Question:
1. (10 points) Prove that if \(G\) is a group of order 385, then \(G\) contains a normal cyclic subgroup of order 77.

Solution:
\(385 = 5 \times 7 \times 11\). Let \(n_p\) be the number of Sylow \(p\)-subgroups of \(G\) for \(p = 5, 7, 11\). By the third Sylow Theorem, \(n_{11} \equiv 1 \pmod{11}\) and \(n_{11} \mid 35 \Rightarrow n_{11} = 1\). Similarly \(n_7 \equiv 1 \pmod{7}\) and \(n_7 \mid 55 \Rightarrow n_7 = 1\). Let \(K\) be the Sylow-7 subgroup and \(L\) the Sylow-11 subgroup. Both \(K, L \triangleleft G\) since they are the only Sylow-7, 11 subgroups. Moreover, \(K \cap L = \{1\}\) since \((7, 11) = 1\), and \(K \approx C_7\) and \(L \approx C_{11}\). Hence \(K \cap L = \{1\}\), and \(|KL| = 77\) then \(KL \approx K \times L \approx C_7 \times C_{11} \approx C_{77}\). Thus \(G\) contains a cyclic subgroup \(KL\) of order 77. It remains to show that \(KL\) is normal. i.e.: \(\forall g \in G\), \(gLg^{-1} = KL\). Let \(k, \ell \in KL \Rightarrow gk\ell g^{-1} = gk g^{-1} \ell g^{-1} = k\ell' \in KL\) since both \(K, L \triangleleft G\). Hence \(KL\) is normal in \(G\).
Question:
2. (10 points)
Prove that there is a non-trivial group homomorphism \( \mathbb{Z}_n \rightarrow \mathbb{Z}_m \) iff \((n, m) \neq 1\).

Solution:
Assume there exists a non-trivial group homomorphism \( \phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m \). We know that 
\[ |\mathbb{Z}_n| = |\ker \phi| = |\phi(\mathbb{Z}_n)| / n. \]
But \( \phi(\mathbb{Z}_n) \leq \mathbb{Z}_m \Rightarrow |\phi(\mathbb{Z}_n)| / m \) since \( \phi \) is non-trivial
(i.e.: \( \phi(x) \neq 0 \forall x \in \mathbb{Z}_n \) \( \Rightarrow \phi(\mathbb{Z}_n) > 1 \Rightarrow (m, n) \neq 1 \).

Next, assume \((n, m) \neq 1\); let \( d = (n, m) > 1 \) let \( k = m / d \). Define
\( \phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m \) by \( \phi([a]) = [k] \) (note \([k] \neq 0\)), then \( \phi([a]) = ak \). We must show that \( \phi \) is well-defined: i.e. if \( [a] = [b] \Rightarrow \phi([a]) = \phi([b]) \). If 
\( [a] = [b] \Rightarrow a - b = 0 \Rightarrow a - b = ng \) for some \( g \in \mathbb{Z} \), then \( \phi(a - b) = \phi(ng) = \bar{n} \bar{g} \bar{k} \)
\( = \frac{ngm}{d} = \frac{ng}{d} \cdot m = 0 \), since \( \frac{n}{d} \in \mathbb{Z} \).
Question:
3. (30 points)

Let \( R = m \in \mathbb{Z} \) and \( \{ a + b\sqrt{m} \mid a, b \in \mathbb{Z} \} \). Let \( d : R \to \mathbb{Z} \) be given by

\[
d(a + b\sqrt{m}) = a^2 - b^2m.
\]

(a) Show that \( R \) is an integral domain.

Solution:
(a) It is straightforward to show that \( R \) is a subring of \( \mathbb{C} \). Thus \( R \) is an integral domain since \( \mathbb{C} \) is.

Question:
(b) What subfield of \( \mathbb{C} \) is isomorphic to the field of fractions for \( R \)? Just give a brief justification for this.

Solution:
(b) Let \( F = \{ p + q\sqrt{m} \mid p, q \in \mathbb{Q} \} \). This is the field of fractions of \( R \), since if \( a + b\sqrt{m} \)

has an inverse \( \frac{1}{a + b\sqrt{m}} \) we have \( \frac{1}{a + b\sqrt{m}} \cdot \frac{a - b\sqrt{m}}{a - b\sqrt{m}} = \frac{1}{a + b\sqrt{m}} 
\]

\[
= \frac{a}{a^2 - b^2m} - \frac{b}{a^2 - b^2m} \sqrt{m} \quad \text{and} \quad \frac{a}{a^2 - b^2m} - \frac{b}{a^2 - b^2m} \in \mathbb{Q}.
\]

Question:
(c) Prove or disprove that \( d \) is a ring homomorphism.

Solution:
(c) For \( d \) to be a ring homomorphism it must preserve both operations. Note that

\[
d(a + b\sqrt{m}) = a^2 - b^2m \quad \text{and} \quad d(c + d\sqrt{m}) = c^2 - d^2m, \quad \text{but}
\]

\[
d(a + b\sqrt{m} + c + d\sqrt{m}) = d((a + c) + (b + d)\sqrt{m})
\]

\[
= (a + c)^2 - (b + d)^2m \neq (a^2 + c^2) - (b^2 + d^2)m.
\]

On the other hand, it is easy to check that \( d(\alpha, \beta) = d(\alpha)d(\beta) \). Hence, while \( d \) is not a ring homomorphism, it is a homomorphism that preserves multiplication.

