal subgroup in G, a contradiction. So G is not simple. QED
$3875 = 5^3 \times 31$
Suppose G is simple then $n_{31} = 31k + 1$, dividing 27 and $k > 0$. So $n_{31} = 125$ and since 31 is a prime, 2 subgroups of order 31 intersect trivially and, hence, there are $125 \times (31 - 1) = 3750$ elements of order 13.
So there are at most 124 elements of order divisible by 5. Since a Sylow 5-subgroup has exactly 124 elements of order divisible by 5, there is only one Sylow 5-subgroup. That implies the Sylow 5-subgroup is a proper normal subgroup in G, a contradiction. So G is not simple. QED
$5313 = 3 \times 7 \times 11 \times 23$
Suppose G is simple then $n_{23} = 23k + 1$, dividing by 231 and $k > 0$. So $n_{23} = 231$

and since 23 is a prime, 2 subgroups of order 23 intersect trivially and, hence, there are $231 \times (23 - 1) = 5082$ elements of order 13.
$n_{11} = 11k + 1$, divisible by 483 and $k > 0$. Since 12 does not divide 483 $n_{11} \geq 23$ and since 11 is a prime, 2 subgroups of order 11 intersect trivially and, hence, there are at least $23 \times (11 - 1) = 230$ elements of order 11. By Lagrange's theorem G has at least one element of order 7 and one element of order 3, so G has at least $5082 + 230 + 1 + 1 = 5314$ distinct elements. QED

6.2.5

6.2.6

Analysis of Groups of Order 2205 (6.2.6)

Dummit and Foote *Abstract Algebra*, section 6.2, exercise 6 (excerpt):

Prove there are no simple groups of order $2205 = 3^2 \cdot 5 \cdot 7^2$.

Proof: Assume G to be a contradiction. By Sylow analysis, we have:

$$n_3 \in \{7, 49\} \quad n_5 \in \{21, 441\} \quad n_7 = 15$$

Index considerations disallow $n_3 = 7$, though we need only look at $n_7 = 15$. Since $15 \not\equiv 1 \mod 7^2$, set $P_0 = P_1 \cap P_2$ for $P_1, P_2 \in Syl_7(G)$ such that $|P_0| = 7$. We have $P_0 \trianglelefteq P_1, P_2$ so that $7^2 \mid |N_G(P_0)| \neq 7^2$. Due to index considerations once more, we have $|N_G(P_0)| = 3 \cdot 7^2$. But in this case $n_7(N_G(P_0)) = 1$, so that there is a unique Sylow 7-subgroup of $N_G(P_0)$, despite P_1 and P_2 being distinct groups of order 7^2 contained therein. □

6.2.6

$2025 = 3^2 \times 5 \times 7^2$

So 14 is the smallest integer k such that $|G|$ divides $k!$. Now suppose G is not simple then $n_7 = 7k + 1$ dividding 45, $k > 0$ then $n_7 = 15 \not\equiv 1(mod 7^2)$ so there P, Q $\in Syl_7(G)$ such that $|P : P \cap Q| = 7$ by lemma 6.2.13. Then P and Q are in $N_G(R)$ for $R = P \cap Q$ since R is the maximal subgroup in each 7-group P and Q. So $N_G(R)$ contains at least 2 distinct Sylow 7-subgroups so $|N_G(R)| = 7^2 * m$ and applying the Sylow theorem for $N_G(R)$ yields $n_7 = 7k + 1 \geq 2$, so $n_7 \geq 8$. But n_7 divides m so $m \geq 8$ so $|G : N_G(R)| \leq \frac{3^2 \times 5 \times 7^2}{7^2 \times 8} < 10$. So G has a subgroup of index k less than 10 and there is a homomorphism from G into S_k, hence —G— divides $k!$. But at the beginning we says $k \geq 14$, so there is a contradiction. Hence G is not simple. QED

$4125 = 3 \times 5^3 \times 11$

If $|G|$ divides $k!$ then $k!$ must have enough power of 5, so k must be no less than 15.

Now suppose G is not simple then $n_5 = 5k + 1$ dividing 33 and $k > 0$. So $n_5 = 11$ and if P is a Sylow 5-subgroup then $|G : N_G(P)| = 11$ so G has a subgroup of index 11 and, by considering the translation action on the left cosets created by that subgroup, there is a homomorphism from G into S_{11}. Thus, $|G|$ divides 11! but $k \geq 15$ so we get a contradiction. Then G is simple. QED

$5103 = 3^6 \times 7$

If $|G|$ divides $k!$ then $k!$ must have enough power of 3, so k must be no less than 15.

Now suppose G is not simple then $n_3 = 3k + 1$ dividing 7 and $k > 0$. So $n_3 = 11$ and if P is a Sylow 3-subgroup then $|G : N_G(P)| = 7$ so G has a subgroup of index 7 and, similarly, a homomorphism into S_7. Thus, $|G|$ divides 7! but $k \geq 15$ so we get a contradiction. Then G is simple. QED

$6545 = 5 \times 7 \times 11 \times 17$

If $|G|$ divides $k!$ then $k!$ must be no less than 17.

Now suppose G is not simple then $n_5 = 5k + 1$ dividing $7 \times 11 \times 17$ and $k > 0$. Simple arithematic shows that $n_5 = 11$. Then if P is a Sylow 5-subgroup then $|G : N_G(P)| = 11$ so G has a subgroup of index 11 and, similarly, a homomorphism into S_{11}. Thus, $|G|$ divides 11! but $k \geq 17$ so we get a contradiction. Then G is simple. QED

$6435 = 3^2 \times 5 \times 11 \times 13$

If $|G|$ divides $k!$ then $k!$ must be no less than 13.

Now suppose G is not simple then $n_5 = 5k + 1$ dividing $3^2 \times 11 \times 13$ and $k > 0$. Simple arithematic shows that $n_5 = 11$. Then if P is a Sylow 5-subgroup then $|G : N_G(P)| = 11$ so G has a subgroup of index 11 and, similarly, a homomorphism into S_{11}. Thus, $|G|$ divides 11! but $k \geq 13$ so we get a contradiction. Then G is simple. QED

6.2.7

6.2.7

$1755 = 3^3 \times 5 \times 13$

Now suppose G is not simple then $n_3 = 3k + 1$ dividing 5×13 and $k > 0$. Therefore, $n_3 = 13$.Then if P is a Sylow 3-subgroup then $|G : N_G(P)| = 13$ so G has a subgroup of index 13 and by considering the translation action on the left cosets created by that subgroup,there is a homomorphism from G into S_{13}.

Now $n_{13} = 13k+1$ dividing 5×3^3 and $k > 0$. Simple arithmetic shows that $n_{13} = 27$ and let Q $\in Syl_{13}(G)$ then $|N_G(Q)| = \frac{|G|}{n_{13}} = 5 \times 13 = 65$. But G can be identified as a subgroup of S_{13}; therefore, Q and $N_G(Q)$ can also be embedded into S_{13} and we use the same notation to denote their embeddings. In S_{13}, following the discussion in 6.2 about permutation representations, the number of Sylow 13-subgroups is: $\frac{13!}{13 \times 12}$ and therefore, $N_{S_{13}}(Q) = 13 \times 12$. Obviously, $N_G(Q) \leq N_{S_{13}}(Q)$ so 65 divides 156, a contradiction. So G is simple. QED// $5265 = 3^4 \times 5 \times 13$

Now suppose G is not simple then $n_3 = 3k + 1$ dividing 5×13 and $k > 0$. Therefore, $n_3 = 13$.Then if P is a Sylow 3-subgroup then $|G : N_G(P)| = 13$ so G has a subgroup of index 13 and, by considering the translation action on the left cosets created by that subgroup,there is a homomorphism from G into S_{13}.

Now $n_{13} = 13k + 1$ dividing 5×3^4 and $k > 0$. Simple arithmetic shows that $n_{13} = 27$ and let Q $\in Syl_{13}(G)$ then $|N_G(Q)| = \frac{|G|}{n_{13}} = 3 \times 5 \times 13 = 195$. But G can be identified as a subgroup of S_{13}; therefore, Q and $N_G(Q)$ can also be embedded into S_{13} and we use the same notation to denote their embeddings. In S_{13}, following the discussion in 6.2 about permutation representations, the number of Sylow 13-subgroups is: $\frac{13!}{13 \times 12}$ and therefore, $N_{S_{13}}(Q) = 13 \times 12$. Obviously, $N_G(Q) \leq N_{S_{13}}(Q)$ so 195 divides 156, a contradiction. So G is simple. QED

6.2.8

6.2.9

6.2.10

6.2.11

6.2.12

6.2.12.

