4.5.30. Note that any element of order 7 generates a subgroup of order 7, and any subgroup of order 7 contains the identity and six elements of order 7.

Hence, we will count the subgroups of order 7.

\[ 168 = 7 \cdot 2^3 \cdot 3, \] so subgroups of order 7 are Sylow 7-subgroups.

Consider \( n_7 \), the number of Sylow 7-subgroups.

We know that \( n_7 \mid 168 \) and \( n_7 \equiv 1 \mod 7 \) (Sylow's theorem).

\[ \therefore n_7 \mid \frac{168}{7} = 24 \] so \( n_7 = 1 \) or \( 8 \).

If \( n_7 = 1 \), then because conjugating a subgroup by anything produces another subgroup of the same order, the unique subgroup of order 7 is normal contradicting the simplicity of our original group.

\[ \therefore n_7 = 8, \] so there are 8 subgroups of order 7.

These subgroups are cyclic, so contain only the identity in common between any two. (Why is this important?)

\[ \therefore \] Each of the 8 subgroups of order 7 has 6 elements of order 7, so there are 48 elements of order 7.
7.1.3) If \( u \) is a unit in \( S \) then there exists \( v \in S \)
with \( uv = vu = 1 \)

But \( S \subseteq R \), so \( v \in R \), so \( uv = vu = 1 \) in \( R \),
so \( u \) is a unit in \( R \).

The reverse implication does not hold. For example,
2 is a unit in \( \mathbb{Q} \) as \( 2 \cdot 1/2 = 1/2 \cdot 2 = 1 \) but
2 is not a unit in the subring \( \mathbb{Z} \).

7.1.5) a) is a subring
b) is not closed under addition \(- \frac{1}{2} + \frac{1}{2} = \frac{1}{1} \)
c) is not closed under subtraction (a ring is an additive abelian group with
additional structure)
d) is not closed under addition \(- 1 + 1 = 2 \)
e) is not closed under addition \(- (1) = 2 \)
f) is a subring.

7.3.2) Let \( \phi : R \rightarrow S \) be an isomorphism of rings.
Then \( r \in R \) is a unit if and only if \( \phi(r) \in S \) is
a unit. (As \( rr^{-1} = 1 \Rightarrow \phi(r) \phi(r^{-1}) = \phi(1) = 1 \))

Then there are the same (potentially infinite) number of units
in \( R \) and \( S \).

The ring \( \mathbb{K}[x] \) has two units \(- 1 \) and \(- 1 \).
The ring \( \mathbb{Q}[x] \) has infinitely many units - all nonzero rationals.

\( \therefore \mathbb{Z}[x] \) and \( \mathbb{Q}[x] \) cannot be isomorphic.
7.3.10) a) is an ideal
b) is not closed under multiplication - $x \cdot (3x^2 + x) = 3x^3 + x^2$

e) is an ideal
f) is not closed under multiplication - $x(5) = 5x$

7.3.24) c) To show that $\mathcal{U}^{-1}(J)$ is a ideal of $R$, we need to show that it is nonempty, closed under subtraction, and closed under multiplication by arbitrary elements of $R$.

$\mathcal{U}(0_R) = 0_S$ and $J$ is an ideal so $0_S \in J$, so $0_R \in \mathcal{U}^{-1}(J)$.

Consider any $a, b \in \mathcal{U}^{-1}(J)$.

$a - b$ is an element of $R$ as $R$ is closed under subtraction.

$\mathcal{U}(a - b) = \mathcal{U}(a) - \mathcal{U}(b)$, and $\mathcal{U}(a), \mathcal{U}(b)$ are in $J$, so $\mathcal{U}(a) - \mathcal{U}(b)$ is in $J$, as $J$ is closed under subtraction.

$\mathcal{U}(a - b) \in J$, so $a - b \in \mathcal{U}^{-1}(J)$.

$\mathcal{U}^{-1}(J)$ is closed under subtraction.

Consider any $a \in \mathcal{U}^{-1}(J)$ and any $c \in R$.

$ca \in R$, so consider $\mathcal{U}(ca) = \mathcal{U}(c)\mathcal{U}(a)$.

$\mathcal{U}(a) \in J$ and $J$ is an ideal so $\mathcal{U}(c)\mathcal{U}(a) \in J$.

$\mathcal{U}(ca) \in J$, so $ca \in \mathcal{U}^{-1}(J)$.

$\mathcal{U}^{-1}(J)$ is closed under multiplication by elements of $R$.

$\mathcal{U}^{-1}(J)$ is an ideal of $R$. 

\[ \mathbb{Q} \]
Now, let \( R \subseteq S \), and let \( \varphi : R \to S \) be the inclusion map.
The set \( \varphi^{-1}(J') \) is \( J \cap R \) for any ideal \( J \) of \( S \), and we know that \( \varphi^{-1}(J') \) is an ideal of \( R \), so \( J \cap R \) is an ideal of \( R \).

We need the inclusion map to actually be a homomorphism, but this is easily checked.

b) Now, let \( \varphi : R \to S \) be a surjective ring homomorphism, and let \( I \) be an ideal of \( R \).

To show that \( \varphi(I) \) is an ideal of \( S \), we need to show that \( A \) is nonempty, closed under subtraction, and closed under multiplication by arbitrary elements of \( S \).

Let \( \varphi(a) \) and \( \varphi(b) \) be arbitrary elements of \( \varphi(I) \), for \( a, b \in I \). Then \( \varphi(a-b) = \varphi(a) - \varphi(b) \), so \( \varphi(a) - \varphi(b) \in \varphi(I) \) as \( a-b \in I \) (\( I \) being closed under subtraction).

Let \( \varphi(a) \) be an arbitrary element of \( \varphi(I) \), and let \( s \) be an arbitrary element of \( S \). We want to show that \( s \varphi(a) \in \varphi(I) \). We know that \( \varphi : R \to S \) is surjective, so there exists some \( r \in R \) with \( \varphi(r) = s \).

Then \( \varphi(r \varphi(a)) = \varphi(r) \varphi(a) = \varphi(ra) \). But \( ra \in I \) and \( I \) is an ideal of \( R \), so \( ra \in I \). Then \( \varphi(ra) = \varphi(r) \varphi(a) \in \varphi(I) \).

Thus, \( \varphi(I) \) is closed under multiplication by arbitrary elements.
$\mathbb{Q}(\mathbb{Z})$ is an ideal of $\mathbb{S}$ as required.

To show that the surjectivity of $\mathbb{Q}$ is necessary, consider the map $\mathbb{Q}: \mathbb{Z} \to \mathbb{Q}$, where $\mathbb{Q}$ is the inclusion map $\mathbb{Q}(n) = n$ for each $n \in \mathbb{Z}$.

The set $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but $\mathbb{Q}(2\mathbb{Z})$, the set of rational numbers which are even integers, is not an ideal of $\mathbb{Q}$. For example, multiplying $2 \in 2\mathbb{Z}$ by $\frac{1}{2} \in \mathbb{Q}$ produces $1$, which is not in $2\mathbb{Z}$. 