Lecture 1, 4/3/23

Definition 0.1. A field extension $F \subseteq K$ is a field F, which is a subfield of a larger field K.
One way to keep track of how these are related is the degree, $[K : F]$. This is the dimension of K as a vector space over F.
If this degree is $< \infty$, then we refer to this as a finite extension (we of course do not mean that they are finite as sets)
If $S \subseteq K$, then $F(S)$ is the subfield of K given by $F \cup S$.
$F[S]$ is the sub-*ring* of K generated by $F \cup S$. These are different in general!
If $S = \{a_1, \ldots, a_n\}$, we use $F(a_1, \ldots, a_n)$ and $F[a_1, \ldots, a_n]$ to denote $F(S)/F[S]$.
If the extension has the form $F[a]$ for some element a, then this is called a simple extension. Here, a is called a primitive element.
An extension $F \subseteq K$ is called algebraic if every $k \in K$ is algebraic over F, meaning is the root of some polynomial in $F[x]$

Example 0.1.

- $Q \subseteq \mathbb{R}$. This is an infinite extension. Further, it is not an algebraic extension. The hard way to show this is to demonstrate that some element of $\mathbb{R}$ is not algebraic. For example, π, e are real, but transcendental over the rationals.

  The easy way is by a simple cardinality argument: Because $\mathbb{Q}$ is countable, $\overline{\mathbb{Q}}$ is, but $\mathbb{R}$ is not

- $\mathbb{R} \subseteq \mathbb{C}$. This is a finite extension. In fact, it is a simple extension, with primitive i.

- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5})$. This is algebraic. Of course, $\sqrt{5}$ is a root of $x^5 - 1$, but what about the other elements of $\mathbb{Q}(\sqrt{5})$?

  Consider $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. This is a subset of $\mathbb{Q}(\sqrt{5})$, a subring, and a subfield: indeed, consider $\frac{1}{a+b\sqrt{5}}$. The "typical high school trick" is to multiply by the conjugate:

  $$\frac{1}{a + b\sqrt{5}} \frac{a - b\sqrt{5}}{a - b\sqrt{5}} = \frac{a - b\sqrt{5}}{a^2 - 5b^2}$$

  So $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, as this is a subfield of $Q(\sqrt{5})$ which contains $\sqrt{5}$, so must contain $\mathbb{Q}(\sqrt{5})$. That is,

  $$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{5}]$$

  It is easy to see that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$

Let $F \subseteq K$ be a field extension, and consider $F[a_1, \ldots, a_n]$.
There exists an evaluation map $\varepsilon : F[X_1, \ldots, X_n] \to K$, given by $\varepsilon(f) = f(a_1, \ldots, a_n)$.
ε is a ring homomorphism, so $\mathrm{Im}(\varepsilon)$ is a subring of K. We have $F[a_1, \ldots, a_n] = \mathrm{Im}\,\varepsilon$
$F(a_1, \ldots, a_n)$ is a quotient field for the ring $F[a_1, \ldots, a_n]$
Let F be a field, x, y be indeterminants which are independent over F. Let $L = F(y)[x]/\langle x^2 - y \rangle$.
We can check that $x^2 - y$ is irreducible in $F(y)[x]$ because it is quadratic, and y has no square roots.
So because this is irreducible, L is a field.
In particular, $F(y)$ embeds in L via the natural map $F(y) \hookrightarrow F(y)[x] \twoheadrightarrow L$. So $F(y) \subseteq L$. This is a degree two extension of $F(y)$.

Proposition 1. *If $[K : F] < \infty$, then $F \subseteq K$ is an algebraic extension.*

Proof. Let $n = [K : F]$, and let $a \in K$. Look at $1, a, a^2, \ldots, a^n$. This is $n + 1$ elements in K, so they must be linearly independent over F. So there exists $c_0, c_1, \ldots, c_n$, not all zero, such that $\sum_{i=0}^{n} c_i a^i = 0$. Then $f = \sum_{i=0}^{n} c_i x^i \in F[x]$ is a polynomial to which a is a solution, so a is algebraic.

■

Theorem 0.1. *(I)*
Let $F \subseteq K$ be a field extension, $a \in K$. Then The Following Are Equivalent (TFAE):

1. *a is algebraic over F*

2. $\dim_F F[a] < \infty$

3. $[F(a) : F] < \infty$

4. $F(a) = F[a]$

Proof. Notice that $3 \Rightarrow 2$ are really saying the same thing. Further, $2 + 4 \Rightarrow 3$. So if we can connect 1, 2, 4, then 3 will come along for the ride. Therefore, it is enough to show that $1, 2, 4$ are equivalent.

$1 \Rightarrow 2$

There exists a nonzero $f \in F[x]$ such that $f(a) = 0$. $f = \sum_{i=0}^{n} c_i x^i$, where $c_n \neq 0$. So $\sum_{i=0}^{n} c_i a^i = 0$, and so $a^n = \sum_{i=0}^{n-1} d_i a^i$, with $d_i \in F$ new coefficients.

Set $V = \sum_{i=0}^{n-1} Fa^i$. Then $a^n \in V$. So

$$\begin{aligned} a^{n+1} &= \sum_{i=0}^{n-1} d_i a^{i+1} \\ &= \sum_{j=1}^{n-1} d_{j-1} a^j + d_{n-1} a^n \end{aligned}$$

But $d_{n-1}a^n = \sum_{i=0}^{n-1} d_{n-1}d_i a^i$.
Induction gets us that $a^j \in V$ for all $j \geq 0$.
So V is closed under multiplication, hence a subring of K.
So $V = F[a]$. Note $\dim_F F[a] = \dim_F V \leq n$, because we used n elements to span in the first place.

$2 \Rightarrow 4$

It will be enough to show $F[a]$ is a field.
Let $x \in F[a]$, $x \neq 0$. Define a map $\mu_x : F[a] \to F[a]$, given by $\mu_x(y) = xy$. This is F-linear, and $\ker \mu_x = 0$. We have an injective linear transformation from a finite dimensional vector space to itself, so it has to be an isomorphism onto its image. So there exists $x' \in F[a]$ so that $\mu_x(x') = 1$, so x is invertible.

Lecture 2, 4/5/23

We continue the proof.