$9995 = 3 \times 5 \times 7^2 \times 13$

Now suppose G is not simple then $n_{13} = 13k + 1$ dividing $3 \times 5 \times 7^2$ and $k > 0$. Simple arithmetic shows that $n_3 = 105$. Then if Q is a Sylow 13-subgroup then $|G : N_G(Q)| = 105$ so $|N_G(Q)| = 7 \times 13 = 91$. We call this normalizer of Q in G as N to ease notation. Applying the Sylow theorem for N yields that it must have a Sylow 7-subgroup. And since 7 does not divide $13 - 1 = 12$ N must be cyclic (an example of group of order pq shown in class). So let P $\in Syl_7(N)$, since Q normalizes P, $Q \leq N_G(P)$.

Since P is a group of order 7 in G, by Sylow therem, there exists $P^* \in Syl_7(G)$ such that $P < P^*$. Since $|P^* : P| = 7$, P is normal in P^* by the thereom in 6.1 about p-groups. P is certainly normal in N as N is cyclic. So $< N, P^* > \leq N_G(P)$. Since $|P^*| = 7^2$, P^* is either cyclic or isomorphic to the abelian group $Z_7 \times Z_7$ (easily proved by take an element of order 49, if any, or an element a of order 7 and b not in $< a >$ and show $| < a,b > | = 49$, then a commutes with b). Furthermore, N is cyclic and $N \cap P^* = P$,$| < N, P^* > | = 7 \times 13 \times 7$. Therefore, $|G : N_G(P)| \mid 15$. Since 13 is the smallest integer k such that $|G| \mid k!$, G can not have a subgroup of index less than 13 (otherwise by considering translation action on left cosets, there is a homomorphism from G into S_k). As a consequence, $|G : N_G(P)| = 15$ and, thus, $|N_G(P)| = 7^2 \times 13$

Applying the Sylow theorem for $N_G(P)$ the number of Sylow 13-subgroup is (13k+1)

which divides 49. Thus, there is only one Sylow 13-subgroup in $N_G(P)$. Recall that $Q \leq N_G(P)$, Q is the only Sylow 13-subgroup in $N_G(P)$, implying that $Q \lhd N_G(P)$. Consequently, $N_G(P) \leq N_G(Q) = N$. But $|N_G(P)| = 7^2 \times 13 > 7 \times 13 = |N_G(Q)|$, so we have a contradiction. Thus G is not simple. QED

6.2.13

6.2.13

By 6.1.4, $R = P \cap Q$, $R < N_P(R) \leq N_G(P)$ and $R < N_Q(R) < N_G(R)$. Since R is maximal, $N_P(R)$ and $N_Q(R)$ are distinct p-subgroups. Now suppose that $N_G(R)$ has only one Sylow subgroup than it must contains both $N_P(R)$ and $N_Q(R)$ by the Sylow theorem applied for this group. Now by applying Sylow theorem again for G, that Sylow p-subgroup of $N_Q(R)$ is contained in some Sylow p-subgroup of G and its intersection with P, Q contains $N_P(R) > R$ and $N_Q(R) > R$. Since at least one intersection is between two distinct Sylow subgroups, that leads to a contradiction to the maximality of R. So $N_G(R)$ contains at least 2 distinct Sylow p-subgroups. We claim that if S is a Sylow p-subgroup of G then S contains R. Suppose not, then RS is a p-subgroup of $N_G(R)$ (since R is normal in $N_G(R)$ and the 2nd Isomorphism theorem) and RS properly contains S, a contradiction to the fact that S is the p-subgroup with highest order in $N_G(R)$. So the intersection of any two Sylow p-subgroups in $N_G(R)$ contains R. Suppose some intersection of S_1 and S_2properly contains R then by Sylow theorem for G, there exist P_1 and P_2 in $Syl_p(G)$ that contain S_1 and S_2 respectively. Then its intersection in G properly contains R, so $P_1 = P_2 = P$. $P \cap N_G(R) = N_P(R)$ a p-group leading to $S_1 = S_2$. So the result follows. QED//

Dummit and Foote *Abstract Algebra*, section 6.2, exercise 13:

Let G be a group with more than one Sylow p-subgroup. Choose $P, Q \in Syl_p(G)$ such that $|P \cap Q|$ is maximal. Prove that $N_G(P \cap Q)$ has more than one Sylow p-subgroup, any two distinct Sylow p-subgroups intersect in $P \cap Q$, and $p \cdot q \cdot |P \cap Q|$ divides $|N_G(P \cap Q)|$ for some prime q other than p.

Proof: Note that since p-groups are nilpotent, $P \cap Q < N_P(P \cap Q)$ and $P \cap Q < N_Q(P \cap Q)$, so that $p \cdot |P \cap Q|$ divides $|N_G(P \cap Q)|$. Prove that $N_P(P \cap Q)$ and $N_Q(P \cap Q)$ are distinct Sylow p-subgroups of $N_G(P \cap Q)$. If $N_P(P \cap Q)$ is not a Sylow subgroup, then place it in one, and call this group P^*. This is a p-group in G, so place P^* in a Sylow p-subgroup P^{**}. Note that if $P^{**} = P$, then since $P^* \leq N_G(P \cap Q)$ we have $P^* \cap P = P^* \leq N_P(P \cap Q)$, a contradiction. Therefore P and P^{**} are distinct Sylow p-subgroups of G and $P \cap Q < N_P(P \cap Q) \leq P \cap P^{**}$, a contradiction by the maximality of $P \cap Q$. The case for $N_Q(P \cap Q) \in Syl_p(N_G(P \cap Q))$ is similar. Now prove that $N_P(P \cap Q) \neq N_Q(P \cap Q)$: Assuming the contrary, we have $P \cap Q < N_P(P \cap Q) \leq P \cap Q$, a clear impossibility.

Assume $N_G(P \cap Q)$ is a p-group, and thus place it in a Sylow p-subgroup of G, calling it M. If $M = P$, then $N_Q(P \cap Q) \leq P$, so that $N_Q(P \cap Q) \leq P \cap Q$, untenable. Therefore $M \neq P$ and $P \cap Q < N_P(P \cap Q) \leq M \cap P$, another contradiction. Therefore q divides $|N_G(P \cap Q)|$.

Finally, let $A, B \in Syl_p(N_G(P \cap Q))$ with $A \neq B$, and prove $A \cap B = P \cap Q$. ($\supseteq$) Let $P \cap Q \leq C$ for some Sylow p-subgroup of $N_G(P \cap Q)$ with $gCg^{-1} = A$ for some $g \in N_G(P \cap Q)$. We have $g(P \cap Q)g^{-1} = P \cap Q \leq A$. The case is parallel for $P \cap Q \leq B$. ($\subseteq$) A and B are p-subgroups of G, so let $A \leq D$ and $B \leq E$ for some $D, E \in Syl_p(G)$. Assume $D = E$: Since $A \neq B$ and $A, B \leq D$, we have $\langle A, B \rangle$ is a p-subgroup (because it is in D) properly containing A and B, a contradiction (since $\langle A, B \rangle \leq N_G(P \cap Q)$ and A and B are supposed to be Sylow in $N_G(P \cap Q)$). So $D \neq E$. We have $A \cap B \leq D \cap E$ so that $|A \cap B| \leq |D \cap E| \leq |P \cap Q|$ and now $A \cap B = P \cap Q$. $\square$

6.2.14

6.2.14.

