Recall. Suppose $A$ is a unital commutative ring. An ideal $I$ of $A$ is called maximal if

1. $I$ is proper; that means $I \neq A$;
2. $I \subseteq J \Rightarrow$ either $J = I$ or $J = A$.

Theorem. Suppose $A$ is a unital commutative ring and $I \triangleleft A$; then $I$ is maximal $\iff A/I$ is a field.

Proof. ($\Rightarrow$) To show $A/I$ is a field we have to show

1. it is a unital commutative ring;
2. it is not the zero ring;
3. any non-zero element is a unit.

1. $(a+I)(a_2+I) = a_1a_2+I = a_2a_1+I = (a_1+I)(a_2+I)$.

2. $(1+I)(a+I) = (1a)+I = a+I$; similarly $(a+I)(1+I) = a+I$ and so $1+I$ is the identity of $A/I$.
3. $A/I \neq 0$ as $I \neq A$.
4. Suppose $a+I \neq 0+I$. Then $a \not\in I$.

Claim. Smallest ideal $J$ of $A$ that contains $I$ as a subset and $a$ as an element is $\{a+r+I \mid r \in A, x \in I\}$.
Proof of claim. First we show

\[ J_0 = \{ ar + x \mid r \in A, x \in I \} \] is an ideal.

\[ (ar_1 + x_1) + (ar_2 + x_2) = a(r_1 + r_2) + (x_1 + x_2) \in J_0. \]

\[ a(r'r) + (r'x) \in J_0. \]

as \( x \in I \)

Second, we observe \( a = (a)(1) + (0) \in J_0 \)

\[ \forall x \in I, x = (a)(0) + x \in J_0 \implies I \subset J_0. \]

Third, if \( J \triangleleft A, I \subset J, \) and \( a \in J, \) then

\[ \forall x \in I, \forall r \in A, ra \in J \text{ and } ra + x \in J. \]

Hence \( J_0 \subset J. \) and claim follows. \( \Box \)

Since \( I \) is a maximal ideal, \( I \subset J_0, \) and \( a \in J_0 \setminus I, \)
we deduce that \( J_0 = A. \) Hence \( 1 \in J_0 \) which implies

\[ \exists r \in A, x \in I \text{ s.t. } ar + x = 1. \]

Therefore \( 1 - ar = x \in I; \) and so \( 1 + I = ar + I = (a + I)(r + I) \).

This implies \( a + I \in (A/I)^x. \)
Since $A/\mathcal{I}$ is a field, $A/\mathcal{I} \neq 0$; and so $\mathcal{I} \neq A$.

Suppose to the contrary that $\mathcal{I}$ is not a maximal ideal.

Since $\mathcal{I} \neq A$, we deduce that

$\exists \mathcal{J} \supseteq \mathcal{I}$ such that $\mathcal{I} \nsubseteq \mathcal{J} \neq A$.

Suppose $a \in \mathcal{J} \setminus \mathcal{I}$. Hence $a + \mathcal{I} \neq 0 + \mathcal{I}$ in $A/\mathcal{I}$. As $A/\mathcal{I}$ is a field, $\exists a' \in A$ st. $(a + \mathcal{I})(a' + \mathcal{I}) = 1 + \mathcal{I}$.

And so $\exists x \in \mathcal{I}$ st. $1 - aa' = x$. Thus $1 = aa' + x$ for some $a' \in A$ and $x \in \mathcal{I}$.

$a \in \mathcal{J} \Rightarrow aa' \in \mathcal{J} \Rightarrow aa' + x \in \mathcal{J} \Rightarrow 1 \in \mathcal{J} \Rightarrow \mathcal{J} = A$

which contradicts (a).

Corollary. Suppose $A$ is a unital commutative ring. If $I$ is a maximal ideal, then $I$ is a prime ideal.

Proof. $I$ maximal $\Rightarrow A/\mathcal{I}$ field

$\Rightarrow A/\mathcal{I}$ integral domain

$\Rightarrow I$ prime.
Corollary. Suppose $A$ is a unital commutative ring, $I \subseteq A$, and $|A/I| < \infty$; then

$I$ is maximal $\iff$ $I$ is prime.

