In the previous lecture we proved:

**Theorem.** Let $R$ be a unital commutative ring and $I \subset R$. Then $I$ is a maximal ideal if and only if $R/I$ is a field.

Using the above theorem, we'd like to show:

**Theorem.** Let $\alpha$ be an algebraic number, and $\varphi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ be the evaluation at $\alpha$. Then $\text{Im} \varphi_\alpha$ is a field.

We have proved that $\ker \varphi_\alpha = \langle m_\alpha(x) \rangle$ where $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$. So the following Proposition implies the above theorem.

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

Then $\langle a \rangle$ is maximal if and only if $a$ is irreducible.

**Proof.** $(\Rightarrow)$ We have to show we have it as $R$ is an integral domain

- $a \neq 0$, $a \neq 1$, and $a$ is not a zero divisor
- If $a = bc$, then either $b \in U(R)$ or $c \in U(R)$.
- Since $I$ is maximal, it is a proper ideal. So $a \neq 1$. 

Maximal ideals and irreducible elements

\[ a = bc \in \langle a \rangle \Rightarrow (b + \langle a \rangle)(c + \langle a \rangle) = 0 \text{ in } R/\langle a \rangle. \]

Since \( R/\langle a \rangle \) is a field, we get that

either \( b + \langle a \rangle = 0 + \langle a \rangle \) or \( c + \langle a \rangle = 0 + \langle a \rangle \).

And so either \( b \in \langle a \rangle \) or \( c \in \langle a \rangle \).

Without loss of generality, let’s assume \( b \in \langle a \rangle \). So \( b = ar \) for some \( r \in R \). So \( a = bc = arc \). By the cancellation law we deduce \( rc = 1 \); this implies \( c \in U(R) \).

(\( \Leftarrow \)) Suppose \( \langle a \rangle \not\subseteq J \) and \( J \not\subseteq R \). Since \( R \) is a PID, \( J = \langle b \rangle \) for some \( b \notin \langle a \rangle \). Since \( a \in \langle b \rangle \), there is \( r \in R \) such that \( a = br \). As \( a \) is irreducible, either \( b \) is a unit or \( r \) is a unit.

If \( b \) is a unit, then \( \langle b \rangle = R \).

If \( r \) is a unit, then \( b = r^{-1}a \in \langle a \rangle \); and this is a contradiction. So overall we get that \( \langle a \rangle \) is maximal.
Corollary. Let $D$ be a PID. Suppose $\alpha$ is irreducible in $D$.

Then $D/<\alpha>$ is a field.

Corollary. If $\alpha \in \mathbb{C}$ is an algebraic number, then

$\text{Im } \phi_\alpha$ is a field.

**Proof.** By the fundamental homomorphism theorem

$$\mathbb{Q}[x]/\ker \phi_\alpha \cong \text{Im } \phi_\alpha.$$  

By part 1 of a theorem proved earlier, $\ker \phi_\alpha = <m_\alpha(x)>$ where $m_\alpha(x) \in \mathbb{Q}[x]$ is irreducible. So by the previous corollary $\mathbb{Q}[x]/<m_\alpha(x)>$ is a field, which implies $\text{Im } \phi_\alpha$ is a field.

So, if $\alpha \in \mathbb{C}$ is an algebraic number, then

1. $m_\alpha(\alpha) = 0$ and
2. $f(\alpha) = 0$ if $f(x) = m_\alpha(x)q(x)$ and $f(x) \in \mathbb{Q}[x]$

If $\deg m_\alpha = d_\alpha$, then

$$\mathbb{Q}[x]:= \{ \sum c_k \alpha^k : c_k \in \mathbb{Q} \text{ and } \sum_k c_k \alpha^k \neq 0 \}$$

is a field.
When do we have that $R/I$ is an integral domain?

Investigation. Since $R$ is a unital commutative ring,

$R/I$ is an integral domain $\iff$ 1 $R/I \neq 0$

\[ \iff 1 \ R \neq I. \]

2. $(x+I)(y+I) = (0+I)$ implies either $x+I = 0+I$
   or $y+I = 0+I$

\[ \iff 1 \ I \text{ is a proper ideal} \quad 2 \ xy \in I \implies (x \in I \text{ or } y \in I). \]

Def. Let $R$ be a unital commutative ring. An ideal $I$ of $R$ is called a prime ideal if

1. $I$ is proper, and
2. $\forall x, y \in R$, $xy \in I \implies (x \in I \text{ or } y \in I)$.

Theorem. Let $R$ be a unital commutative ring, and $I \triangleleft R$.

Then $I$ is a prime ideal if and only if $R/I$ is an integral domain.

(We have already proved it.)

Corollary. In a commutative unital ring, a maximal ideal is prime.

1. If $I$ is maximal, then $R/I$ is a field. So $R/I$ is an integral domain which implies $I$ 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 if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n$ 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 $0\mathbb{Z}$ is a prime ideal, but not a maximal ideal. Overall we have:

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

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

Ex. Suppose $R$ is a unital commutative ring, and $I \trianglelefteq R$, and $R/I$ is finite. Then $I$ is a prime ideal if and only if $I$ is a maximal ideal.
Proof. \( I \) is prime \( \iff \mathbb{R}/I \) is an integral domain.

Since a finite integral domain is a field and \( \mathbb{R}/I \) is finite, we get that \( I \) is prime \( \iff \mathbb{R}/I \) is a field.