$144 = 2^4 \times 3^2$

Suppose G is not simple then, $n_3 = 3k + 1$ dividing 16, and $k > 0$. Therefore, n_3 is either 4 or 16. In either case, $n_3 \not\equiv 1 (mod 3^2)$ so there are P, Q $\in Syl_3(G)$ such that $|P : P \cap Q| = 3$ (lemma 6.2.13). Let $R = P \cap Q$ then both P and Q are in $N_G(R)$ as P is the maximal subgroup in 3-groups P and Q (theorem in 6.1 about p-groups). So $|N_G(P)| = 3^2 m$ and $m \geq 4$ since the number of Sylow 3-groups in $N_G(P)$ is at least 2, congruent to 1 mod 3, and divides m. So $|G : N_G(P)| \leq \frac{16}{4} = 4$. That is, G has a subgroup of index k less than or equal to 4. By considering the translation action of left cosets created by that subgroups, we obtain an homomorphism from G into S_k. Since G is simple, and the action is transitive, the homomorphism must be injective and $|G| \mid |S_k| \leq 4! = 24$, a contradiction. So G is not simple. QED

$525 = 3 \times 5^2 \times 7$

Suppose G is not simple then, $n_5 = 5k + 1$ dividing 21, and $k > 0$. Therefore, $n_5 = 21 \not\equiv 1 (mod 5^2)$ so there are P, Q $\in Syl_5(G)$ such that $|P : P \cap Q| = 5$. Let $R = P \cap Q$ then both P and Q are in $N_G(R)$ as P is the maximal subgroup in 5-groups P and Q (theorem in 6.1 about p-groups). So $|N_G(P)| = 5^2 m$ and $m \geq 6$ since the number of Sylow 5-groups in $N_G(P)$ is at least 2, congruent to 1 mod 5, and divides m. So $|G : N_G(P)| \leq \frac{21}{6} < 4$. That is, G has a subgroup of index k less than 4. By considering the translation action of left cosets created by that subgroups, we obtain an homomorphism from G into S_k. Since G is simple, and the action is transitive, the homomorphism must be injective and $|G| \mid |S_k| < 4! = 24$, a contradiction. So G is not simple. QED

$2025 = 3^4 \times 5^2$
Suppose G is not simple then, $n_3 = 3k + 1$ dividing 25, and $k > 0$. Therefore, $n_3 = 25 \not\equiv 1(mod 3^2)$ so there are P, Q $\in Syl_3(G)$ such that $|P : P \cap Q| = 3$. Let $R = P \cap Q$ then both P and Q are in $N_G(R)$ as P is the maximal subgroup in 3-groups P and Q (theorem in 6.1 about p-groups). So $|N_G(P)| = 3^4 m$ and $m \geq 4$ since the number of Sylow 3-groups in $N_G(P)$ is at least 2, congruent to 1 mod 3, and divides m. So $|G : N_G(P)| \leq \frac{25}{4} < 7$. That is, G has a subgroup of index k less than or equal to 6. By considering the translation action of left cosets created by that subgroups, we obtain an homomorphism from G into S_k. Since G is simple, and the action is transitive, the homomorphism must be injective and $|G| \mid |S_k| \leq 6! = 720$, a contradiction. So G is not simple. QED
$3159 = 3^5 \times 13$
Suppose G is not simple then, $n_3 = 3k + 1$ dividing 13, and $k > 0$. Therefore, $n_3 = 13 \not\equiv 1(mod 3^2)$ so there are P, Q $\in Syl_3(G)$ such that $|P : P \cap Q| = 3$. Let $R = P \cap Q$ then both P and Q are in $N_G(R)$ as P is the maximal subgroup in 3-groups P and Q (theorem in 6.1 about p-groups). So $|N_G(P)| = 3^5 m$ and $m \geq 4$ since the number of Sylow 3-groups in $N_G(P)$ is at least 2, congruent to 1 mod 3, and divides m. So $|G : N_G(P)| \leq \frac{13}{4} < 4$. That is, G has a subgroup of index k less than 4. By considering the translation action of left cosets created by that subgroups, we obtain an homomorphism from G into S_k. Since G is simple, and the action is transitive, the homomorphism must be injective and $|G| \mid |S_k| < 4! = 24$, a contradiction. So G is not simple. QED

6.2.15

6.2.16

Search for Simplicity (6.2.16)

Dummit and Foote *Abstract Algebra*, section 6.2, exercise 16:

Prove there are no simple groups of odd composite order < 10,000.

Proof: I will record some difficult cases:

1575: Sylow analysis gives us $n_5 = 21$. Since $21 \neq 1 \mod 5^2$, we have $P_5 \cap Q_5$ of order 5 and due to index crunching we obtain $|N_G(P_5 \cap Q_5)| = 3 * 5^2$. But now $n_5(N_G(P_5 \cap Q_5)) = 1$, even though $P_5 \neq Q_5$ and $P_5, Q_5 \in Syl_5(N_G(P_5 \cap Q_5))$.

3465: Lemma 1: Let G be a group, let $P \in Syl_p(G)$ and assume $N_G(P)$ is cyclic. Then there are precisely $n_p \cdot \varphi(|N_G(P)|)$ elements of order $|N_G(P)|$ in G. Proof: Since $P \trianglelefteq N_G(P)$, we have distinct normalizers of Sylow p-subgroups for distinct Sylow p-subgroups, so that there are n_p distinct normalizers. As well, if $|x| = |N_G(P)|$, then for some $Q \in Syl_p(G)$ we have $Q \trianglelefteq \langle x \rangle$ so that $\langle x \rangle = N_G(Q)$, and now every element of such an order is contained in a normalizer. Since these normalizers are conjugate to one another and are thus cyclic as well, we have each normalizer contains $\varphi(|N_G(P)|)$ elements of the specified order, and since no two distinct normalizers share elements of this order, we have the lemma proven. □

Lemma 2: A group G of order $231 = 3 * 7 * 11$ has an element of order 33. Proof: We have $P_{11} \trianglelefteq G$, so that $P_3P_{11} \cong Z_{33}$ is a subgroup of G. □

By Sylow analysis on 3465, we obtain:

$$n_3 \in \{7, 55, 385\} \quad n_5 \in \{11, 21, 231\} \quad n_7 \in \{15, 99\} \quad n_{11} = 45$$

This reveals that $N_G(P_{11}) \cong Z_{77}$ (in particular, this implies G has no elements of order 33). By the first lemma, there are $45 * 60 = 2700$ elements of order 77 in G. By $n_{11} = 45$, we obtain 450 elements of order 11. Now, if $n_7 = 99$, this would produce 594 elements of order 7, which overloads the order of G. Therefore $n_7 = 15$, and now $|N_G(P_7)| = 231$ and contains an element of order 33 by the second lemma, a terminating contradiction.

9765: By Sylow analysis and index crunching, we obtain:

$$n_3 \in \{31, 217\} \quad n_5 \in \{31, 651\} \quad n_7 = 155 \quad n_{31} = 63$$

We have $|N_G(P_7)| = 3^2 * 7$. Now, if $n_5 = 31$, we have $|N_G(P_5)| = 3^2 * 5 * 7$, so that $P_7 \trianglelefteq P_5P_7$ and then $35 \mid |N_G(P_7)| = 63$, a contradiction. So $n_5 = 651$ and $N_G(P_5) \cong Z_{15}$, so that by lemma 1 we have 5208 elements of order 15. With Sylow, we obtain at least $5208 + 651 * 4 + 155 * 6 + 63 * 30 = 10,632$ elements in G, an impossibility. □

6.2.17

6.2.18

Dummit and Foote *Abstract Algebra*, section 6.2, exercises 18-20:
18. Prove $|G| = 36 \Rightarrow n_2 = 1 \vee n_3 = 1$.
19. Prove $|G| = 12 \ \wedge \nexists H(H \leq G \wedge |H| = 6) \Rightarrow G \cong A_4$.
20. Prove $|G| = 24 \ \wedge \nexists g(g \in G \wedge |g| = 6) \Rightarrow G \cong S_4$.

