Solutions for Homework Assignment 5

Page 154, Problem 2. Every element of \( \mathbb{C}^* \) can be written uniquely in the form \( a + bi \), where \( a, b \in \mathbb{R} \), not both equal to 0. The fact that \( a \) and \( b \) are not both 0 is equivalent to the inequality \( a^2 + b^2 > 0 \). Let

\[
H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R}, \text{ and } a^2 + b^2 > 0 \right\}.
\]

For \( a, b \in \mathbb{R} \), the condition \( a^2 + b^2 > 0 \) means that \( a^2 + b^2 \neq 0 \), which in turn means that the determinant of any matrix in \( H \) is nonzero. Hence \( H \) is a subset of \( GL_2(\mathbb{R}) \). We will see that it is a subgroup as a consequence of the proof below.

Define a map \( \varphi : \mathbb{C}^* \to H \) as follows:

\[
\varphi(a + bi) \rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.
\]

for all \( a + bi \in \mathbb{C}^* \). The above remarks make it clear that \( \varphi \) is one-to-one and onto. Thus, \( \varphi \) is a bijective map from \( \mathbb{C}^* \) to \( H \). We now show that \( \varphi \) is a homomorphism. Since \( \varphi \) is bijective, it follows that \( \varphi \) is indeed an isomorphism.

Suppose that \( a + bi \) and \( c + di \) are elements of \( \mathbb{C}^* \). Then

\[
\varphi((a + bi)(c + di)) = \varphi((ac - bd) + (ad + bc)i) = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix}.
\]

On the other hand, we have

\[
\varphi(a + bi)\varphi(c + di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix},
\]

where the second equality is simply matrix multiplication in \( GL_2(\mathbb{R}) \). It is the operation defining the group \( GL_2(\mathbb{R}) \).

Thus, we see that if \( a + bi \) and \( c + di \) are elements of \( \mathbb{C}^* \), then

\[
\varphi((a + bi)(c + di)) = \varphi(a + bi)\varphi(c + di)
\]

and hence \( \varphi \) is indeed a homomorphism from \( \mathbb{C}^* \) to \( H \). We have proved that \( \mathbb{C}^* \) and \( H \) are isomorphic.
Page 154, Problem 3. The groups $U(8)$ and $\mathbb{Z}_4$ are not isomorphic. The reason is that $\mathbb{Z}_4$ is a cyclic group of order 4 and hence has an element of order 4. In contrast, every element of $U(8)$ has order 1 or 2. The identity element is $1 + 8\mathbb{Z}$ and has order 1. The other three elements of $U(8)$ are $3 + 8\mathbb{Z}$, $5 + 8\mathbb{Z}$, and $7 + 8\mathbb{Z}$, and satisfy

$$(3 + 8\mathbb{Z})^2 = 1 + 8\mathbb{Z}, \quad (5 + 8\mathbb{Z})^2 = 1 + 8\mathbb{Z}, \quad (7 + 8\mathbb{Z})^2 = 1 + 8\mathbb{Z}$$

and hence have order 2 (since their orders aren’t equal to 1). Therefore, $U(8)$ has no element of order 4. Therefore, since an isomorphism preserves the order of elements, it follows that $U(8)$ is not isomorphic to $\mathbb{Z}_4$.

Page 154, Problem 9. Let $G = \{ r \in \mathbb{R} \mid r \neq -1 \}$. We define an operation on $G$ by

$$a \ast b = a + b + ab$$

for all $a, b \in G$. Note that $G$ is a group. This was proved in problem set 1. Define a map $\varphi : G \to \mathbb{R}^*$ by

$$\varphi(a) = 1 + a$$

Since $a \neq -1$ means that $1 + a \neq 0$, it is clear that $\varphi$ is a bijective map from $G$ to $\mathbb{R}^*$. Furthermore, we have

$$\varphi(a \ast b) = \varphi(a + b + ab) = 1 + a + b + ab = (1 + a)(1 + b) = \varphi(a)\varphi(b).$$

Hence $\varphi$ is a homomorphism. Therefore, $\varphi$ is indeed an isomorphism from $G$ to $\mathbb{R}^*$ and so those two groups are indeed isomorphic.

Page 156, Problem 24. No such group exists. To see this, suppose that $G$ is an abelian group and that $|G| = 51$. We proved in class (using Problem C below) that if $G$ is a finite abelian group and $p$ is a prime dividing $|G|$, then $G$ has at least one element of order $p$. Applying this to the case where $|G| = 51$, it follows that $G$ has at least one element $a$ of order 3 and at least one element $b$ of order 17. Let $c = ab$, an element of $G$.