On the other hand, \( \mathbb{R}/I \) is a field \( \iff \) \( I \) is a maximal ideal. \( \blacksquare \)

As it was mentioned at the beginning of the course, algebra was developed in order to study zeros of polynomials. We notice that an arbitrary polynomial in \( F[x] \), where \( F \) is a field, can be written as a product of irreducible polynomials:

1. If \( f(x) \) is irreducible, we are done;

2. If not, write \( f(x) \) as a product of smaller degree polynomials and continue this process for each one of the factors.

So suppose \( f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_k(x) \) where \( p_i(x) \) are irreducible in \( F[x] \). Now, if \( \alpha \) is a zero of \( f \) (in a field \( E \)), then \( 0 = p_1(\alpha) \cdot p_2(\alpha) \cdot \ldots \cdot p_k(\alpha) \), which implies \( \alpha \) is a zero of \( p_{i_0}(x) \) for some \( i_0 \). Therefore we can focus on zeros of irreducible polynomials.
We would like to study zeros of an irreducible polynomial $p(x) \in \mathbb{F}[x]$ in a possibly larger field $E$. But the question is if there is a field $E$ which contains a zero of $p$.

For instance, the fundamental theorem of algebra states that any polynomial $f(x) \in \mathbb{C}[x]$ of degree $\geq 1$ has a zero in $\mathbb{C}$. But how about a polynomial in $\mathbb{Z}_p[x]$?

**Theorem.** Let $F$ be a field, and $p(x)$ be an irreducible polynomial in $F[x]$. Then, there are a field $E$, an embedding $i : F \hookrightarrow E$, and $\alpha \in E$ such that

$$i(p)(\alpha) = 0,$$

where $i \left( \sum_{j=0}^{\infty} c_j \cdot x^j \right) = \sum_{j=0}^{\infty} i(c_j) \cdot x^j$.

(We often simply write $p(\alpha) = 0$ with an understanding that we are viewing $F$ as a subfield of $E$).

**Idea of the proof.**

Suppose we have found such $(E, \alpha)$. Let $\phi_\alpha : F[x] \to E$ be the evaluation at $\alpha$. Then

$\exists$ an irreducible polynomial $m_\alpha(x) \in F[x]$ such that

$\ker \phi_\alpha = \langle m_\alpha(x) \rangle$; and $F[x]/\langle m_\alpha(x) \rangle \cong F[\alpha]$, where

$F[\alpha] = \text{im } \phi_\alpha$ is a field.

Since $p(\alpha) = 0$, we get $p(x) \in \ker \phi_\alpha$; which implies
\( p(x) = m_\alpha(x) q(x) \) for some \( q(x) \in F[x] \). Since \( p \) is irreducible, either \( m_\alpha \) is a unit or \( q \) is a unit (in \( F[x] \)). Since \( m_\alpha \) is irreducible, it is not a unit. Therefore \( q(x) \in U(F[x]) \), and so \( q \in F \setminus \{0\} \), which implies \( m_\alpha(x) = q^{-1} p(x) \), and so \( \langle m_\alpha(x) \rangle = \langle p(x) \rangle \). So we should let \( E = F[x]/\langle p(x) \rangle \), and the poly. which under the evaluation at \( \alpha \) is mapped to \( \alpha \) is the polynomial \( x \). So we should let \( \alpha = x + \langle p(x) \rangle \).

**Proof.** Since \( p(x) \) is irreducible and \( F[x] \) is a PID, we have that \( \langle p(x) \rangle \) is a maximal ideal. Therefore \( E = F[x]/\langle p(x) \rangle \) is a field. Let \( \iota: F \to E \) be \( \iota(c) = c + \langle p(x) \rangle \).

\( \iota \) is a ring homomorphism.

\[
\iota(c_1 + c_2) = (c_1 + c_2) + \langle p(x) \rangle = \left( c_1 + \langle p(x) \rangle \right) + \left( c_2 + \langle p(x) \rangle \right) = \iota(c_1) + \iota(c_2).
\]

\[
\iota(c_1 c_2) = c_1 c_2 + \langle p(x) \rangle = \left( c_1 + \langle p(x) \rangle \right) \left( c_2 + \langle p(x) \rangle \right) = \iota(c_1) \iota(c_2).
\]

**Injective.** Suppose \( \iota(c) = 0 \). Then \( c + \langle p(x) \rangle = \langle p(x) \rangle \).
Then \( c \in \langle p(x) \rangle \). Since \( \langle p(x) \rangle \) is a proper ideal,

\[
\langle p(x) \rangle \cap U(F^{\times}) = \emptyset.
\]

So \( \langle p(x) \rangle \cap (F\setminus\mathbb{Q}) = \emptyset \). On the other hand, \( c \in \langle p(x) \rangle \cap F \).

Therefore \( c = 0 \).

\[
\alpha = x + \langle p(x) \rangle \quad \text{is a zero of } i(p)(x).
\]

Suppose \( p(x) = \sum_{j=0}^{n} c_j x^j \). We have to show

\[
i(c_0) + i(c_1)\alpha + \ldots + i(c_n)\alpha^n = 0
\]

in \( E = F[x]/\langle p(x) \rangle \).

\[
i(c_0) + i(c_1)\alpha + \ldots + i(c_n)\alpha^n = (c_0 + \langle p(x) \rangle) + (c_1 + \langle p(x) \rangle)\alpha + \ldots + (c_n + \langle p(x) \rangle)\alpha^n
\]

\[
= \frac{\langle c_0 + c_1 x + \ldots + c_n x^n \rangle + \langle p(x) \rangle = p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle}{\text{in } E = F[x]/\langle p(x) \rangle}.
\]

We say \( E \) is a field extension of \( F \), which has a zero of \( p(x) \).