Proof: (18) Sylow analysis reveals:

$$n_2 \in \{3, 9\} \quad n_3 = 4$$

Let G act by left multiplication on the four cosets of $N_G(P_3) = P_3$; the kernel N of this action is the largest normal subgroup of G contained in P_3. Since $P_3 \not\trianglelefteq G$ and $N = 1$ allows G isomorphic passage into S_4 of order 24, we must have $|N| = 3$. We have $|G/N| = 12$, so there is either a normal Sylow 2-subgroup or a normal Sylow 3-subgroup of G/N. Assuming the latter, we have $K/N \trianglelefteq G/N$ is of order 3, so that its preimage K is of order 9 and normal in G, a contradiction. Therefore let $K/N \trianglelefteq G/N$ be of order 4 so that $K \trianglelefteq G$ is of order 12. It contains some Sylow 2-subgroup of G, and by its normality it contains all of them, so $n_2 = 3$. Let K act by left multiplication on the three cosets of P_3 it contains; once again, we must have a normal subgroup T of order 2 in K. This can only be the 2-core of K, which is characteristic in K, and now normal in G. We have TN is a normal subgroup of order 6, so that $P_3(TN)$ is a subgroup; since $P_3 \not\leq TN$ and $P_3 \cap TN = 1$ implies $P_3(TN)$ is a subgroup of order 54, we must have $|P_3 \cap TN| = 3$ and $P_3(TN)$ is a subgroup of order 18. This subgroup is normal by its index, contains a Sylow 3-subgroup and thus contains all of them, and yet Sylow purports $n_3 = 1$. □

6.2.19

(19) Since $G \ncong A_4$ by assumption, we have $n_3 = 1$. Take x of order 2 and we have $\langle x \rangle P_3$ is a subgroup of order 6. □

6.2.20

(20) We have:

$$n_2 \in \{1,3\} \quad n_3 \in \{1,4\}$$

If $n_3 = 4$, then letting G act on the cosets of P_3 allows isomorphic passage into S_4 so that by order $G \cong S_4$. In addition, assume $n_2 = 1$; then $G = P_2P_3 \cong P_2 \times P_3$. If $Z(P_2) = P_2$, then $Z(G) \cong Z(P_2) \times Z(P_3) = P_2 \times P_3$, so that G is abelian and the elements x and y of orders 2 and 3 respectively combine for a product xy of order 6. If $|Z(P_2)| = 2$ (the only other option for $Z(P_2)$), then $Z(P_2)\ \mathrm{char}\ P_2 \trianglelefteq G$ so that $Z(P_2) \trianglelefteq G$ and now $Z(P_2)P_3 \cong Z_6$. Ultimately, $n_2 = 3$. Since $3 \not\equiv 1 \mod 2^2$ we have $P_2 \cap Q_2$ of order 4; by exercise 13, we must have $N_G(P_2 \cap Q_2) = G$ so that $P_2 \cap Q_2 \trianglelefteq G$, and by 4.5.37 $P_2 \cap Q_2$ is contained in every Sylow 2-subgroup, so that the sum of the distinct elements of order 2, 4, and 8 can be explicitly calculated; there is the intersection point of order 4 minus the identity, and the three Sylow 3-subgroups that each provide 4 unique elements (lest the intersection between two distinct Sylow 2-subgroups be greater than 4, an impossibility), yielding 15 such elements. Comparing this with the following chart of possible orders of elements that can be determined thus far:

Order	# of elements
1	1
2	?
3	2
4	?
6	0
8	?
12	0
24	0

we invariably end up with only 18 elements of G, a contradiction. □

6.2.21

6.2.22

6.2.23

6.2.24

6.2.25

6.2.26

Groups of Order 168 (6.2.26)

Dummit and Foote *Abstract Algebra*, section 6.2, exercise 26:

Evaluate the validity of the following statement:

$$|G| = 168 \wedge \ n_7(G) > 1 \Rightarrow G \text{ is simple}$$

Proof: The statement is false. Let $Z_2^3 \rtimes Z_7$ denote the semidirect product afforded by a homomorphism of the generator of Z_7 into a generator of a cyclic Sylow 7-subgroup of $Aut(Z_2^3) \cong GL_3(Z_2)$ of order $168 = 2^3 * 3 * 7$. This implies $Z_7 \ntrianglelefteq Z_2^3 \rtimes Z_7$, so that $n_7(Z_7 \rtimes Z_2^3) > 1$. Now, observe the group $G = (Z_2^3 \rtimes Z_7) \times Z_3$ of order 168. We have the former group as a subgroup of this one, so that $n_7(G) > 1$. Furthermore, if $((a,b),c) \in P_3 \in Syl_3(G)$, then $((a,b),c)^3 = ((a,b)^3, c^3) = ((1,1),1)$, and since (a,b) is an element of the subgroup of order 56, we must have $(a,b) = (1,1)$ so that there are only $|Z_3| = 3$ distinct elements of G satisfying $x^3 = 1$, therefore $n_3(G) = 1$, $P_3 \trianglelefteq G$ and G is not simple. $\square$

6.2.27

6.2.28

The Millionaire (6.2.28)

Dummit and Foote *Abstract Algebra*, section 6.2, exercises 28:

Let G be simple and of order $3^3 * 7 * 13 * 409 = 1,004,913$. Calculate the number of Sylow p-subgroups for each prime dividing $|G|$.

Proof: Preliminary Sylow analysis shows:

$$n_3 \in \{7, 13, 91, 409, 2863, 5317, 37219\} \quad n_7 \in \{351, 47853\}$$

$$n_{13} \in \{27, 25767\} \quad n_{409} \in \{819\}$$

Removing the numbers that violate the index restrictions, we have all of them solved except for n_3. Assume $n_3 = 409$, and we have $|N_G(P_3)| = 3^3 * 7 * 13$, so for some P_7 we have P_3P_7 is a subgroup of $N_G(P_3)$, so that naturally $P_7 \trianglelefteq P_3P_7$, meaning $|P_3P_7| = 189 \mid |N_G(P_7)| = 21$, a contradiction. Assuming $n_3 = 5317$, we end up with the same contradiction as then $|N_G(P_3)| = 3^3 * 7$.

A brief digression: By counting the elements of order 7, 13, and 409, we obtain $930,474$ elements. If there is an element x of order 21, then $P_7 \trianglelefteq \langle x \rangle$ so that $\langle x \rangle = N_G(P_7)$ by order, so that by 6.2.16's first lemma there are $12 * 47853 = 574,236$ elements of order 21, overloading G.

Now assume $n_3 = 37219$, and since $37129 \not\equiv 1 \mod 3^2$, we have an order-$3^2$ intersection of two Sylow 3-subgroups $P_3 \cap Q_3$, whose normalizer is of order $3^3 * 7$, $3^3 * 13$, or $3^3 * 7 * 13$. If $3^3 * 7$, then by the above the only order the elements in this normalizer can take are 1, 7, and powers of 3. Sylow shows $n_3 = 7$ (by 6.2.13) and $n_7 = 1$, so that there are $3^3 * 7 - 6 = 183$ elements in the Sylow 3-subgroups. Without taking intersections into account, there is a maximum of $7 * 26 + 1 = 183$ elements possible, so that there is no intersection between Sylow 3-subgroups taking place, despite $P_3, Q_3 \leq N_G(P_3 \cap Q_3)$ and $P_3 \cap Q_3 \neq 1$, or 6.2.13 in general. If $3^3 * 13$ or $3^3 * 7 * 13$, the order of the normalizer forces only one Sylow 3-subgroup, despite once again $P_3, Q_3 \leq N_G(P_3 \cap Q_3)$ being distinct Sylow 3-subgroups. Therefore, $n_3 = 2863$ by default. □

6.2.29

6.2.30

6.3 A Word on Free Groups 215

6.3.1

Exercise 6.3.1 on page 220 (first half) Let F_1 and F_2 be free groups of finite rank. Prove that $F_1 \cong F_2$ if and only if they have the same rank.

Suppose F_1 and F_2 are free groups of the same rank, say $F_1 = F(X)$, $F_2 = F(Y)$, and we have set maps $\alpha\colon X \to Y$ and $\beta\colon Y \to X$ such that $\alpha\beta$ and $\beta\alpha$ are the identity on Y and X respectively. Then there exist homomorphisms $\theta\colon F(X) \to F(Y)$ such that $\theta(x) = \alpha(x)$ and $\phi\colon F(Y) \to F(X)$ such that $\phi(y) = \beta(y)$ for all $x \in X$ and $y \in Y$. Note that $\theta\phi\colon F(Y) \to F(Y)$ is a homomorphism such that $\theta\phi(y) = \alpha\beta(y) = y$ for all $y \in Y$. By uniqueness of homomorphisms, we see that $\theta\phi$ is the identity map on $F(Y)$. Similarly $\phi\theta$ is the identity map on $F(X)$. This proves that $F(X) \cong F(Y)$. We haven't used the hypothesis of finite rank in this part.