We will prove that $c$ has order 51. It follows that $\langle c \rangle$ is a subgroup of $G$ of order 51 and hence we must have $G = \langle c \rangle$. This implies that $G$ is cyclic. Since $a$ has order 3 and $3|51$, it follows that $a^{51} = e$, where $e$ denotes the identity element of $G$. Since $b$ has order 17 and $17|51$, it follows that $b^{51} = e$. To see that $c$ has order 51, we use the fact that $G$ is abelian. We have

$$c^{51} = (ab)^{51} = a^{51}b^{51} = ee = e$$
and therefore $|c|$ divides 51. Thus $|c| \in \{1, 3, 17, 51\}$. On the other hand,

$$c^3 = a^3b^3 = eb^3 = b^3 \neq e, \quad c^{17} = a^{17}b^{17} = a^{17}e = a^{17} \neq e.$$  

We have used the facts that $|b| = 17$ does not divide 3, and $|a| = 3$ does not divide 17, respectively. It follows that $|c|$ does not divide 3 and $|c|$ does not divide 17. Therefore, the only possibility is that $|c| = 51$.

As pointed out above, the fact that $|c| = 51$ implies that $G$ is a cyclic group.

**Page 156, Problem 25.** A non-cyclic abelian group $G$ of order 52 does indeed exist. Let $A$ be the Klein 4-group. Thus, $|A| = 4$ and every element of $A$ has order 1 or 2. Thus, $a^2 = e$ for all $a \in A$, where $e$ is the identity element in $A$. Let $B$ be a cyclic group of order 13. Let $f$ be the identity element in $B$. Then $b^{13} = f$ for all $b \in B$.

Let $G = A \times B$. Then $|G| = |A||B| = 4 \cdot 13 = 52$. The identity element in the group $G$ is $(e, f)$. Consider an element $g \in G$. Then $g = (a, b)$, where $a \in A$ and $b \in B$. We will verify that $g^{26} = (e, f)$. To see this, note that since $a^2 = e$, we have $a^{26} = e$ and since $b^{13} = f$, we also have $b^{26} = f$. Therefore,

$$g^{26} = (a, b)^{26} = (a^{26}, b^{26}) = (e, f),$$

as stated. It follows that $|g|$ divides 26. Therefore, no element of $G$ has order 52. Hence $G$ is not a cyclic group.

**Page 157, Problem 48.** By definition,

$$G \times H = \{ (g, h) \mid g \in G, \ h \in H \}, \quad H \times G = \{ (h, g) \mid h \in H, \ g \in G \}.$$

The group operations on these sets were defined in class one day. We can define a map $\varphi$ from $G \times H$ to $H \times G$ by $\varphi\left( (g, h) \right) = (h, g)$. Thus, any element $(h, g)$ in $H \times G$ is the image under the map $\varphi$ of the element $(g, h)$ in $G \times H$, and of no other element in $G \times H$. That is, the map $\varphi$ is a bijective map.

It remains to verify that $\varphi$ is a homomorphism. To see this, suppose that $(g_1, h_1)$ and $(g_2, h_2)$ are elements of $G \times H$. Then, by definition, $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$. Hence

$$\varphi\left( (g_1, h_1)(g_2, h_2) \right) = \varphi\left( (g_1g_2, h_1h_2) \right) = (h_1h_2, g_1g_2) = (h_1, g_1)(h_2, g_2).$$

On the other hand, we have

$$\varphi\left( (g_1, h_1) \right)\varphi\left( (g_2, h_2) \right) = (h_1, g_1)(h_2, g_2).$$
Hence we have \( \varphi \big( (g_1, h_1)(g_2, h_2) \big) = \varphi \big( (g_1, h_1) \big) \varphi \big( (g_2, h_2) \big) \). This means that \( \varphi \) is indeed a homomorphism from \( G \times H \) to \( H \times G \). Since \( \varphi \) is also bijective, \( \varphi \) is an isomorphism. Therefore, \( G \times H \) is isomorphic to \( H \times G \), as stated.

Page 166, Problem 4. This question concerns various subgroups of \( GL_2(\mathbb{R}) \), namely

\[
T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \ \bigg| \ a, b, c \in \mathbb{R}, ac \neq 0 \right\}, \quad U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \ \bigg| \ x \in \mathbb{R} \right\}.
\]

This notation is used because the elements of \( T \) are triangular matrices (more precisely, upper triangular) and the elements of \( U \) are unipotent matrices (referring to the fact that the eigenvalues are equal to 1).

