Last Time:

- Gauss Lemma
- \( \text{f irred mod } p \Rightarrow \text{irred ov } \mathbb{Q} \)
- Eisenstein.

\[ \text{Lemma: Let } f, g \in \mathbb{Z}[x] \text{ be primitive, } \]
\[ \text{so } \gcd(\text{coefficient of } f) = \pm 1, \ f \neq 0, \]
\[ \text{and likewise for } g. \text{ Then } fg \text{ is primitive.} \]

- By induction on degree of \( fg \). Obvious when \( fg \) constant: \( fg = \pm 1 \).
- Suppose true for \( \deg(fg) \leq d \), and let

\[ f = a_nx^n + \ldots + a_0 \quad \text{and } \quad g = b_mx^m + \ldots + b_0. \]

\[ m + n = d + 1, \quad f, g \text{ primitive.} \]

Write \( f = ax^n + A \tilde{f}(x) \) where \( A = \gcd(a_{n-1}, \ldots, a_0), \ \tilde{f}(x) \text{ primitive.} \)

Thus

\[ fg = (anb + \tilde{f}(x)) + A \tilde{f}(x)g(x), \]
\[ \text{primitive, primitive, by induction.} \]

Thus \( \gcd(\text{coeffs of } fg) = \gcd(anA) = \pm 1 \) by assumption on \( f \).
Bases of fields

Recall the basic construction of new fields for all $f$:

1. Given $F$, if $\exists f \in F[x]$ s.t. $f$ is irreducible and has no roots in $F$, define a new ring $K = F[x]/(f)$.

   $K$ is a field and a fin-dim vector space over $F$.

2. This is more transcendental. Let $K = \text{Quot}(F[x])$.

   Now you can repeat (1) taking $F = K$.

Note: We've seen (1) produces a field before. For completeness: let $\alpha = x \in K$ be the image of $x$ under $F[x] \rightarrow K$. By long division of polynomials, any $h \in F[x]$ can be written $h = q \alpha^r + r$ where $\deg(r) < \deg(h)$. Moreover, given $h$ and $f$, $q$ and $r$ are unique; this shows $K = \text{Span}(\sum_{i=0}^{\deg(f)-1} x^i)$ as an $F$-vector space.

$K$ is a field b/c $F[x]$ is a PID and $(f) + (\alpha)$. Here $(f)$ is maximal.

Thinking now of $f$ as a polynomial of coeff's in $K$, note that $f(\alpha) = 0$ by def'n of $K$. Here we think of $K$ as the ring obtained by adjoining a root (any root!) of $f$ to $F$. 
Since our main tool for making/studying fields will be by solving polynomials, let's gather some basics.

**Def.** Let $R \subseteq S$ be rings. $y \in S$ is called algebraic over $R$ if $f(y) = 0 \in S$.

$S$ is called algebraic over $R$ if every $y \in S$ is algebraic over $R$.

**Def.** Let $L$ be a field. $L$ is called algebraically closed if every $f \in \mathbb{F}[x]$ has a root in $L$.

An algebraic closure for a field $K$ is a field $\overline{K}$ together with an embedding homomorphism $K \hookrightarrow \overline{K}$ such that:

1. $\overline{K}$ is algebraically closed.
2. $\overline{K}$ is algebraic over $K$.

We'll see:

The any field $K$ admits an algebraic closure $\overline{K}$.

$\overline{K}$ is unique up to $K$-linear isomorphism.
Proof. Fix a algebraic and \( f \in K[x], \ K \subset L. \)

TFAE:

1. \( f \) is monic and \( \text{deg}(f) = \text{deg}(f_K) \)
2. \( f \) is monic and \( f \) is a polynomial of least degree with \( f(a) = 0, \ a \neq 0. \)
3. \( f \) is monic, irreducible, and \( f(a) = 0. \)

\( \rightarrow (1) \Rightarrow (2): \) \( f = \text{Ker}(f_K) \Rightarrow f \) is least deg polynomial \( f(a) = 0; \) by Euclid, any two such polynomials related by a divisor \( d, \) have monicity define \( f. \)

\( (2) \Rightarrow (3): \) If \( f \) were reducible, \( f(a) = g(a) h(a); \) that \( g(a) h(a) = 0 \)

means \( a \) satisfies \( g \) or \( h, \) violating "least degree" of \( f. \) Monicity defines \( f. \)

\( (3) \Rightarrow (1): \) \( (0) = (f) \subset \text{Ker}; \) since \( f \) irreducible, \( \langle f \rangle \) is prime, and since \( PID \) has divisor \( 1, \ f = \text{Ker}. \) Monicity defines \( f \) among such generators. \( \Box \)

**Def.** The unique \( f \in K[x] \) as above is called the irreducible polynomial of \( a. \)

We can imagine adjoining a root \( \alpha \) to \( f, \) to obtain \( K_1 = K(\alpha). \)

Then \( \alpha \in K_1[x], \) and so forth. All these \( K_i \) will be fields containing the original \( K \) as a subfield.
So we review basic facts about field extensions.

**Def.** A field extension is a choice of homomorphism 
\[ K \to L, \]
where \( L, K \) are fields.

**Rmk.** Since \( L, K \) are fields, the homomorphism is an injection.

**Rmk.** We often say "let \( K \leq L \) be a field extension" by identifying \( K \) with the image; we also say "let \( L/K \) be an extension."

**Rmk.** We also say "\( L \) is an extension of \( K \)."

This makes \( L \) into a \( K \)-algebra, hence a \( K \)-module. (I.e., a \( K \)-vector space.)