Conversely suppose $F_1 \cong F_2$, say $F_1 \cong F(X)$ and $F_2 \cong F(Y)$ where $|X| = r$ and $|Y| = s$, and that F_1 and F_2 have different rank. Without loss of generality $r > s$. Also we have an isomorphism $\theta\colon F(Y) \to F(X)$. Write $X = \{x_1, \ldots, x_r\}$ and $Y = \{y_1, \ldots, y_s\}$. By using the universal property for free groups, we may define an epimorphism $\alpha\colon F(X) \to \mathbb{Z}_2^r$ by $\alpha(x_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 is in the ith position. This yields an epimorphism $\beta = \alpha\theta\colon F(Y) \to \mathbb{Z}_2^r$. Therefore $\mathbb{Z}_2^r$ is generated by the s elements $\beta(y_i)$. Since $\mathbb{Z}_2^r$ is abelian and $\beta(y_i)$ has order 1 or 2, we deduce that every element of $\mathbb{Z}_2^r$ can be written in the form

$$(\beta(y_1))^{\varepsilon_1} \ldots (\beta(y_s))^{\varepsilon_s}$$

where $\varepsilon_i = 0$ or 1. We conclude that $|\mathbb{Z}_2^r| \leq 2^s$, which contradicts the fact that $|\mathbb{Z}_2^r| = 2^r$, and the proof is complete.

1. [In general, *if we assume the Axiom of Choice*, then F_1 and F_2 are isomorphic if, and only if, S_1 and S_2 have the same cardinality. [Of course, we don't need the Axiom of Choice for the finite case.]]

Let S_1 and S_2 be sets with the same cardinality that generate F_1 and F_2 respectively. Let then $\phi : S_1 \to S_2$ be a bijection. By the universal property of free groups there is a homomorphism $\Phi : F_1 \to F_2$.

We claim that Φ is an isomorphism. Indeed, if $x_1^{r_1} \cdots x_k^{r_k}$ is a reduced word, then $\Phi(x_1^{r_1} \cdots x_k^{r_k}) = \phi(x_1)^{r_1} \cdots \phi(x_k)^{r_k} \neq 1$, since the $\phi(x_i)$'s are distinct elements of S_2 [since ϕ is injective] and hence are free. So, Φ is injective.

Moreover, given $y_1^{s_1} \cdots y_k^{s_k} \in F_2$, with $y_i \in S_2$, we have that there are $x_i \in S_1$ such that $\Phi(x_i) = \phi(x_i) = y_i$ [since ϕ is onto], and hence $\Phi(x_1^{s_1} \cdots x_k^{s_k}) = y_1^{s_1} \cdots y_k^{s_k}$. Thus, Φ is onto.

Now suppose that S_1 and S_2 have different cardinality. Assume that $|S_1| \leq |S_2|$ [i.e., there is no surjective function from S_1 into S_2], but that $\phi : F_1 \to F_2$ is an isomorphism [where again $F_i \stackrel{\text{def}}{=} \langle S_i \rangle$].

Case 1: Assume S_1 and S_2 are finite, say $|S_1| = n < m = |S_2|$.

Suppose that $\phi : F_1 \to F_2$ is an isomorphism. Let F_i' be the commutator subgroup of F_i. We have then that $\phi(F_1') = F_2'$. Indeed, clearly $\phi(F_1') \subseteq F_2'$, since it is generated by commutators of F_2. Since ϕ is onto, then also all commutators of F_2 are in $\phi(F_1')$, and hence $F_2' \subseteq \phi(F_1')$.

Therefore, we have that $\bar{\phi} : F_1/F_1' \to F_2/F_2'$, defined by $\phi(x \cdot F_1') \stackrel{\text{def}}{=} \phi(x)F_2'$ is a well defined isomorphism. [The map $x \mapsto \phi(x) \mapsto \phi(x)F_2'$ is clearly a homomorphism, and by the above remark it's kernel is F_1'. Moreover, it is onto since ϕ is onto, making it an isomorphism.]

By Problem 11, we have that $F_1/F_1' \cong \mathbb{Z}^n$ and $F_2/F_2' \cong \mathbb{Z}^m$. Hence, it suffices to show that $\mathbb{Z}^n \ncong \mathbb{Z}^m$. For that, let $\psi : \mathbb{Z}^m \to \mathbb{Z}^n$ an isomorphism [e.g., $\bar{\phi}^{-1}$ from above]. Let $e_i \in \mathbb{Z}^m$, for $i \in \{1, \ldots, m\}$, be defined as the vector with 1 in the i-th coordinate and zeros everywhere else. By hypothesis, ψ must be injective. But, $\psi(e_i)$ is a linearly dependent set *over* $\mathbb{Q}$, since $m > n$. [So, we are switching of view to see $\psi(e_i) \in \mathbb{Q}^n$.] Let $\sum_{i=1}^m k_i \psi(e_i) = 0$, with $k_i \in \mathbb{Q}$, not all zero. By clearing denominators, we can assume $k_i \in \mathbb{Z}$, and hence $\psi(k_1, \ldots, k_m) = 0$, but $(k_1, \ldots, k_m) \neq 0$, contradicting the assumption that ψ is injective.

Hence, $F_1 \ncong F_2$.

Case 2: Assume $|S_1| = n < \infty$, but and $|S_2| = \infty$. [No need of Axiom of Choice in this case either.]

Suppose that $\phi : F_1 \to F_2$ is an isomorphism, and therefore, F_2 is generated by $\phi(S_1)$. If $S_1\{a_1, \ldots, a_n\}$, then there are finitely many elements of S_2 that generate the $\phi(a_i)$'s [since each is generated by finitely many elements of S_2], say $S \stackrel{\text{def}}{=} \{b_1, \ldots, b_m\} \subseteq S_2$.

Since $|S_2| = \infty$, there is some $y \in S_2$ which is not in S. Also, since the $\phi(S_1)$ generates F_2, and S generates $\phi(S_1)$, we have that S generates F_2. Thus, in particular y is generated by elements of S. But this contradicts the fact that S_2 is free. [Note $S \subseteq S_2$ and $y \in S_2 - S$.]

Hence, $F_1 \ncong F_2$.

Case 2: Assume that S_1 is infinite [and thus so is S_2] and that the Axiom of Choice holds.

Since ϕ is onto, we have that $\phi(S_1)$ generates F_2.

On the other hand, $|\phi(S_1)| = |S_1|$ since ϕ is injective. But then, each element $y \in S_2$ is generated by finitely many elements of $\phi(S_1)$, say by $S_y \subseteq \phi(S_1)$. Hence, the set

$$\mathcal{S} \stackrel{\text{def}}{=} \bigcup_{y \in S_2} S_y$$

generates all elements of S_2, and hence, it generates F_2. On the other hand, since $|S_1| = \infty$ and $|S_y| < \infty$, we have [assuming the Axiom of Choice]

$$|\mathcal{S}| \leq \left| \bigcup_{n=1}^{\infty} S_1^n \right| = |S_1|\,,$$

and so $|\mathcal{S}| = |S_1|$. [To see this equality of cardinalities above, we need to do some *cardinality arithmetic*: we have

$$\left| \bigcup_{n=1}^{\infty} S_1^n \right| = \sum_{n \in \mathbb{N}} |S_1^n| = \sum_{n \in \mathbb{N}} |S_1| = \aleph_0 \cdot |S_1| = |S_1|\,.$$

Check, for instance, R. Stoll's *"Set Theory and Logic"*, Theorems 2.9.4 and 2.9.5.]

Therefore, since $|\mathcal{S}| \leq |S_1| < |S_2|$, there exists $y \in S_2 - \mathcal{S}$. But since F_2 is generated by $\mathcal{S}$, there would be elements in S_2 is generated by other elements of S_2. But this contradicts the fact that S_2 is free in F_2.

Hence, $F_1 \ncong F_2$.