Proof. $I$ is maximal $\iff$ $A/I$ is a field

because $|A/I| < \infty$ $\iff$ $A/I$ is an integral domain $\iff$ $I$ is prime.
Ex. Determine all the prime and maximal ideals of $\mathbb{Z}$.

Solution. Any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.

To determine, if $n\mathbb{Z}$ is either prime or maximal, we need to study the quotient ring $\mathbb{Z}/n\mathbb{Z}$.

We know that, if $n \geq 2$, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. And $\mathbb{Z}_n$ is an integral domain $\iff$ $\mathbb{Z}_n$ is a field $\iff$ $n$ is a prime.

- If $n=1$, then $n\mathbb{Z} = \mathbb{Z}$; and so it is neither prime nor maximal.

- If $n=0$, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$; which is an integral domain, but not a field. So $\mathfrak{p}_{\mathbb{Z}}$ is a prime ideal, but not a maximal ideal. Overall we have:

  the set of maximal ideals of $\mathbb{Z} = \{ p\mathbb{Z} \mid p \text{ is a prime number} \}$

  the set of prime ideals of $\mathbb{Z} = \{ n\mathbb{Z} \mid n \text{ is either 0 or a prime number} \}$

Next we show $m_0(\mathbb{Q}[x])$ is a maximal ideal and deduce
\( \mathbb{Q}[x] \cong \mathbb{Q}[x]/m_2(x) \mathbb{Q}[x] \) is a field. We have already proved that \( m_2(x) \) is irreducible in \( \mathbb{Q}[x] \); so the following proposition gives us the above claim.

**Theorem.** Let \( R \) be a PID, and \( a \in R \setminus \{0\} \).

Then \( I = aR \) is maximal if and only if \( a \) is irreducible.

**(⇒)** We have to show

1. \( a \neq 0, a \notin R^\times \)
2. If \( a = bc \), then either \( b \in R^\times \) or \( c \in R^\times \).
3. Since \( I \) is maximal, it is a proper ideal. So \( a \notin R^\times \).
4. \( a = bc \in aR \implies \) either \( b \in aR \) or \( c \in aR \).

\( aR \) maximal \implies \( aR \) prime.

If \( b \in aR \), then \( b = ab' \). Hence \( a = bc = ab'c \); and so by the cancellation law \( b'c = 1 \) which implies \( c \in R^\times \).

Similarly, if \( cebR \), we can deduce that \( b \in R^\times \).

**(⇐)** Suppose \( a \) is irreducible. Then \( a \notin R^\times \); and so \( 1 \notin aR \),
Lecture 14: Maximal ideals and irreducible elements

which implies $aR \neq R$. Now suppose $aR \subseteq J$ and $J \neq R$.

Since $R$ is a PID, $J = bR$ for some $b$. As $a \in aR \subseteq bR$, $\exists r \in R$ such that $a = br$. As $a$ is irreducible, either $b$ is a unit or $r$ is a unit.

If $br \in R$, $J = bR = R$. If $r$ is a unit,

$$b = ar^{-1} \in aR; \text{ and so } bR \subseteq aR.$$ 

On the other hand, $aR \subseteq bR$; therefore $J = bR = aR$.

So $aR$ is maximal. \[ \Box \]

Corollary Let $D$ be a PID. Suppose $a$ is irreducible in $D$.

Then $D/\langle a \rangle$ is a field.

Corollary. If $\alpha \in \mathbb{C}$ is an algebraic number, then $\mathbb{Q}[\alpha]$ is a field.

\[ \text{Proof.} \text{ Earlier based on the 1st isomorphism theorem we proved } \mathbb{Q}[\alpha] = \text{Im } \phi_\alpha \cong \mathbb{Q}[x]/\ker \phi_\alpha = \mathbb{Q}[x]/m_\alpha(x) \mathbb{Q}[x]. \]

We have also proved that $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$. 

\[ \]
Hence by the previous corollary and the fact that $\mathbb{Q}[x]$ is a PID, we get the claim. ☐