$4 \Rightarrow 1$

If $A = 0$, we are done. If $A \neq 0$, then $\frac{1}{a} \in F(a) = F[a]$.
So $\frac{1}{a} = \sum_{i=1}^{m} c_i a^i$ where each $c_i \in F$. Note $1 = \sum_{i=0}^{m} c_i a^{i+1}$, so a is a root of $-1 + \sum_{i=0}^{m} c_i x^{i+1} = 0$
Thus a is algebraic over F.

■

Theorem 0.2. *Assume a is algebraic over K.*

(i) There exists a unique monic polynomial $p \in F[x]$ such that $p(a) = 0$ with minimal degree. We call this the minimal polynomial for a over F, and write $p_{a,F}$.

(ii) p is irreducible.

(iii) *If $g \in F[x]$, $g(a) = 0$, then $p \mid g$ in $F[x]$.*

(iv) $[F(a) : F] = \deg p$

(v) *If $n = \deg p$, then $(1, a, a^2, \ldots, a^{n+1})$ is a basis for $F(a)$ over F.*

(vi) *Let $\varepsilon : F[x] \to K, \varepsilon(f) = f(a)$. This induces an isomorphism of rings $\overline{\varepsilon} : \frac{F[x]}{\langle p \rangle} \to F(a), \overline{\varepsilon}(f + \langle p \rangle) = f(a)$*

Proof.

(i) Since a is algebraic over F, there exists $f \in F[x]$ such that $f(a) = 0$. Note that we can divide by the leading coefficient to make f monic with a as a root. Find minimal polynomial of this form, and call it p.

Uniqueness: Suppose $p' \in F[x]$ is monic, $p'(a) = 0$ minimal. Then $(p - p')(a) = 0$. Since $\deg(p - p') < \deg p$, if $p - p' \neq 0$, we have found a monic polynomial with smaller degree than p with a as a root. Contradiction

(ii) Let $\varepsilon : F[x] \to F(a) = F[a]$ be the evaluation map. ε induces $\overline{\varepsilon} : \frac{F[x]}{\ker \varepsilon} \to F(a)$. Note $\ker \varepsilon = 0$. Since $F[x]$ is a PID, $\ker \varepsilon = \langle q \rangle$ where $0 \neq q \in F[x]$. Without loss of generality, assume q is monic. We know

- q is irreducible
- $q(a) = 0$
- When $g \in F[x], g(a) = 0$, then $q \mid g$

Thus, if $g \neq 0$, $\deg(q) \leq \deg(g)$. This implies that $q = p$.

(iii) See above

(iv) $\overline{\varepsilon}$ is also an isomorphism of vectors over F. Exercise: If $x \in X + \langle p \rangle$, then $(1, x, x^2, \ldots, x^{n+1})$ is a basis for $\frac{F[x]}{\langle p \rangle}$. Thus $(1, a, a^2, \ldots, a^{n-1})$ is a basis for $F(a)$

Furthermore, $[F(a) : F] = n = \deg p$

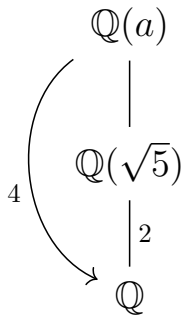
■

Let $F \leq K$ be a field extension, $a \in K$ algebraic over F. If $p \in F[x]$ is monic and irreducible with $p(a) = 0$, then $p = p_{a,F}$

(v) See iv

(vi) See ii

Example 0.2. Let $a = \sqrt[4]{5} \in \mathbb{R}_{>0}, p = X^4 - 5 \in \mathbb{Q}[x]$. Since p is irreducible over $\mathbb{Q}[x]$, $p = p_{a,F}$.
Note that p is reducible over $\mathbb{Q}(\sqrt{5})[x]$. In fact, $p_{a,\mathbb{Q}[\sqrt{5}]} = x^2 - \sqrt{5}$. We have the tower of fields:



Let $F \subseteq K \subseteq L$ be a tower of fields. If $a \in L$ is algebraic in F, then a is also algebraic over K. Furthermore, $p_{a,K} \mid p_{a,F}$ in $K[x]$.

Proposition 2. *If $f \in F[x]$ is a nonzero polynomial of degree n, then f has at most n roots in n.*

Proof. By induction.
$n = 0$: trivial.
$n > 0$: if there are no roots, we're okay.
Otherwise, there exists $a \in F$ such that $f(a) = 0$. So $f = (x - alg$, for some $g \in F(x)$.
$g \neq 0, \deg g = n - 1$. Thus g has $\leq n - 1$ roots in F.
Since $\{\text{roots of } f\} = \{a\} \cup \{\text{roots of } g\}$, there are $\leq n$ roots of f.
Let $F \subseteq K$ be a field extension. Let $\mathcal{A} = \{a \in K, a \text{ algebraic over } F\}$.
If F is infinite, then $|\mathcal{A}| = |F|$. If F is finite, $|\mathcal{A}|$ is countable.
Let $\mathbb{A}$ denote the complex numbers which are algebraic over $\mathbb{Q}$. Note $|\mathbb{A}| = |\mathbb{Q}| = \aleph_0$

Lecture 3, 4/7/23

Theorem 0.3. *(Tower rule)*
Let $F \subseteq K \subseteq L$ be a tower of fields. Then $[K : F][L : K] = [L : F]$.

Proof. If $[K : F] = \infty$ or $[L : K] = \infty$, we are done.
So assume $[K : F] = m, [L : K] = n, m, n < \infty$.
Let $\{b_1, \ldots, b_n\}$ be a basis for L over K, and let $\{a_1, \ldots, a_m\}$ be a basis for K over F.
We claim $\{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for L over F.
We check it spans: choose $x \in L$. Note $x = \sum_{j=1}^{n} u_j b_j$, where each $u_j \in K$. Each $u_j = \sum_{i=1}^{m} v_{ij} a_i$, where each $v_{ij} \in F$. Thus $x = \sum_{j=1}^{n} \sum_{i=1}^{m} v_{ij} a_i b_j$

Linear independence: suppose $\sum_{i=1}^{m} \underbrace{\sum_{j=1}^{n} v_{ij} a_i \, b_j}_{\in K} = 0$.