Free Groups and Rank (6.3.1)

Dummit and Foote *Abstract Algebra*, section 6.3, exercise 1:

Let $\langle a_1, \ldots, a_n \rangle = F_1$ and $\langle b_1, \ldots, b_m \rangle = F_2$ be free groups. Prove that $F_1 \cong F_2$ if and only if $n = m$. Consider the case when the two's ranks are infinite, as well.

Proof: ($\Rightarrow$) Assume $n \neq m$, and generally n is of smaller cardinality than m. Let φ be the isomorphism from F_1 to F_2. For an arbitrary element $x \in F_2$, we have $x = \varphi(a_1^{k_1} \ldots a_n^{k_r}) = \varphi(a_1)^{k_1} \ldots \varphi(a_r)^{k_r}$, so that F_2 is generated by a number of elements of smaller than or equal cardinality to those of F_1, a contradiction. ($\Leftarrow$) Let there be a bijection between the generators of F_1 and the generators of F_2, operating on the index by π. Define a mapping $\varphi : F_1 \to F_2$ by $\varphi(a_i) = b_{\pi(i)}$ and homomorphically extend it. For any two generators in F_1, we have:

$$\varphi(a_i)^x = \varphi(a_j)^y \Rightarrow b_{\pi(i)}^x = b_{\pi(j)}^y \Rightarrow \pi(i) = \pi(j) \Rightarrow i = j \Rightarrow a_i = a_j$$

Now observe:

$$\varphi(a_1^{k_1} \ldots a_r^{k_r}) = \varphi(a_1^{j_1} \ldots a_s^{j_s}) \Rightarrow b_{\pi(1)}^{k_1} \ldots b_{\pi(r)}^{k_r} = b_{\pi(1)}^{j_1} \ldots b_{\pi(s)}^{j_r} \Rightarrow \forall i [b_{\pi(i)}^{k_i} = b_{\pi(i)}^{j_i}]$$

$$\Rightarrow \forall i [\varphi(a_i)^{k_i} = \varphi(a_i)^{j_i}] \Rightarrow \forall i [a_i^{k_i} = a_i^{j_i}] \Rightarrow a\pi(1)^{k_1} \ldots a_{\pi(r)}^{k_r} = a_1^{j_1} \ldots a_s^{j_s}$$

So that φ is an injective homomorphism. Similarly, we can construct an injective homomorphism from F_2 into F_1, therefore providing an isomorphism. This argument did not assume the finiteness of rank, merely the equivalency of cardinality, so is therefore applicable to infinite groups as well. □

6.3.2

Exercise 6.3.2 on page 220 Prove that if $|S| > 1$, then $F(S)$ is nonabelian.

Let $x, y \in S$ be distinct. Then $xy \neq xy$, hence $F(S)$ is nonabelian.

6.3.3

3. Let $F \stackrel{\text{def}}{=} \langle a, b \rangle = \langle a, b \ : \ \rangle$ [i.e., the free group in two elements], and F' be its commutator subgroup.

Let ϕ be the homomorphism $\phi : F \to \mathbb{Z} \times \mathbb{Z}$, defined by $\phi(a) = (1, 0)$, $\phi(b) = (0, 1)$. [This is a well defined homomorphism by the universal property of free groups.]

Claim: $F' = \ker \phi$, and so, $a^{m_1} b^{n_1} \cdots a^{m_k} b^{n_k} \in F'$ if, and only if, $\sum_{r=1}^{k} m_r = \sum_{r=1}^{k} n_r = 0$.

Proof. Since ϕ is clearly onto, we have $F/\ker \phi \cong \mathbb{Z} \times \mathbb{Z}$, which is abelian. Hence, $F' \subseteq \ker \phi$.

But $F/F' \cong \mathbb{Z} \times \mathbb{Z}$ by Problem 11. We then have that $F/\ker \phi \cong (F/F')/(\ker \phi/F')$, and so $\mathbb{Z} \times \mathbb{Z}$ must be a quotient of one $\mathbb{Z} \times \mathbb{Z}$ itself.

But if $H \leq \mathbb{Z} \times \mathbb{Z}$ with $(\mathbb{Z} \times \mathbb{Z})/H \cong \mathbb{Z} \times \mathbb{Z}$, then $H = \{(0, 0)\}$. Indeed, if $(a, b) \in H - (0, 0)$ then: if $\gcd(a, b) = d > 1$, and $(a/d, b/d) \notin H$, then we have that $(\mathbb{Z} \times \mathbb{Z})/H$ has a non-zero element of finite order, namely $((a/d, b/d) + H)$, and so $(\mathbb{Z} \times \mathbb{Z})/H \ncong \mathbb{Z} \times \mathbb{Z}$. If $(a/d, b/d) \in H$ or $d = 1$, we may assume that $\gcd(a, b) = 1$. In this case, we have that there are $c, d \in \mathbb{Z}$ such that $ac - bd = 1$. Therefore, (a, b) and (c, d) generate $\mathbb{Z} \times \mathbb{Z}$: given $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, we have

$$(x, y) = (dx - cy)(a, b) + (-bx + ay)(c, d).$$

But in that case, $(\mathbb{Z} \times \mathbb{Z})/H$ is generated by a single element, namely $((c, d) + H)$, and therefore cannot be isomorphic to $\mathbb{Z} \times \mathbb{Z}$.

Thus, $F' = \ker \phi$.

□

Claim: Let $\{x, y\} = \{a, b\}$. Then, for $k \geq 1$:

$$x^{m_1} y^{n_1} \cdots x^{m_k} y^{n_k} = \left(\prod_{i=1}^{k-1} [x^{M_i}, y^{N_i}][y^{N_i}, x^{M_{i+1}}] \right) [x^{M_k}, y^{N_k}] y^{N_k} x^{M_k}, \tag{4}$$

$$x^{m_1} y^{n_1} \cdots x^{m_k} y^{n_k} x^{m_{k+1}} = \left(\prod_{i=1}^{k-1} [x^{M_i}, y^{N_i}][y^{N_i}, x^{M_{i+1}}] \right) [x^{M_k}, y^{N_k}] y^{N_k} x^{M_{k+1}}, \tag{5}$$

where $M_i \stackrel{\text{def}}{=} \sum_{r=1}^{i} m_r$ and $N_i \stackrel{\text{def}}{=} \sum_{r=1}^{i} n_r$.

Proof. This can be easily proved by induction. For $k = 1$, observe that $M_1 = m_1$ and $N_1 = n_1$, and then:

$$x_1^{m_1} y_1^{n_1} = [x^{M_1}, y^{N_1}] y^{N_1} x^{M_1}.$$

Hence, (4) holds and since $M_1 + m_2 = M_2$, formula (5) also holds.

For the second step, just observe that,

$$\begin{aligned} y^{N_k} x^{M_k} x^{m_{k+1}} y^{n_{k+1}} &= y^{N_k} x^{M_{k+1}} y^{N_{k+1} - N_k} \\ &= [y^{N_k}, x^{M_{k+1}}][x^{M_{k+1}}, y^{N_{k+1}}] y^{N_{k+1}} x^{M_{k+1}}, \end{aligned}$$

and $x^{M_{k+1}} x^{m_{k+2}} = x^{M_{k+2}}$.

□

Claim: We have that $F' = \langle [a^m, b^n] \ : \ m, n \in \mathbb{Z} \rangle$. [Note that $[b^n, a^m] = [a^m, b^n]^{-1}$.]

Proof. Let $c \in F'$. Then, by our first claim, either

$$c = x^{m_1} y^{n_1} \cdots x^{m_k} y^{n_k}, \quad \text{with } M_k = \sum_{r=1}^{k} m_r = N_k = \sum_{r=1}^{k} n_r = 0,$$

or,

$$c = x^{m_1} y^{n_1} \cdots x^{m_k} y^{n_k} x^{m_{k+1}}, \quad \text{with } M_{k+1} = \sum_{r=1}^{k+1} m_r = N_k = \sum_{r=1}^{k} n_r = 0,$$

where $\{x, y\} = \{a, b\}$.

By our previous claim, we have that, in either case,

$$c = \left(\prod_{i=1}^{k-1} [x^{M_i}, y^{N_i}][y^{N_i}, x^{M_{i+1}}] \right).$$

[Note: some of the commutators in the above product may be equal to one, when either M_r or N_r is zero.]