The identity matrix \( I_2 \) is in both \( U \) and \( T \). To see that \( U \) and \( T \) are subgroups of \( GL_2(\mathbb{R}) \), we have (by matrix algebra)

\[
\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}, \quad \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + y \\ 0 & 1 \end{pmatrix}.
\]

Note also that \( ac \neq 0 \) and \( df \neq 0 \) implies that \((ad)(cf) \neq 0 \). Thus, both \( T \) and \( U \) are closed under matrix multiplication, which is the group operation in \( GL_2(\mathbb{R}) \). Furthermore, concerning inverses, we have

\[
\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} c^{-1} & -b(ac)^{-1} \\ 0 & a^{-1} \end{pmatrix}, \quad \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix},
\]

where we have used a standard formula for computing the inverse of a \( 2 \times 2 \) matrix with nonzero determinant. It follows that if \( \tau \in T \), then \( \tau^{-1} \in T \) and that if \( \eta \in U \), then \( \eta^{-1} \in U \).

The above discussion shows that \( T \) and \( U \) are subgroups of \( GL_2(\mathbb{R}) \). Also, \( U \subset T \) and hence \( U \) is a subgroup of \( T \). The fact that \( U \) is abelian follows from observing that

\[
\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y + x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}
\]

for all \( x, y \in \mathbb{R} \).

For the rest of this question, it will be useful to note that if \( ac \neq 0 \), then \( a \neq 0 \) and we have

\[
\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & ba^{-1} \\ 0 & 1 \end{pmatrix}.
\]
Thus, every element $\tau \in T$ can be expressed as $\tau = \delta \eta$, where $\eta \in U$ and $\delta$ is a diagonal matrix. Let

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \middle| a, c \in \mathbb{R}, ac \neq 0 \right\},$$

which is another subgroup of $GL_2(\mathbb{R})$. (The verification that $D$ is a subgroup is similar to the verification for $T$.) Thus, if $\tau \in T$, then we can express $\tau$ as $\tau = \delta \eta$, where $\delta \in D$, $\eta \in U$.

To verify that $U$ is a normal subgroup of $T$, suppose that $\tau \in T$ and $u \in U$. We must verify that $\tau u \tau^{-1} \in U$. We can write $\tau$ as $\tau = \delta \eta$ as in the previous paragraph. Then

$$\tau u \tau^{-1} = (\delta \eta) u (\delta \eta)^{-1} = (\delta \eta) u (\eta^{-1} \delta^{-1} = \delta (\eta u \eta^{-1}) \delta^{-1} = \delta \nu \delta^{-1}$$

where $\nu = \eta u \eta^{-1}$. Note that $\nu \in U$ because $u \in U$, $\eta \in U$ and $\eta^{-1} \in U$. Thus, it is sufficient to verify that $\delta \nu \delta^{-1} \in U$ for all $\nu \in U$ and all $\delta \in D$. This fact becomes clear from the following matrix identity (valid for $ac \neq 0$ and any $x \in \mathbb{R}$):

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & ac^{-1}x \\ 0 & 1 \end{pmatrix}.$$

And so we have shown that $U$ is indeed a normal subgroup of $T$.

Now we will prove that $T/U$ is abelian. Suppose that $\tau_1$ and $\tau_2$ are in $T$. As above, we can write $\tau_1 = \delta_1 \eta_1$ and $\tau_2 = \delta_2 \eta_2$, where $\delta_1, \delta_2 \in D$ and $\eta_1, \eta_2 \in U$. This will be very helpful because we then have

$$\tau_1 U = \delta_1 \eta_1 U = \delta_1 (\eta_1 U) = \delta_1 U, \quad \tau_2 U = \delta_2 \eta_2 U = \delta_2 (\eta_2 U) = \delta_2 U.$$

We have used the fact that $\eta U = U$ for all $\eta \in U$.

Note that $D$ is an abelian group. This is clear from the facts that

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & 0 \\ 0 & cf \end{pmatrix} = \begin{pmatrix} da & 0 \\ 0 & fc \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & f \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}.$$

Thus, $\delta_1 \delta_2 = \delta_2 \delta_1$ for all $\delta_1, \delta_2 \in D$. It follows that

$$(\tau_1 U)(\tau_2 U) = (\delta_1 U)(\delta_2 U) = \delta_1 \delta_2 U = \delta_2 \delta_1 U = (\delta_2 U)(\delta_1 U) = (\tau_2 U)(\tau_1 U)$$

and this shows that $T/U$ is indeed an abelian group.