Thus $\sum_{j=1}^{n} v_{ij} a_i = 0$. Thus all $v_{ij} = 0$.

■

Corollary 0.4. *Let $F \subseteq K$ be a field extension, $a_1, \ldots, a_n \in K$ all algebraic over F. Then $F[a_1, \ldots, a_n] = F(a_1, \ldots, a_n)$ and $[F(a_1, \ldots, a_n) : F] < \infty$.*

Corollary 0.5. *Let $F \subseteq K$ be a field extension.*

(a) If $a, b \in K$ are algebraic over F, then $[F(a) : F] \mid [F(a,b) : F], [F(b) : F] \mid [F(a,b) : F], pF(a,b) : F] \leq [F(a) : F], [F(b) : F]$

(b) $\{a \in K \mid a$ algebraic over $F\}$ is a subfield of K.

(c) If $S \subseteq K$ is a set of elements algebraic over F, then $F(S)$ is algebraic over F.

(d) Say $K \leq L$ is a field extension. Then L is algebraic over F if and only if L is algebraic over K and K is algebraic over F.

Proof. ■

Definition 0.2. Let $F \subseteq K$ be a field extension. An $\underline{F\text{-automorphism of } K}$ is any isomorphism $\phi : K \to K$ such that $\phi|_F = \mathrm{Id}_F$.
The $\underline{\text{Galois group}}$ of K over F is $G(K : F) = \{F-\text{automorphisms of } K\}$

Proposition 3. *Let $F \subseteq K$ be a field extension, $\phi \in G(K : F)$, f a polynomial in $F(x)$. Then ϕ permutes $\underbrace{\{a \in K \mid f(a) = 0\}}_{R_f}$.*

Proof. :
Let $f = \sum_{i=1}^{n} c_i x^i$, wheree $c_i \in F$.
Choose $a \in K$. $\phi(f(a)) = \phi(\sum_{i=1}^{n} c_i a^i) = \sum_{i=1}^{n} c_i \phi(a_i) = f(\phi(a))$.
Thus $a \in R_f \iff \phi(a) \in R_f$.
So ϕ restricts mto an injective map $R_f \to R_f$. Thus there is a bijection.

■

Example 0.3. $\mathbb{R} \subseteq \mathbb{C}$. $\phi \in G(\mathbb{C} : \mathbb{R})$ must permute roots of $x^2 + 1$, so $\phi(i) = \pm i$. ϕ is $\mathbb{R}$-linear and $(1, i)$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.
Thus $G(\mathbb{C} : \mathbb{R}) = \{\mathrm{Id}, \overline{-}\}$

Example 0.4. Let $F \subseteq K$ be a field extension of degree 2, $\mathrm{char}\, F \neq 2$.
Chose $a \in K \setminus F$. Note $F[a] = F(a) = K$. So a is algebraic over F, $\deg p_{a,F} = 2$. We know $p_{\alpha,F} = X^2 + bX + c$.

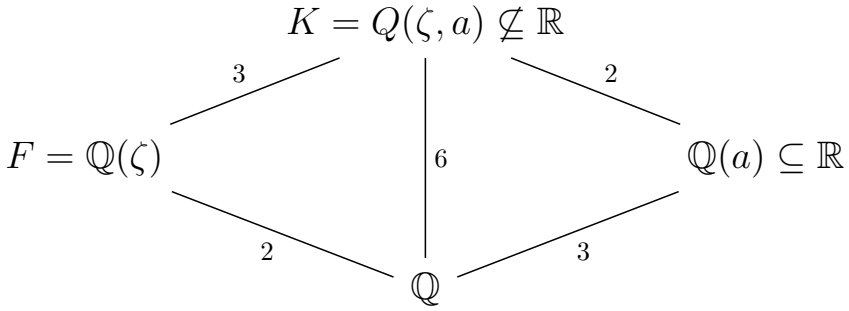
By quadratic formula,

$$a = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

i.e. there is some $r \in K$ such that $r^2 = b^2 - 4ac$ and $a = \frac{-b+r}{2}$.
$\frac{-b-r}{2}$ is another root of $p_{\alpha,F}$. Since $a \notin F, r \notin F$. So $r \neq 0$, i.e. $r \neq -r$.
Thurs $F[r] = F(r) = K$. So $p_{\alpha,F} = X^2 - (b^2 - 4c)$.
If $\phi \in \mathrm{Gal}(K : F)$, $\phi(r) = \pm r$.
Thus $|\mathrm{Gal}(K : F)| \leq 2$.
Exercise: $|\mathrm{Gal}(K : F)| = 2$.

Example 0.5. See chapter 2: there exists $F \subseteq K, [K : F] = 2, \mathrm{char}\, F = 2, \mathrm{Gal}(K : F) = \{e\}$.

Example 0.6. $F = \mathbb{Q}(\zeta) \subseteq K = \mathbb{Q}(\zeta, a), \zeta = e^{\frac{2\pi i}{3}}, a = \sqrt[4]{5} \in \mathbb{R}$.
ζ is a root of $X^3 - 1 = (X - 1)(X^2 + X + 1)$.
Thus $p_{\zeta,\mathbb{Q}} \mid X^2 + X + 1$. Since $\zeta \notin \mathbb{Q}, \deg p_{\alpha,\mathbb{Q}} \mid X^2 + X + 1$.
Since $\zeta \notin \mathbb{Q}, \deg p_{\zeta,\mathbb{Q}} > 1$. Thus $p_{\zeta,\mathbb{Q}} = X^2 + X + 1, [F : \mathbb{Q}] = 2$
Now note a is a root of $X^3 - 5$, which is irreducible.
Thus $p_{a,\mathbb{Q}} = X^3 - 5, [\mathbb{Q}(a) : \mathbb{Q}] = 3$.



Lecture 4, 4/10/23

Definition 0.3. Let $F \subseteq K$ be a field extension, $F[X]$ a polynomial ring. $f \in F[X]$ splits over K if $f = a_0(X - a_1)(X - a_2)\cdots(X - a_n)$ for $a_i \in K$. 4

Definition 0.4. A splitting field for $S \subseteq F[X]$ over F is a field K containing F such that all $f \in S$ split over K, and K is minimal. In other words, if $F \subseteq E \subseteq K$, and for all $f \in S, f$ splits over E, then $E = K$.