□

Claim: Let $c_1 c_2 \cdots c_k \in F$, where $c_i = [a^{m_i}, b^{n_i}] \neq 1$ or $c_i = [b^{n_i}, a^{m_i}] \neq 1$, with $c_{i+1} \neq c_i^{-1}$. Then, if $c_1 = [x^{m_1}, y^{n_1}]$ and $c_k = [w^{m_k}, z^{n_k}]$, where $\{x, y\} = \{w, z\} = \{a, b\}$, then the *reduced* expansion of $c_1 c_2 \cdots c_k$ in F [i.e, after all possible cancellations] has the form

$$c_1 c_2 \cdots c_k = x^{m_1} y^{n_1} x^r \cdots z^s w^{-m_k} z^{-n_k}, \quad \text{with } r, s \neq 0.$$

In particular, if $k \geq 1$ [and with the restrictions above], then $c_1 \cdots c_k$ is not equal to 1.

Proof. We proceed again by induction on k. The case $k = 1$ is trivial [with $r = -m_1 \neq 0$ and $s = n_1 \neq 0$].

Suppose it's now true for k and consider $c_1 c_2 \cdots c_k c_{k+1}$. If $c_{k+1} = [w^{m_{k+1}}, z^{n_{k+1}}]$, then there can be no cancellation in the end of this new reduced word, i.e.,

$$c_1 c_2 \cdots c_k c_{k+1} = x^{m_1} y^{n_1} x^r \cdots z^s w^{-m_k} z^{-n_k} w^{m_{k+1}} z^{n_{k+1}} w^{-m_{k+1}} z^{-n_{k+1}}.$$

If $c_{k+1} = [z^{n_{k+1}}, w^{m_{k+1}}]$, then there we consider two cases: if $n_{k+1} \neq n_k$, then,

$$c_1 c_2 \cdots c_k c_{k+1} = x^{m_1} y^{n_1} x^r \cdots z^s w^{-m_k} z^{n_{k+1}-n_k} w^{m_{k+1}} z^{-n_{k+1}} w^{-m_{k+1}},$$

and since $n_{k+1} - n_k \neq 0$, there is no other cancellation, and we are done. On the other hand, if $n_{k+1} = n_k$, then $m_{k+1} \neq m_k$ [since $c_{k+1} \neq c_k^{-1}$], and we have:

$$c_1 c_2 \cdots c_k c_{k+1} = x^{m_1} y^{n_1} x^r \cdots z^s w^{m_{k+1}-m_k} z^{-n_{k+1}} w^{-m_{k+1}},$$

and so the statement still holds [since $m_{k+1} - m_k \neq 0$].

□

Claim: The set $\{[a^m, b^n] \ : \ m, n \in \mathbb{Z}\}$ is *free*, i.e., no nontrivial *reduced* word of elements in this set [i.e., a product of $c_1 \cdots c_k$, where either c_i or c_i^{-1} is in this set, with $k \geq 1$, and $c_{i+1} \neq c_i, c_i^{-1}$] is equal to 1. Therefore, this set gives a free basis for F' [since it generates F' by a previous claim].

Proof. This is an easy consequence of the previous claim, since the reduced words will have the form of the $c_1 \cdots c_k$ in the statement, and hence different from 1 for $k > 1$.

□

Finally, we can prove the statement. Just observe that by the above, F' is isomorphic to a free group in infinite [but countably many] elements. If F' is also generated by a finite set, then it would also be isomorphic to a free group in finitely many elements. But, by Problem 1, this cannot happen.

6.3.4

6.3.4

Suppose w is the word of finite order h. Since w can be written in reduced form as $x_1 ... x_n$, w can also be written in the form aba^{-1} for b is in reduced form and furthermore, the last term in b is not the inverse of the first term (a can be chosen to be the identity). Then $1 = w^h = ab^h a^{-1}$ so $b^h = 1$. But b^h is a reduced word by the condition on its first and last term. So $b^h = 1$ iff $b = 1$ or w is the identity elemement. Thus every nonidentity element of a free group is of infinite order. QED

6.3.5

Exercise 6.3.5 on page 220 Establish a finite presentation for A_4 using 2 generators.

Let F denote the free group on $\{x,y\}$, let $a = (1\ 2)(3\ 4)$, $b = (1\ 2\ 3)$, and define $\theta : F \to A_4$ by $\theta x = a$, $\theta y = b$. Let $K = \ker\theta$. It is easy to check that $\langle a,b\rangle = A_4$. Indeed by Lagrange's theorem $6 \big| |\langle a,b\rangle| \big| 12$, so if $\langle a,b\rangle \neq A_4$, then $|\langle a,b\rangle| = 6$. But a group of order 6 has a unique subgroup of order 3, so has exactly 2 elements of order 3. Since b, b^2, aba are three distinct elements of order 3, we have a contradiction. Thus $\langle a,b\rangle = A_4$ as asserted and we conclude that θ is onto. Therefore $F/K \cong A_4$ by the fundamental homomorphism theorem.

Next note that $\theta x^2 = \theta y^3 = \theta(xy)^3 = 1$. In view of this, we will try $x^2, y^3, (xy)^3$ for our set of relators. Let N denote the normal closure of $\{x^2, y^3, (xy)^3\}$ in F. Then $\langle x,y \mid x^2 = 1,\ y^3 = 1,\ (xy)^3 = 1\rangle$ is by definition isomorphic to F/N. We want to show that $F/N \cong A_4$, that is $F/N \cong F/K$. Since $x^2, y^3, (xy)^3 \in K$, we certainly have $N \subseteq K$. We want to show equality, and to do this it will be sufficient to show that $|F/N| \leq 12$, because $|F/K| = 12$.

Let us work in F/N, or equivalently in F modulo N. We claim that every element of F modulo N can be written in the form $x^a y^b x^c$, where $a, c = 0$ or 1 and $b = 0, 1$ or 2. If not, then either $yxy^b x$ or $xy^b xy$ cannot be written in this form, where $b = 1$ or 2. However from $(xy)^3 = 1$, we obtain using $yxy = xy^{-1}x = xy^2x$, and then going through the 4 possibilities, we see that this is not the case. We conclude that F/N has at most $2 * 3 * 2 = 12$ elements and consequently $N = K$. Therefore a presentation for A_4 with 2 generators is $\langle x,y \mid x^2 = 1,\ y^3 = 1,\ (xy)^3 = 1\rangle$.

6.3.6

Exercise 6.3.6 on page 220 Establish a finite presentation for S_4 using 2 generators.

We follow similar steps to the previous problem; we let $a = (1\ 4\ 3\ 2)$ and $b = (1\ 2\ 3)$. Then $ab = (3\ 4)$, so $a^4 = b^3 = (ab)^2 = 1$. Also $\langle a,b\rangle = S_4$; one way to see this is to note that $\langle a^2,b\rangle = A_4$ by the same argument as the previous problem, and $a \notin A_4$. Let F denote the free group on x,y, and define $\theta : F \to S_4$ by $\theta x = a$, $\theta y = b$. Then θ is onto and $\theta x^4 = \theta y^3 = \theta(xy)^2 = 1$, so our proposed presentation is going to be $\langle x,y \mid x^4 = 1,\ y^3 = 1,\ (xy)^2 = 1\rangle$. Let $K = \ker\theta$, let $R = \{x^4, y^3, (xy)^2\}$ and let N denote the normal closure of R in F. Obviously $N \subseteq K$, and we need to prove $N = K$ because then $F/N \cong S_4$. Since $|F/K| = |S_4| = 24$, it will be sufficient to show that $|F/N| \leq 24$. We will in fact show that every element of F modulo N can be written in the form $x^a y^b x^c$ where $a = 0,2$, $b = 0,1,2$, $c = 0,1,2,3$; this will show that we have at most $2*3*4$ elements. To establish this, it will be sufficient to show that if we multiply $x^a y^b x^c$ on the left or right by x or y, then we can use the relations to put it back in the same form. This is easily done by using $xyx = y^2$ (derived from $(xy)^2 = 1$). For example, $x^2y^2xy = x^2yx^3$.