Finally, we will show that $T$ is not a normal subgroup of $GL_2(\mathbb{R})$. Consider the following matrices:

$$\tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. $$
Then we have $\tau \in T$ and $\gamma \in GL_2(\mathbb{R})$, but

$$\gamma \tau \gamma^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$$

and hence $\gamma \tau \gamma^{-1} \notin T$. Hence, $\gamma T \gamma^{-1} \not\subseteq T$. Thus, $T$ is not a normal subgroup of $GL_2(\mathbb{R})$.

**Page 167, Problem 5.** Suppose that $H$ and $K$ are normal subgroups of a group $G$. We have proved previously that $H \cap K$ is a subgroup of $G$. We now prove that $H \cap K$ is a normal subgroup. Suppose that $g \in G$ and $a \in H \cap K$. Consider $gag^{-1}$.

First of all, we have $a \in H$. Since $H$ is a normal subgroup of $G$, we also have $gag^{-1} \in H$. Furthermore, $a \in K$. Since $K$ is a normal subgroup of $G$, we have $gag^{-1} \in H$. Therefore, $gag^{-1} \in H$ and $gag^{-1} \in K$. It follows that $gag^{-1} \in H \cap K$ for all $g \in G$ and all $a \in H \cap K$. This implies that the subgroup $H \cap K$ is indeed a normal subgroup of $G$.

**Page 167, Problem 7.** The statement is not true. Consider $G = Q_8$. Let $H = \langle j \rangle$. Then $H$ is a subgroup of $G$. Furthermore, $|H| = 4$ and $[G : H] = |G|/|H| = 8/4 = 2$. Thus, $H$ is a subgroup of $G$ which has index 2. As proved in class, this implies that $H$ is a normal subgroup of $G$.

Now $G/H$ is a group of order 2 and must be cyclic, and hence abelian. Also, $H$ is a group of order 4. Recall that groups of order 4 must be abelian. Thus, both $H$ and $G/H$ are abelian. However, $G$ itself is a nonabelian group.

**Page 167, Problem 9.** This statement is not true. Let $G$ be the Klein 4-group. Recall that every element of $G$ has order 1 or 2. But $|G| = 4$. Hence $G$ is not a cyclic group. However, if $a \in G$ and $a$ is not the identity element of $G$, then let $H = \langle a \rangle$. Then $H$ is a cyclic group of order 2. Also, $H$ is a normal subgroup of $G$ because $G$ is abelian. Now $G/H$ has order equal to $|G|/|H| = 4/2 = 2$. Hence $G/H$ is a group of order 2 and must be cyclic.

In summary, $G$ is not cyclic, but $H$ is cyclic and $G/H$ is also cyclic.

The example given in problem 7 would also be an example disproving the statement in this problem.

**Page 176, Problems 2a, c.** First we consider part (a). If $a, b \in \mathbb{R}^*$, then

$$\phi(ab) = \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} = \phi(a)\phi(b)$$
and therefore $\phi$ is a homomorphism from $\mathbb{R}^*$ to $GL_2(\mathbb{R})$.

The identity element in $GL_2(\mathbb{R})$ is $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. If $a \in \mathbb{R}^*$ and $\phi(a) = I_2$, then $a = 1$, which is the identity element in $\mathbb{R}^*$. Therefore, the kernel of $\phi$ is $\{1\}$, the trivial subgroup of $\mathbb{R}^*$.

Now consider part (c). The map $\phi$ is not a homomorphism. The easiest way to see this is to notice that $\phi(I_2) = 1 + 1 = 2$. The identity element in $GL_2(\mathbb{R})$ is $I_2$. The identity element in $\mathbb{R}$ is 0. But $\phi(I_2) \neq 0$. If $\phi$ were a homomorphism, then this could not happen.

**Page 176, Problem 4.** Suppose that $n, m \in \mathbb{Z}$. Then
\[
\phi(n + m) = 7(n + m) = 7n + 7m = \phi(n) + \phi(m)
\]
and hence $\phi$ is indeed a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$. To find the kernel, note that 0 is the identity element in $\mathbb{Z}$. We have
\[
\phi(n) = 0 \iff 7n = 0 \iff n = 0
\]
and therefore the kernel of $\phi$ is the subgroup $\{0\}$ of $\mathbb{Z}$. The image of $\phi$ is obviously the subgroup $7\mathbb{Z}$ of $\mathbb{Z}$.

**Page 177, Problem 9.** We are given that $G$ is abelian. It turns out that $\phi(G)$ is a subgroup of $H$. To prove that $\phi(G)$ is abelian, suppose that $a, b \in \phi(G)$. This means that $a = \phi(u)$ and $b = \phi(v)$, where $u, v \in G$. We have $uv = vu$ because $G$ is abelian. Therefore,
\[
ab = \phi(u)\phi(v) = \phi(uv) = \phi(vu) = \phi(v)\phi(u) = ba .
\]
Thus, $ab = ba$ for all $a, b \in \phi(G)$. This proves that $\phi(G)$ is indeed abelian.