Definition 0.5. F is algebraically closed if every $f \in F[X]$ splits over F.

Definition 0.6. An algebraic closure of F is a field extension K containing F such that $F \subseteq K$ is algebraic and K is algebraically closed.

Theorem 0.6. *(Fundamental theorem of algebra)*
$\mathbb{C}$ *is algebraically closed.*
$\mathbb{C}$ *is an algebraic closure of* $\mathbb{R}$*, and is thus a splitting field for* X^2+1 *over* $\mathbb{R}$*.*
Another splitting field for X^2+1 *over* $\mathbb{Q}$ *is* $\mathbb{Q}(i)$*.*
A splittinng field for X^3-2 *over* $\mathbb{Q}$ *is* $\mathbb{Q}(a,\zeta)$*,* $a=\sqrt[3]{2}, \zeta$ *a root of* X^2+X+1*.*
$X^3-2=(X-a)(X-a\zeta)(X-a\zeta^2)$

$$\begin{array}{ccc} \mathbb{Q}(a,\zeta) & & \mathbb{Q}(\zeta)(a) \\ \Big| 6 & & 3 \Big| \\ \mathbb{Q} & & \mathbb{Q}(\zeta) \\ & & 2 \Big| \\ & & \mathbb{Q} \end{array}$$

Let $F \subseteq K$ *be3 a field extension,* $F[X]$ *a polynomial ring. Say* K *is a splitting field for* $S \subseteq F[X]$ *over* F*. Define*

$$R \stackrel{\text{def}}{=} \{a \in K \mid f(a)=0 \text{ for some } f \in S\}$$

Then $K=F(R)$*. So* K *is algebraic over* F*.*

Claim. *Suppose* K *is a splitting field over* F *for some non-constant* $f \in F[X]$*. Let* $a_1,\dots,a_r$ *be the roots of* $f \in K$*. Then we know* $K=F(a_1,\dots,a_r)$*. Wee claim that* $[K:F] \leq (\deg f)!$*.*

Proof. Let $n=\deg f$. We know $p_{a,F} \mid f$, so $[F(a_1) \mid F]=\deg p_{a_1,F} \leq \deg f = n$.
So $f=(X-a_1)g$, where $\deg g = n-1$.
The roots of g are $\subseteq \{a_1,\dots,a_r\}$. Thus $K=F(a_1)(a_1,\dots,a_r)$.
By induction, $[K:F(a_1)] \leq (n-1)!$.
By the tower rule, $[K:F] \leq n!$.

■

Claim. *Suppose* K *is algebraically closed. Take* L *to be the algebraic closure of* F *in* K*. Then* L *is algebraically closed.*

Proof. If $f \in L[X]$ is not constant, it has a root $a \in K$.
$L \subseteq L(a)$ is algebraic, $F \subseteq L$ is algebraic, so $F \subseteq L$ is algebraic, thus $L(a) \subseteq L$.
This implies that f has a root in L.

■

Say R, S are rings, $R[X], S[X]$ polynomial rings, $\phi : R \to S$ a ring homomorphism. Then there exists a unique ring homomorphism $\tilde{\phi} : R[X] \to S[X]$ such that $\tilde{\phi}|_R = \phi$ and $\tilde{\phi}(X)=X$.

Formula:

$$\tilde{\phi}\left(\sum_{i=0}^{d} r_i X^i\right) = \sum_{i=0}^{d} \phi(r_i) X^i$$

Theorem 0.7 (Kronecher's Theorem)**.** *Let F be a field, $f \in F[X]$ a non-constant polynomial. Then there exists a field extension $F \subseteq K$ such that f has a root in K, and $[K : F] \leq \deg f$.*

Proof. Let p be some irreducible factor of f.
Define $L = F[X]/\langle p \rangle$, which is a field.
Let $\overline{h} = h + \langle p \rangle$ for $h \in F[X]$.
Define $\phi : F \to L$ by $\phi(c) = \overline{c}$. We have $\tilde{\phi} : F[X] \to L[X]$.
We claim $\overline{X}$ is a root of $\tilde{\phi}(f)$.
$p = \sum_{i=0}^{n} c_i X^i$, $c_i \in F$.
Then $\tilde{\phi}(p) = \sum_{i=0}^{m} \overline{c_i} X^i$

$$\begin{aligned}
\tilde{\phi}(p)(\overline{X}) &= \sum_{i=0}^{m} \overline{c_i}\,\overline{X^i} \\
&= \overline{\sum_{i=0}^{m} c_i X^i} \\
&= \overline{p} \\
&= \overline{0}
\end{aligned}$$

Thus $\overline{X} \in L$ is a root of $\tilde{\phi}(f)$.

Lecture 5, 4/12/23

We continue the proof.
Choose a set U disjoint from F with $|U| = |L \setminus \phi(F)|$. Say $\beta : U \to L \setminus \phi(F)$ is a bijection.
Extend to a bijection $\beta : F \coprod U \to L$ such that $\beta(a) = \phi(a)$ for all $a \in F$.
Define $+, \cdot$ on $F \coprod U$ by

$$\begin{aligned}
-a + b &= \beta^{-1}(\beta(a) + \beta(b)) \\
-a \cdot b &= \beta^{-1}(\beta(a)\beta(b))
\end{aligned}$$

we need to check new $+, \cdot$ agree with OG on F. We also need to check that $F \coprod U$ is a field. We will do this later.
Define $K = F \coprod U$. Note F is a subfield of K. $\beta : K \to L$ is an isomorphism,$\beta|_F = \phi$.
Define $p = \sum_{i=0}^{m} c_i X^i, c_i \in F$.

$$\begin{aligned} 0 &= \tilde{\phi}(p)(\overline{X}) \\ &= \sum_{i=0}^{m} \phi(c_i)\overline{X^i} \\ &= \sum_{i=0}^{m} \beta(c_i)\beta(\beta^{-1}(\overline{X}))^i \\ &= \beta\left(\sum_{i=0}^{m} c_i \beta^{-1}(\overline{X})^i\right) \\ &= \beta(p(\beta^{-1}(\overline{X})) \end{aligned}$$

thus $p(\beta^{-1}(\overline{X})) = 0$.
$[K : F] = \dim_F K = \dim_F L = \deg p \leq \deg f$.