6.3.7

Presentation of the Quaternion Group (6.3.7)

Dummit and Foote *Abstract Algebra*, section 6.3, exercise 7:

Prove the following is a valid presentation:

$$Q_8 = \langle\ a,b\ \mid\ a^2 = b^2,\ a^{-1}ba = b^{-1}\ \rangle$$

Proof: By the first, we have $a^2b^{-2} = 1$. However, by the second, we also have $a^2b^{-2} = a^2(a^{-1}ba)(a^{-1}ba) = ab^2a$, so that $ab^2a = 1$, then $a^4 = 1$. Now, $a^2 = b^2 \Rightarrow a^4 = 1 = b^4$.

Prove by induction that $b^k a = ab^{-k}$. The case holds for $k = 1$ by the presentation, and $b^{k+1}a = bb^k a = bab^{-k} = ab^{-1}b^{-k} = ab^{-(k+1)}$. By extension, $ab^k = b^{-k}a$. We can see by repeated multiplication the left by a, that generally $a^i b^k = b^{\pm k}a^i$.

Attempt to observe any element with a reduced width n greater than 2, necessarily in either the form $\ldots a^{e_{n-2}}b^{e_{n-1}}a^{e_n} = \ldots a^{e_{n-2}+e_n}b^{\pm e_{n-1}}$ or $\ldots b^{e_{n-2}}a^{e_{n-1}}b^{e_n} = \ldots b^{e_{n-2}\pm e_n}a^{e_{n-1}}$, a contradiction in any case. So every element can be reduced to the form $a^x b^y$ or $b^x a^y$ (with $0 \leq x,y \leq 3$), the latter of which can be ignored as $b^x a^y = a^y b^{\pm x}$. Using the relations we have been given and have established, we can easily establish equivalency classes among these sixteen candidates to provide a maximum of eight distinct elements (e.g. $ab^3 = aa^2b = a^3b$). Since $i,j \in Q_8$ fulfill the relations presented above for a,b and $\langle\ i,j\ \rangle = Q_8$, we have the presentation validated. □

6.3.8

6.3.9

6.3.10

6.3.11

11. [I'll do this one first to use it in the others.] In order to be able to define $\Phi(s) \stackrel{\text{def}}{=} \phi(s)$ and extend it multiplicatively to a homomorphism, all we need to do it to check that all relations of $A(S)$ are compatible with ϕ.

In this case, we need to show that for all $s, t \in S$, we have $\Phi([s,t]) = \Phi(1)$. But, since G is abelian, we have $\Phi([s,t]) = \Phi(sts^{-1}t^{-1}) = \phi(s)\phi(t)\phi(s)^1\phi(t)^{-1} = 1 = \Phi(1)$.

Now, if $S = \{s_1, \ldots, s_n\}$, then $A(S)$ is a finitely generated abelian group with n generators. Thus, by the Fundamental Theorem of Finitely Generated Abelian Groups, we have that $A(S) \cong T \times \mathbb{Z}^m$, where $T \cong Z_{n_1} \times \cdots Z_{n_k}$, and $k + m \leq n$.

But, by the universal property, there is a homomorphism from $A(S)$ *onto* $\mathbb{Z}^n$, by mapping s_i to the element of $\mathbb{Z}^n$ with 1 in the i-th coordinate and 0's at all other coordinates. Hence, the only possibility is that $A(S) \cong \mathbb{Z}^n$. [Note that since $\mathbb{Z}^n$ has no torsion, we would have that any torsion of $A(S)$ would be mapped to zero, and hence we would need $m = n$ to be onto, and therefore there can be no torsion in $A(S)$.]

6.3.12

6.3.12

Formulate the notion: A free nilpotent group on S of nilpotence class c is described by the presentation: $N_{S,c} =< S \mid R >$ for R contains all the word of the form: $[[...[x_1, x_2],...], x_{c+1}]$ with $x_i \in S$. Another equivalent notion is to define $N_{S,c} = F(S)/F_c(S)$ with F_c the c-th term in the lower central series.
Universal mapping property: Let G be a nilpotent group of class less then or equal c, and $\varphi : S \to G$ a set map and $\iota : S \to N_{S,c}$ the inclusion map. Then there is a unique group homomorphism $\phi : N_{S,c} \to G$ such that $\phi\iota = \varphi$
Proof of the UMP: If G is a nilpotent class of nilpotent class less then or equal c then $G_c = 1$. Thus the identity $[[...[x_1, x_2],...], x_{c+1}] = 1$ holds with $x_i \in G$.
By the UMP for presentation, there is a unique homomorphism $\Phi : F(S) \to G$ that extends the set map φ ($R \leq Ker(\Phi)$ so the normal closure of R in F(S) is also contained in the kernel of Φ as the kernel is itself a normal group. QED

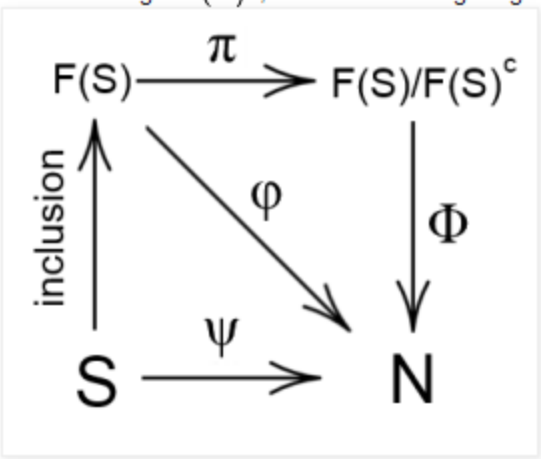
Proof: Let N be any group of nilpotence class $\leq c$ and let $\psi : S \to N$ be a set map with $G = \langle \operatorname{img} \psi \rangle$. We have a unique homomorphism $\varphi : F(S) \to N$ (fixing S) so that $F(S)/\ker \varphi \cong G$. We prove that there is a unique homomorphism $\Phi : F(S)/F(S)^c \to N$ such that $\Phi \mid_{\pi(S)} = \psi$ (where π is the natural homomorphism from $F(S)$ to $F(S)/F(S)^c$). Assume $F(S)^c \not\leq \ker \varphi$; we then have a contradiction:

$$G^c \cong (F(S)/\ker \varphi)^c = F(S)^c/\ker \varphi \neq 1$$

Therefore there is the desired homomorphism afforded by:

$$(F(S)/F(S)^c)/(\ker \varphi/F(S)^c) \cong F(S)/\ker \varphi \cong G$$

Assume $\Phi_1 \neq \Phi_2$ are two homomorphisms from $F(S)/F(S)^c$ to N fixing $\pi(S)$; then $\Phi_1 \circ \pi \neq \Phi_2 \circ \pi$ are two homomorphisms from $F(S)$ to G fixing S, a contradiction. We thus have $\ker \varphi$ factors through $F(S)^c$, and the following diagram commutes:



□

Note that this theorem can be paralleled to produce a similar result regarding a free solvable group on a set S.

6.3.13

6.3.13

Suppose there is such a nilpotent group N generated by two elements, then denote its nilpotence class c. Since every nilpotent group K which is generated by 2 elements is a homomorphic image, the homomorphism from N to K is surjective. Therefore, any commutator in K is the image of a commutator in N; and hence, any term in the lower central series of K is the image of a corresponding term in the lower central series of N. Since N has nilpotence class c, the lower central series terminates (goes to the identity) at the c-th term. Therefore, the lower central series of K must also terminate before or at the c-th term. Thus K has nilpotence class less than or equal c. (1)

Now we show that a D_{2^n} is a nilpotent group of class n-1 by induction. It certainly trues for $n = 1$. Suppose it is true for D_{2^k}. Consider $D_{2^{k+1}}$. Using the notation as in section 1.2, it is easy to see that $Z(D_{2^{k+1}}) = (1, r^{2^{k-1}})$ and the list $(r^i, r^{2^{k-1}+i}), (sr^i, sr^{2^{k-1}+i})$ for $0 \leq i < 2^{k-1}$ exhausts all coset with respect to the center. So it is straightforward calculation to show that $D_{2^{k+1}}/Z(D_{2^{k+1}}) \cong D_{2^k}$. Then we can apply the induction hypothesis to conclude the claim.

Certainly a finite dihedral group is generated by 2 elements and the above claim shows that the nilpotence class can be as large as we want. That contradicts (1) and leads the priori assumption to absurdity. So there does not exist such a group N. QED

6.3.14