Proposition 6.3.7 Let $\phi: R \to S$ be a surjective ring homomorphism, and let $J = \ker(\phi)$.
For $B \subseteq S$, consider $\phi^{-1}(B) \subseteq R$.
The mapping $B \to \phi^{-1}(B)$ gives a bijection between

- $\{\text{subgroups of } (S,+) \}$ \leftrightarrow \{\text{subgroups of } (R,+) \text{ containing } J \}$
- $\{\text{subrings of } (S,+) \}$ \leftrightarrow \{\text{subrings of } (R,+) \text{ containing } J \}$
- $\{\text{ideals in } (S,+) \}$ \leftrightarrow \{\text{ideals in } (R,+) \text{ containing } J \}$

The statement about subgroups was proved already. It's an exercise to show that the correspondence takes subrings to subrings and ideals to ideals.

Definition A maximal ideal in a ring $R$ is an ideal $M$ such that
- $M \neq R$
- If $I$ is an ideal and $M \subseteq I \subseteq R$, then either $I = R$ or $I = M$.
  "There are no proper ideals bigger than $M"$

Lemma If $R$ is a ring with 1 and $I \subseteq R$ is an ideal, then $1 \in I \implies I = R$.
Proof Take any $r \in R$. Then $r = r \cdot 1 \in I$ since $1 \in I$. 
Proposition. Let $R$ be a commutative ring with 1. Assume $1 \neq 0$.
Then $R$ is a field if and only if the only ideals in $R$ are $\{0\}$ and $R$.

Proof. Suppose $R$ is a field. Let $I \leq R$ be an ideal. If $I \neq \{0\}$,
there is some $a \neq 0$ in $I$. Then $1 = a^{-1}a \in I$ so $I = R$.

Conversely, suppose the only ideals in $R$ are $\{0\}$ and $R$. Let $a \in R$
be a non-zero element. Then $(a) = \{ra | r \in R\}$ is an ideal
in $R$, and $(a) \neq \{0\}$, so $(a) = R$ so $1 \in (a)$ and
$1 = ra$ for some $r \in R$. Then $r$ is a multiplicative inverse for $a$.

Proposition. Let $R$ be a commutative ring with 1. An ideal $M \leq R$
is maximal if and only if $R/M$ is a field.

Proof. Consider $\pi : R \to R/M$. There is a bijection

\[
\begin{align*}
\{ \text{ideals } B \leq R/M \} & \leftrightarrow \{ \text{ideals } B' \leq R \text{ such that } MSB' \leq R \} \\
B & \mapsto \pi^{-1}(B) = B'
\end{align*}
\]

$R/M$ is a field $\iff$ only two ideals in $R/M$ are only two ideals in $R$ that contain $M$

\[
\begin{align*}
\{ M/M, R/M \} & \leftrightarrow \{ M, R \} \\
M & \text{ is maximal.}
\end{align*}
\]
Integral domains and prime ideals

In some rings, it is possible to have non-zero elements whose product is zero.
- In \( \mathbb{Z}_5 \), \([2][2] = [0]\), even though \([2]+[0][2] \neq [0]\).
- In \(2 \times 2\) matrices, \(n = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\) satisfies \(n^2 = 0\).

Rings in which this cannot happen have a name.  
**Definition** let \( R \) be a commutative ring with 1.

\( R \) is an **integral domain** if the product of two non-zero elements is non-zero:
\[a \neq 0 \text{ and } b \neq 0 \implies a \cdot b \neq 0.\]

**Example** \( \mathbb{Z}, \text{ fields, } K[x] \) (\( K \) a field)

Some equivalent conditions:
(a) The set \( R - \{0\} \) is closed under multiplication.
(b) If \( ab = 0 \), then either \( a = 0 \) or \( b = 0 \).
(c) \( R \) has no **zero divisors**

**Definition** \( a \in R \) is a **zero divisor** if \( a \neq 0 \) and \( \exists b \neq 0 \) such that \( ab = 0 \).

There is a somewhat similar definition for ideals.

**Definition** An ideal \( I \subseteq R \) is **prime** if whenever \( ab \in I \), then \( a \in I \) or \( b \in I \).

Equivalent conditions:
- If \( a \notin I \) and \( b \notin I \) then \( ab \notin I \).
- The set \( R - I \) is closed under multiplication.
Proposition  R is an integral domain if and only if \( \mathfrak{p} \mathbb{Z} \) is a prime ideal.

Proof  \( R \) integral domain \( \iff \mathfrak{p} \mathbb{Z} \) closed under multiplication \( \iff \mathfrak{p} \mathbb{Z} \) is prime.

Example: Let \( p \in \mathbb{N} \) be a prime number. We have the ideal \( (p) = p\mathbb{Z} = \{pk \mid k \in \mathbb{Z} \} \). Then \( p \) is a prime ideal:

If \( ab \in (p) \) then \( p | ab \) so \( p | a \) or \( p | b \) so \( a \in (p) \) or \( b \in (p) \).

Conversely, if \( n \in \mathbb{N} \) is composite \( n = ab, \ 1 < a, b < n \)
\( ab \in (n) \) but \( a \notin (n) \) and \( b \notin (n) \), so \( (n) = n\mathbb{Z} \) is not prime.

Example: Let \( K \) be a field, and let \( f \in K[x] \)
then \( (f) = fK[x] \) is a prime ideal
if and only if \( f \) is irreducible.

Proposition: Let \( R \) be a commutative ring with 1, and let \( I \subseteq R \)
be an ideal. Then \( R/I \) is an integral domain if and only if \( I \) is a prime ideal.

Proof Suppose \( R/I \) is an integral domain, and let \( ab \in I \)
than in \( R/I \), \( 0 + I = ab + I = (a + I)(b + I) \)

Since \( R/I \) is integral domain, \( a + I = 0 + I \) or \( b + I = 0 + I \)
so \( a \in I \) or \( b \in I \)

Thus, \( I \) is prime.

Conversely, suppose \( I \) is prime and that \( (a + I)(b + I) = 0 + I \).

Then \( ab + I = 0 + I \) and \( ab \in I \)
thus either \( a \in I \) or \( b \in I \) so \( a + I = 0 + I \) or \( b + I = 0 + I \).

and \( R \) is an integral domain.
Corollary: Let $R$ be a commutative ring with $1$. Any maximal ideal in $R$ is prime.

Proof: $M \leq R$ maximal ideal $\Rightarrow$ $R/M$ is a field
$\Rightarrow$ $R/M$ is an integral domain
$\Rightarrow$ $M$ is prime