■

Ordinals

I'm not typing all this up i don't get it

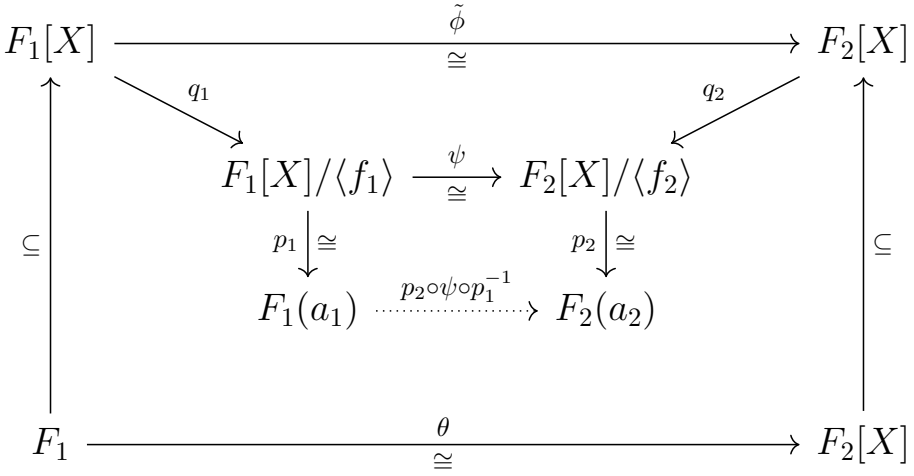
Lecture 6, 4/14/23

Lemma 1 (Extension Lemma)**.** *Let $F_1 \subseteq K_1, F_2 \subseteq K_2$ be field extensions, $\phi : F_1 \to F_2$ an isomorphism. Let $F_2[X]$ be a polynomial ring, $f_1 \in F_1[X]$ irreducible, $f_2 = \tilde{\phi}(f_1)$, $a_i \in K_i$ a root of f_i. Then ϕ extends to an isomorphism $\theta : F_1(a_1) \to F_2(a_2)$ such that $\theta(a_1) = a_2$.*

$$\begin{array}{ccc} K_1 & & K_2 \\ | & & | \\ F(a_1) & \overset{\exists\theta}{\dashrightarrow} & F(a_2) \\ | & & | \\ F_1 & \xrightarrow{\theta} & F_2 \end{array}$$

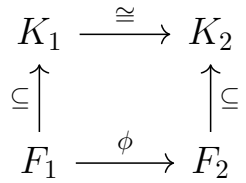
The proof is in the form of this diagram, I guess:

Proof.



■

Theorem 0.8. *Let F_1, F_2 be fields, $F_2[X]$ a polynomial ring, $S_i \subseteq F_i[X]$, and let $\phi : F_1 \to F_2$ be an isomorphism, where $\phi_1(S_1) = S_2$. Let K_i be a splitting field of S_i over F_i. Then ϕ extends to an isomorphism $K_1 \to K_2$.*



Proof. Set $\mathscr{M} = \{(L, \theta) \mid F_1 \subseteq L \subseteq K_1$ a tower, $\theta : L \to K_2$ a homomorphism extending $\phi\}$.
Define $(L_1, \theta_1) \leq (L_2, \theta_2)$ iff $L_1 \subseteq L_2$, $\theta_1 \subseteq \theta_2$

- $\leq$ is a partial ordering of $\mathscr{M}$.
- $(F_1, \theta) \in \mathscr{M}$.
- If $\{(L_i, \theta_i)\}_{i\in I}$ is a nonempty chain on $\mathscr{M}$, then

$$\left(\bigcup_{i\in I} L_i, \bigcup_{i\in I} \theta_i\right) \in \mathscr{M}$$

  is an upper bound for the chain.

By Zorn's lemma, there exists a maximal $(M, \psi) \in \mathscr{M}$

$$\begin{array}{ccc} K_1 & \xrightarrow{\cong} & K_2 \\ | & & | \\ M & \xrightarrow[\cong]{\psi} & M' = \psi(M) \\ \subseteq\uparrow & & \uparrow\subseteq \\ F_1 & \xrightarrow{\phi} & F_2 \end{array}$$

Towards contradiction, suppose $M \subsetneq K_1$
Then there exists some $g \in S_1$ which does not split over M. In $M[X]$, there exists an irreducible factor $f \mid g$ such that $\deg f \geq 2$
g splits over K, so f splits over K.
Thus f has a root $a_1 \in K_1$.
$\tilde{\psi}(f) \in M'$ is irreducible, has a root $a_2 \in K_2$, because $\tilde{\psi}(f) \mid \tilde{\psi}(g) = \tilde{\phi}(g)$ in $M'[X]$.
By Extension Lemma, ψ extends to an isomorphism $\theta : M(a_1) \to M'(a_2)$.
Now $(M(a_2), \theta) \in \mathscr{M}$, contradicting that (M, ψ) is the maximal element.

■

Corollary 0.9. *Let F_1, F_2 be fields, $\phi : F_1 \to F_2$ an isomorphism, K_i an algebraic closure of F_i. Then ϕ extends to an isomorphism $K_1 \to K_2$.*

Proof. Observe that K_i is a splitting field for $S_i = F_i[X]$ over F_i. $\tilde{\phi}(S_1) = S_2$. Apply the previous theorem.