**Page 177, Problem 14.** Recall the following fact. Suppose that $G$ and $G'$ are groups and that $\phi : G \to G'$ is an isomorphism. Suppose that $g \in G$. Then $\phi(g)$ has the same order as $g$. We proved this in class one day. It will be useful in this problem. Note for example that if $G$ has an element $g$ of order 2, then $G'$ will also have an element of order 2, namely $\phi(g)$.

Let $G = \mathbb{Q}/\mathbb{Z}$. Then $G$ has an element of order 2, namely the element
\[
g = \frac{1}{2} + \mathbb{Z} .
\]
This is a left coset of $\mathbb{Z}$ in $\mathbb{Q}$. Furthermore, $\frac{1}{2} \notin \mathbb{Z}$ and hence $g$ is not the identity element of $\mathbb{Q}/\mathbb{Z}$ (which is the left coset $0 + \mathbb{Z} = \mathbb{Z}$). However,

$$2g = g + g = \left( \frac{1}{2} + \mathbb{Z} \right) + \left( \frac{1}{2} + \mathbb{Z} \right) = 1 + \mathbb{Z} = \mathbb{Z}$$

and so $g$ has order 2. However, the identity element in $\mathbb{Q}$ is 0. If $r \in \mathbb{Q}$ and $2r = 0$, then $r = 0$. Hence no element of $\mathbb{Q}$ can have order 2.

In summary, $\mathbb{Q}/\mathbb{Z}$ has an element of order 2, but $\mathbb{Q}$ has no elements of order 2. Hence those two groups cannot be isomorphic.

**Problem A.** We must show that if $\sigma \in S_n$, then $\sigma$ and $\sigma^{-1}$ are conjugate in $S_n$. We know that two elements of $S_n$ are conjugate if and only if they have the same cycle decomposition type. And so one must show that $\sigma$ and $\sigma^{-1}$ have the same cycle decomposition type.

Suppose first that $\sigma$ is a $k$-cycle. Thus $\sigma = (i_1 i_2 \ldots i_k)$, where $i_1, i_2, \ldots, i_k$ are distinct elements in the set $\{1, \ldots, n\}$. But $\sigma^{-1}$ is also a $k$-cycle. In fact, $\sigma^{-1} = (i_k i_{k-1} \ldots i_1)$, which is indeed a $k$-cycle. Now if $\sigma$ is a product of $t$ disjoint cycles of lengths $k_1, \ldots, k_t$, then $\sigma^{-1}$ will be a product of the inverses of those cycles, and so $\sigma^{-1}$ will also be a product of $t$ disjoint cycles of lengths $k_1, \ldots, k_t$. Thus, $\sigma$ and $\sigma^{-1}$ indeed have the same cycle decomposition type.

**Problem B.** This problem is identical to problem 5 on page 167.

**Problem C.** Suppose that $G$ is a finite group, that $N$ is a normal subgroup of $G$, and that $G/N$ has an element of order $m$, where $m$ is a positive integer.

The elements of $G/N$ are of the form $aN$, where $a \in G$. Suppose that $a$ is chosen so that $aN$ is an element of $G/N$ which has order $m$. The rest of this proof will concern the element $a$.

Since $a \in G$ and $G$ is finite, it follows that the subgroup $\langle a \rangle$ of $G$ is a finite group. Thus $a$ has finite order. Let $n$ be the order of $a$. In particular, $a^n = e$, where $e$ is the identity element of $G$.

In the group $G/N$, we have $(aN)(bN) = abN$ for all $a, b \in G$. In particular, we have $(aN)^2 = a^2N$. A straightforward mathematical induction proof shows that $(aN)^k = a^kN$ for all positive integers $k$. 

8
Since $a^n = e$, it follows that $(aN)^n = a^n N = eN = N$. Now we chose $a$ at the beginning of this proof so that $aN$ is an element in the group $G/N$ of order $m$. Therefore, the fact that $(aN)^n = e$ implies that $m$ divides $n$.

The subgroup $\langle a \rangle$ of $G$ which is generated by $a$ has order $n$. It is a cyclic group of order $n$. We proved in class that if $d$ is a positive integer which divides $n$, then a cyclic group of order $n$ must contain an element of order $d$. In particular, since $m$ divides $n$, it follows that $\langle a \rangle$ contains an element of order $m$. Therefore, it follows that $G$ contains an element of order $m$. This is what we wanted to prove.