Question:
(d) Prove that for \( \alpha \in R \), \( \alpha \) is a unit iff \( d(\alpha) = \pm 1 \).

Solution:
(d) It is straightforward to show that \( \forall \alpha, \beta \in R \), \( d(\alpha\beta) = d(\alpha)d(\beta) \). Thus \( \alpha \) is a unit if and only if

\[
\exists \alpha^{-1} \in R \quad \text{such that} \quad \alpha\alpha^{-1} = 1 \iff d(\alpha\alpha^{-1}) = 1 = d(\alpha)d(\alpha^{-1}) \iff d(\alpha^{-1}) = \frac{1}{d(\alpha)}.
\]

But \( d(x) \in \mathbb{Z}, \forall x \in R \). Hence, \( d(\alpha^{-1}) = \frac{1}{d(\alpha)} \iff d(\alpha) = \pm 1 \).
Question:
(e) Prove that if $m < 0$, then $R^*$ is finite, where $R^*$ is the group of units of $R$.

Solution:
(e) If $m < 0$, let $n = -m$. We have $d(a + b\sqrt{m}) = a^2 - b^2m = a^2 + b^2n = \pm 1$ (from d)
$\iff a^2 = 0$ and $b^2n = \pm 1 \iff b = \pm 1$ and $n = \pm 1$ or $a^2 = \pm 1$ and $b^2n = 0 \iff a = \pm 1$.
So in all cases $R^*$ is finite.

Question:
(f) Prove that if $m = -6$, then $2$, $3$, and $\sqrt{-6}$ are all irreducible elements of $R$.

Solution:
(f) Prove that $2$, $3$, $\sqrt{-6}$ are irreducible in $R$. Note that when $m = -6$, $d(a + b\sqrt{m}) = a^2 + 6b^2$ and $d(2) = 4$, $d(-3) = 9$ and $d(\sqrt{-6}) = 6$, so for $2$ to be irreducible we must find two elements $\alpha, \beta$ s.t. $d(\alpha\beta) = d(\alpha)d(\beta) = 4$ with $d(\alpha), d(\beta) \neq \pm 1$. So $d(\alpha) = d(\beta) = 2$. But clearly there are no integers $a, b$ such that $a^2 + 6b^2 = 2$. Similarly, since $d(-3) = 9$ we are looking for elements $\alpha$ such that $d(\alpha) = 3$. But again there are no integers such that $a^2 + 6b^2 = 3$.
Lastly, if $\sqrt{-6}$ was reducible we would find elements $\alpha, \beta$ such that $d(\alpha) = 2$ and $d(\beta) = 3$, which we just showed was impossible.
Question:
4. (20 points) Remember to prove/justify all of your assertions.
   (a) What is the degree of $\sqrt{3}$ over $\mathbb{Q}$?

Solution:
   (a) Let $f(x) = x^2 - 3$, $f(\sqrt{3}) = 0$, and $x^2 - 3$ is irreducible over $\mathbb{Q}$ since $-\sqrt{3}$ is also a root of $f(x)$ $\Rightarrow$ $f(x) = (x - \sqrt{3})(x + \sqrt{3})$ is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

Question:
(b) Find $[\mathbb{Q}(\sqrt{2}), \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$.

Solution:
   (b) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$ is the degree of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. But $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$ since if it was reducible this would mean that $\sqrt{3} = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ $\iff 3 = a^2 + 2b^2 + ab\sqrt{2} \iff ab = 0 \iff a = 0$ or $b = 0$. But if $a = 0$ then $3 = 2b^2$ has no rational solution, and if $b = 0$ then $3 = a^2$ which also does not have any rational solution. Hence $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Question:
(c) Find the degree of $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.

Solution:
   (c) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$
      $= 2.2$
      $= 4$.

Question:
(d) Find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}$.
Solution:

(d) From c we are looking for a basis with 4 elements. Let $B = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Clearly each element of $B \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We are left to show that $1, \sqrt{2}, \sqrt{3}$ and $\sqrt{6}$ are linearly independent over $\mathbb{Q}$. Let $a \sqrt{2} + b \sqrt{3} + c \sqrt{6} = 0$, then we must have that $a = 0$ and $b \sqrt{2} + c \sqrt{3} + d \sqrt{6} = 0$

$\iff 2b + c \sqrt{2} \sqrt{3} + d \sqrt{2} \sqrt{6} = 0$

$\iff 2b + c \sqrt{6} + 2d \sqrt{3} = 0$

$\iff b = 0$ and $c \sqrt{6} + 2d \sqrt{3} = 0$

$\iff b = 0$ and $c \sqrt{6} + 2d \sqrt{3} = 0$

$\iff c \sqrt{18} + 6d = 0 \iff 3c \sqrt{2} + 6d = 0$

$\iff d = 0$ and $c = 0$. 

Note, there are several ways to show that $B$ is a linearly independent set. In particular, from (b) and (c) we already know that $1, \sqrt{2}$, and $\sqrt{3}$ are linearly independent.