**Def.** The dimension

\[ \dim_K L =: [L:K] \]

is called the **degree** of \( L \) over \( K \).

If the degree is finite, we say \( L \) is a **finite** extension of \( K \).
Prop: If $K \subseteq L$ is a finite extension, every $\alpha \in L$ is algebraic over $K$.

Proof: $1, \alpha, \ldots, \alpha^{[L:K]}$ cannot be linearly independent. Hence $\exists \lambda \in K^*$ such that

$$a_0 + a_1 \alpha + \cdots + a_{[L:K]} \alpha^{[L:K]} = 0.$$ 

Prop: Let $K \subseteq L$ be a field extension, $\alpha \in L$, and $K(\alpha) \subseteq L$ the subring generated by $\alpha$. If $\alpha$ is algebraic, $K(\alpha)$ is a field.

Proof: The induced map $K(\alpha) \rightarrow L$ has kernel since $\alpha$ is algebraic. Since $L$ a domain (field), kernel is prime, hence maximal since $K(\alpha)$ is a PID.

Prop: Let $\alpha$ be algebraic, and let $f \in K(\alpha)$ generate the kernel. Then

$$\dim_K K(\alpha) = \deg(f).$$

Proof: By any division, any $[g] \in K(\alpha)/f$ is represented by some $g \in K(\alpha)$ of degree $\leq \deg f$. Hence $1, \alpha, \ldots, \alpha^{\deg f-1}$ span $K(\alpha)$. Otherwise, they are linearly independent — else a lesser degree polynomial would be solvable by $\alpha$, contradicting $f$ generating $\alpha$. //
Prop. Let \( K_0 \subseteq K_1 \subseteq K_2 \) be fields.

Then

\[
[K_2 : K_0] = [K_2 : K_1] [K_1 : K_0].
\]

Proof: Let \( \alpha_1, \ldots, \alpha_n \) be a basis for \( K_1 \) over \( K_0 \)

\( \beta_1, \ldots, \beta_m \)

be a basis for \( K_2 \) over \( K_1 \).

We claim \( \alpha_i \beta_j \) is a basis for \( K_2 \) over \( K_0 \).

\text{Spanning: Obvious.} \quad y \in K_2 \Rightarrow y = \sum \beta_j \alpha_i \quad (\beta_j \in K_2 \text{ over } K_1)

\Rightarrow \quad \beta_j = \sum \alpha_i \beta_j \quad \quad (\alpha_i \in K_1 \text{ over } K_0)

\Rightarrow \quad y = \sum \alpha_i \beta_j \quad \quad (y \in K_2 \text{ over } K_0)

\text{Linear independence: If} \quad 0 = \sum_{ij} a_{ij} \alpha_i \beta_j \quad \text{(since } \beta_j \text{ are lin ind over } K_1) \quad \Rightarrow \quad 0 = \sum a_{ij} \beta_j \quad \text{(since } \alpha_i \text{ are lin ind over } K_0) \quad \Rightarrow \quad 0 = a_{ij} \forall ij \quad \text{(since } a_{ij} \text{ are lin ind over } K_0) \]

In what follows, it'll be convenient to know that algebraic closures exist.

\text{Def: A field } L \text{ is called algebraically closed if every } f \in L[x] \text{ has a root in } L. \]

An algebraic closure of \( K \) is an algebraically closed \( L \) such that \( L \) is algebraic over \( K \).

Thm: For any \( K \), an algebraic closure \( \overline{K} \) exists. Any two

are isomorphic as fields over \( K \).
Prop. Let \( L = K[x] \), if \( \phi \) is \( K \)-module homomorphism of \( K \)-algebras. Then for every root of \( f \in K \), \( \exists ! K \)-linear embedding \( L \rightarrow K \).

**Proof:**

\[
\begin{array}{ccc}
K[x] & \xrightarrow{\phi} & K \\
/ (f) & \phi & \\
\phi \circ \phi^{-1} : & \phi & \\
/ \alpha & \phi & \\
L & \phi^{-1} & \\
\end{array}
\]

So it suffices to show any \( K[x]/(f) \xrightarrow{\phi^*} K \) is uniquely determined by a choice of root \( \beta \). This is clear by \( \text{univ prop of quotients} \):

\[
\begin{array}{ccc}
K[x] & \xrightarrow{\phi} & K \\
/ (f) & \phi & \\
\phi^{-1} & \phi^{-1} & \\
/ \alpha & \phi & \\
L & \phi & \\
\end{array}
\]

- \( \phi \) uniquely determined by \( \phi(x) = : \beta \) (\( \text{univ prop of } K[x] \))
- \( \exists ! \phi \) iff \( f(\beta) = 0 \) (so \( f \in K[\bar{\beta}] \)), and \( \exists ! \phi \) when a lift exists. \( \Box \)
Prove that \( L/K \) be an extension of degree \( n \), and suppose \( L = K(\alpha) \), and let \( g \) be the minimal polynomial of \( \alpha \) (all coefficients in \( K \)).

TFAE:

1. \( L \) has a \( K \)-algebra map \( L \to \overline{K} \), for any algebraic closure \( \overline{K} \) of \( K \).
2. \( g \) has \( n \) distinct roots in any algebraic closure \( \overline{K} \) of \( K \).
3. \( \gcd(g, g') = 1 \) is a unit.
4. \( g' \neq 0 \).
5. Either \( \text{char}(K) = 0 \) or \( n(x^{p}) \) is a unit
   - If \( \text{char}(K) = p > 0 \), \( g \neq h^{p} \) for some \( h \in \overline{K}^{\times} \).
6. \( g'(\alpha) \neq 0 \).