■

Example 0.7. $K = \mathbb{Q}(a, \zeta) \subset \mathbb{C}$, $a = \sqrt[3]{5}$, $\zeta =$ a root of $X^2 + X + 1$.
Roots of $X^3 - 5 : a, a\zeta, a\zeta^2$
Roots of $X^2 + X + 1 : \zeta, \zeta^2$

$$K = \mathbb{Q}(a, \zeta) = \mathbb{Q}(a\zeta, \zeta) = \mathbb{Q}(a\zeta^2, \zeta)$$

$$\begin{array}{ccccc} K = \mathbb{Q}(a, \zeta) & = & \mathbb{Q}(a\zeta, \zeta) & = & \mathbb{Q}(a\zeta^2, \zeta) \\ \Big|{\scriptstyle 2} & & \Big|{\scriptstyle 2} & & \Big|{\scriptstyle 2} \\ \mathbb{Q}(a\zeta) & & \mathbb{Q}(a\zeta) & & \mathbb{Q}(a\zeta^2) \\ & \searrow^{3} & \Big|{\scriptstyle 3} & \swarrow_{3} & \\ & & \mathbb{Q} & & \end{array}$$

$i = 0, 1, 2$, there exists $\mathbb{Q}$-automorphism $\phi_i : \mathbb{Q}(a) \to \mathbb{Q}(a, \zeta^i)$ such that $\phi_i(a) = a\zeta^i$.
ϕ_i extends to $\phi_{ij} : K \to K$ such that $\phi_{ij}(\zeta) = \zeta^j$

Lecture 7, 4/17/23

Exercise: $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
Let $a = e^{\frac{2}{5}\pi i}$. $\mathrm{Gal}(\mathbb{Q}(a):\mathbb{Q}) \cong \mathbb{Z}_4$

Definition 0.7.

- Let $H \leq \mathrm{Gal}(K:F)$. Then define

$$\mathrm{Fix}_K(H) \stackrel{\text{def}}{=} \{k \in K \mid h(k) = k \text{ for all } h \in H\}$$

  This will be an intermediate field.

- Let $F \subseteq K$ be a field extension. Then we define

$$\mathrm{Intermed}(F \subseteq K) \stackrel{\text{def}}{=} \{\text{fields } L \mid F \subseteq L \subseteq K\}$$

$$\mathrm{SubGal}(K \supseteq F) \stackrel{\text{def}}{=} \{\text{subgroups of } \mathrm{Gal}(K:F)\}$$

  We have $\mathscr{F} : \mathrm{SubGal} \to \mathrm{Intermed}, H \mapsto \mathrm{Fix}_K(H)$, $\mathscr{G} : \mathrm{Intermed} \to \mathrm{SubGal}, L \mapsto \mathrm{Gal}(K:L)$.

- $L \in \mathrm{Intermed}$ is <u>closed</u> if $\mathscr{F}(\mathscr{G}(L)) = L$. It is <u>stable</u> if $\phi(L) \subseteq L$ for all $\phi \in \mathrm{Gal}(K:F)$. $H \in \mathrm{SubGal}$ is <u>closed</u> if $\mathscr{G}(\mathscr{F}(H)) = H$

If L is stable, $\phi(L) \subseteq L, \phi^{-1}(L) \subset L$ for all $\phi \in \mathrm{Gal}(K:F)$, so $\phi(L) = L$.
We have restriction map $\rho : \mathrm{Gal}(K:F) \to \mathrm{Gal}(L:F), \rho(\phi) = \phi|_L$. We have $\ker(\rho) = \mathrm{Gal}(K:L)$

Proposition 4.

1. *$\mathscr{F}$ and $\mathscr{G}$ preserve inclusions.*

2. *(a)* $L \subseteq \mathscr{F}\mathscr{G}(L)$ *and* $\mathscr{G}(L) = \mathscr{F}\mathscr{F}\mathscr{G}(L)$ *for all* $L \in \mathrm{Intermed}$
(b) $H \subseteq \mathscr{G}\mathscr{F}(H)$ *and* $\mathscr{F}(H) = \mathscr{F}\mathscr{G}\mathscr{F}(H)$ *for all* $H \in \mathrm{SubGal}$

3. *(a)* $L \in \mathrm{Intermed}$ *is closed iff* $L \in \mathrm{Im}(\mathscr{F})$
(b) $H \in \mathrm{SubGal}$ *is closed iff* $H \in \mathrm{Im}(\mathscr{G})$

4. *$\mathscr{G}$ and $\mathscr{F}$ restrict to inverse bijections.*

So there is a bijection between $\{$*closed* $L \in \mathrm{Intermed}\}$ *and* $\{$*closed subgroups*$\}$

Proposition 5.

1. *Let* $E \subseteq L$ *in* Intermed *such that* $[L:E] < \infty$. *Then*

(a) $[\mathscr{G}(E) : \mathscr{G}(L)] \subseteq [L : E]$

(b) *If E is closed, then so is L, and a becomes an equality.*

2. *Let $H \subseteq J$ in* SubGal *such that $[J : H] < \infty$.*

(a) $[\mathscr{F}(H) : \mathscr{F}(G)] \leq [J : H]$

(b) *If H is closed, so is J, and a is an equality*

Proof.

1. (a) $L = E(a_1, \ldots, a_m)$. Induct on m.
For $m = 1$, $L = E(a)$. Since $[L : E] < \infty$, a is algebraic over E. So it has minimal polynomial $p = p_{a,E}$.
The number of roots of p in K is less than or equal to $\deg p = [L : E]$.
We need to show $[\mathscr{G}(E), \mathscr{G}(L)] \leq$ number of roots of p in K.
$H = \mathscr{G}(L), J = \mathscr{G}(E)$.
$\phi_1(H), \cdots, \phi_n(H)$ are distinct left cosets of H in J.
for $i \neq j$, $\phi_i(H) \neq \phi_j(H)$, so $\phi_j^{-1}\phi_i(a) \neq a$, so $\phi_i(a) \neq \phi_j(a)$.
ϕ_i permutes roots of p in K, so $\phi_i(a) =$a root of p.
Therefore $\phi_1(a), dots, \phi_n(a)$ are n distinct roots of p in K.
Thus $[J : H] = n \leq$ number of roots of p in $K \leq \deg p = [L : E]$
For $m > 1$, let $M = E(a_1, \ldots, a_{m-1})$, $L = M(a_m)$. Then $[\mathscr{G}(E) : \mathscr{G}(M)] \leq [M : E]$, $[\mathscr{G}(M) : \mathscr{G}(L)] \leq [L : M]$. So $[\mathscr{G}(E) : \mathscr{G}(L)] \leq [L : E]$

2. (a) $n = [J : H]$, $\phi_1(H), \ldots, \phi_n(H)$ are distinct left cosets of H in J.
So $E = \mathscr{F}(J) \subseteq L = \mathscr{F}(H)$.
Suppose $[L : E] > n$.
Then there exists $a_1, \ldots, a_{n+1} \in L$, linearly independent over E.
There exists $(\phi_i(a_j)) = n \times (n + 1)$ matrix over K.

Lecture 8, 4/19/23

We continue the proof

1. (a) Done

(b) Consider the tower $F \subseteq E \subseteq L \subseteq K$, where $[L : E] < \infty$.
$E = \mathscr{F}\mathscr{G}(E)$.
$[L : E] = [L : \mathscr{F}\mathscr{G}(E) \leq [\mathscr{F}\mathscr{G}(L) : \mathscr{F}\mathscr{G}(E)]$

By 1a, $[\mathscr{G}(E) : \mathscr{G}(L)] \leq [L : E]$.
By 2a, $[\mathscr{F}\mathscr{G}(L) : \mathscr{F}\mathscr{G}(E)] \leq [\mathscr{G}(E), \mathscr{G}(L)]$.
Thus

$$\begin{aligned}[L : E] &\leq [\mathscr{F}\mathscr{G}(L) : \mathscr{F}\mathscr{G}(E)] \\ &\leq [\mathscr{G}(E) : \mathscr{G}(L)] \\ &\leq [L : E]\end{aligned}$$

So these inequalities are actually all equalities.
Therefore $[\mathscr{G}(E) : \mathscr{G}(L)] = [L : E]$.
$[\mathscr{F}\mathscr{G}(L) : E] = [\mathscr{F}\mathscr{G}(L) : \mathscr{F}\mathscr{G}(E)] = [L : E]$
By linear algebra, $\mathscr{F}\mathscr{G}(L) = L$

2. (a) So we have our $n \times (n+1)$ matrix A over K. We have a linear transformation $K^{n+1} \to K$, $x \mapsto (Ax^T)^T$
$|A\rangle \neq \{0\}$
Chose $b \in \ker(A), b \neq 0$,where $b = (b_1, \ldots, b_n)$ with $|\{b_i \mid b_i \neq 0\}|$ minimal.
$\sum_{i=0}^{n+1} \phi_i(a_j)b_j = 0$ for all i..
It is okay to permute js, so without loss of generality, $g = (b_1, \ldots, b_k, 0, \ldots, 0)$ where $b_1, \ldots, b_k \neq 0$.
Without loss of generality, suppose $b_1 = 1$
We claim there exists ℓ such that $b_\ell \notin \mathscr{F}(J)$.
If all $b_j \in \mathscr{F}(J)$, then $\phi_i(b_j) = b_j$ for all i, j.
Now for all i, $0 = \sum_j \phi_i(a_j)b_j = \sum_j \phi_i(a_j)\phi_i(b_j) = \sum_i(\sum_j a_j b_j)$
Thus $\sum_j a_j b_j = 0$ for all j, as this is in both $\mathscr{F}(H), \mathscr{F}(J)$
This contradicts the linear independence of $a_i s$ over $\mathscr{F}(J)$.
Thus there exists $\ell \in \{2, \ldots, k\}$ such that $b_\ell \notin \mathscr{F}(J)$.
Permute $j = 2, \ldots, k$ to get $\ell = 2$.
Now $b = \{1, \underbrace{b_2}_{\notin \mathscr{F}(J)}, \ldots, b_j, 0, \ldots, 0\}$
Thus there exists $\phi \in J$ such that $\phi(b_2) \neq b_2$.
So $\phi\phi_1(H), \ldots, \phi\phi_n(H)$ is another list of distinct left cosets of H in J.
Thus there exists $\pi \in S_n$ such that $\phi\phi_j(H) = \phi_{\pi(j)}(H)$ for all j.
$\sum_j \phi_{\pi(i)}(a_j)\phi(b_j) = \sum_j \phi\phi_i(a_j)\phi(b_j) = 0$ for all i.
Chose $b' = (1, \phi(b_2), \ldots, \phi(b_k), 0, \ldots, 0)$ in $\ker A'$, where $A' = (\phi_{\pi(i)}(a_j))$.
$\ker A' = \ker A$, so $b' \in \ker A$.

Thus $c = b - b' = (0, \underbrace{b_2 - \phi(b_2)}_{\neq 0}, \ldots, b_k - \phi(b_k), 0, \ldots, 0) \in \ker(A)$

This contradicts the minimality of k.

(b) Analagous to 1b

■

Corollary 0.10.

(a) All finite subgroups of $\mathrm{Gal}(K : F)$ *are closed.*

(b) $[K : F] < \infty$ *implies* $|\mathrm{Gal}(K : F)| \leq [K : F]$ *is finite*

(c) $[K : F] < \infty$ *implies* $\mathscr{F}$ *is injective and* $\mathscr{G}$ *is surjective.*

Proof. $\{\mathrm{Id}_K\} = \mathscr{G}(K)$ closed. For all $H \in \mathrm{Gal}(K : F), H = \mathscr{G}^{-1}\mathscr{F}(H)$.

■

Proposition 6.

(a) $L \in$ Intermed *stable implies that* $\mathrm{Gal}(K : L)$ *is a normal subgroup of* $\mathrm{Gal}(K : F)$

(b) H *a normal subgroup of* $\mathrm{Gal}(K : F)$ *implies* $\mathscr{F}(H) \in$ Intermed *is stable.*

Proof.

(a) $\theta \in \mathrm{Gal}(K : L), \phi \in \mathrm{Gal}(K : F)$. $\theta(x) = x$ for all $x \in L$. Since we have stability, $\phi(x) \in L$ for all $x \in L$.

$$\begin{aligned} &\Rightarrow \theta\phi(x) = \phi(x) \\ &\Rightarrow \phi^{-1}\theta\phi(x) = x \\ &\Rightarrow \phi^{-1}\theta\phi \in \mathrm{Gal}(K : F) \end{aligned}$$

(b) $\phi \in H$, so $\phi(x) = x$ for all $x \in \mathscr{F}(H)$. Say $\theta \in \mathrm{Gal}(K : F)$.

By normality of H, $\theta^{-1}\phi\theta \in H$.

$$\begin{aligned} &\Rightarrow \theta^{-1}\phi\theta(x) = x && \forall x \in \mathscr{F}(H) \\ &\Rightarrow \phi\theta(x) = \theta(x) && \forall x \in \mathscr{F}(H), \phi \in H \\ &\Rightarrow \theta(x) \in \mathscr{F}(H) && \forall x \in \mathscr{F}(H) \end{aligned}$$

Lecture 10, 4/21/23

Definition 0.8. A field extension $F \subseteq K$ is Galois if $F = \mathrm{Fix}_K \mathrm{Gal}(K : F)$

Theorem 0.11 (Little Theorem of Galois Theory)**.** *Let $F \subseteq K$ be a field extension, $[K : F] < \infty$. Then the following are equivalent:*

1. *$F \subseteq K$ is Galois*

2. *$\mathscr{F}, \mathscr{G}$ are inverse bijections*

3. $|\mathrm{Gal}(K : F)| = [K : F]$

If so, for all $L \in$ Intermed, $L \subseteq K$ is Galois.

Proof. $[K : F] < \infty$ implies $\mathrm{Gal}(K : F)$ finite.
So all $H \in$ SubGal are closed.

$1 \Rightarrow 2$

Galois $\implies$ F closed.
So by prop, all $L \in$ Intermed are closed.

$2 \Rightarrow 3$

$F = \mathscr{F}\mathscr{G}(F) \implies F$ closed.
So by prop,

$$\begin{aligned} |\mathrm{Gal}(K : F)| &= |\mathscr{G}(F) : \{\mathrm{Id}_K\}] \\ &= |\mathscr{G}(F) : \mathscr{G}(K)] \\ &= [K : F] \end{aligned}$$

$3 \Rightarrow 1$

$F \subseteq \mathscr{F}\mathscr{G}(F) \subseteq K$.

$$\begin{aligned} [K : F] &\geq [K : \mathscr{F}\mathscr{G}(F)] \\ &= [\mathscr{F}(\{\mathrm{Id}_K\}) : \mathscr{F}\mathscr{G}(F)] \\ \text{by prop} \quad &= [\mathscr{G}(F) : \{\mathrm{Id}_K\}] \\ \text{by def} \quad &= |\mathrm{Gal}(K : F)| \\ \text{by assumption} \quad &= [K : F] \end{aligned}$$

Thus $[K : F] = [K : \mathscr{F}\mathscr{G}(F)]$.
So $[\mathscr{F}\mathscr{G}(F) : F] = 1$, i.e. $\mathscr{F}\mathscr{G}(F) = F$.
If we have 1-3, then L closed, so $L = \mathscr{F}\mathscr{G}(L) = \mathrm{Fix}_K \mathrm{Gal}(K : L)$. Thus $L \subseteq K$ is Galois.

■

Example 0.8. $F \subseteq K, [K : F] = 2, \mathrm{char}\, F \neq 2 \implies F \subseteq K$ Galois
Reason: $|\mathrm{Gal}(K : F)| = 2$.
$F = \mathbb{Q} \subseteq K = \mathbb{Q}(a, \zeta) \subseteq \mathbb{C}$, $a = \sqrt[3]{2} \in \mathbb{R}, \zeta =$root of $X^2 + X + 1$
There exists $\phi_{ij} \in \mathrm{Gal}(K : F)$ such that $\phi_{ij}(a) = a\zeta^i$ $(i = 0, 1, 2)$ and $\phi_{ij}(\zeta) = \zeta^j$ $(j = 1, 2)$
Therefore $|\mathrm{Gal}(K : F)| = 6 = [K : F]$.
For all $L \in \mathrm{Intermed}, L \subseteq K$ is Galois.
$F \subseteq \mathbb{Q}(a)$ is not Galois.

Lemma 2. *Let $F \subseteq K$ be Galois, $f \in F[X]$ an irreducible polynomial with a root in K. Then f splits over K and has no multiple roots.*

Proof. Without loss of generality, suppose f is monic.
Say $a_i \in K$ is a root of f.
Let $a_1, a_2, \ldots, a_r$ be the distinhct roots of f in K.
Set $g = (X - a_1)(X - a_2) \cdots (X - a_r) \in K[X]$.
We claim $g \in F[X]$.
Let $\phi \in G = \mathrm{Gal}(K : F)$.
ϕ permutes $\{a_1, \ldots, a_r\}$
$\tilde{\phi}(g) = g$ so $\phi(c_i) = c_i$ for all coefficients c_i of g.
Thus all $c_i \in \mathrm{Fix}_K(F) = F_1$, i.e. $g \in F[X]$.
Let $f = p_{a_1,F}$.
$g(a_1) = 0 \implies f \mid g$.
$\deg(g) = r \leq \deg(f)$.
Thus $f = g$

■

Corollary 0.12. *Let $F \subseteq L \subseteq K$ be a tower fo fields. If L is algebraic over V and Galois over F, then L is stable.*

Proof. Chose $a \in L, \phi \in \mathrm{Gal}(K : F)$. $p_{a,F} \in F[X]$ is irreducible, with a as a root. By lemma, $p_{a,F}$ splits over L. So all rotos of $p_{a,F}$ in K are in L.
ϕ sends a to a root of $p_{a,F}$. Thus $\phi(a) \in L$.

Theorem 0.13 (Main Theorem of Galois Theory)**.** *Let $F \subseteq K$ be a Galois field extension, $[K : F] < \infty$. Then*

1. *There exist inverse bijections*

$$\{\textit{intermediate fields of } F \subseteq K\} \underset{\mathscr{G}}{\overset{\mathscr{F}}{\rightleftarrows}} \{\textit{subgroups of } \mathrm{Gal}(K:F)\}$$

such that $\mathscr{G}(L) = \mathrm{Gal}(K:L), \mathscr{F}(H) = \mathrm{Fix}_K(H)$.

2. *If* $E \subseteq L$ *are intermediate fields,* $[\mathscr{G}(E) : \mathscr{G}(L)] = [L:E]$.

3. *If* $H \leq J \leq \mathrm{Gal}(K:L)$, $[\mathscr{F}(H) : \mathscr{F}(J)] = [J:H]$.

4. *For all intermediate fields* $L, L \subseteq K$ *is Galois, and*

$$F \subseteq L \textit{ Galois} \iff L \textit{ is stable} \iff \mathrm{Gal}(K:L) \textit{ is a normal subgroup } \mathrm{Gal}(K:F)$$

If so, $\mathrm{Gal}(K:F)\,\mathrm{Gal}(K:L) \cong \mathrm{Gal}(L:F)$