# 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 $S = \{a_1, \dots, a_n\}$, we use $F(a_1, \dots, a_n)$ and $F[a_1, \dots, a_n]$ 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, $\pi, e$ 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 $\varepsilon(f) = f(a_1, \ldots, a_n)$.
$\varepsilon$ 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 <u>minimal polynomial</u> 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. $\varepsilon$ 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:

$$\begin{tikzcd}
\mathbb{Q}(a) \arrow[d, dash] \arrow[dd, bend right=60, "4"'] \\
\mathbb{Q}(\sqrt{5}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

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

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 $\phi$ 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 $\phi$ 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 $\phi(i) = \pm i$. $\phi$ 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, 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.** $F = \mathbb{Q}(\zeta) \subseteq K = \mathbb{Q}(\zeta, a), \zeta = e^{\frac{2\pi i}{3}}, a = \sqrt[4]{5} \in \mathbb{R}$.
$\zeta$ 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 $p_{a,\mathbb{Q}} = X^3 - 5, [\mathbb{Q}(a) : \mathbb{Q}] = 3$.

$$\begin{tikzcd}
 & K = Q(\zeta, a) \not\subseteq \mathbb{R} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] \arrow[dd, dash, "6"] & \\
F = \mathbb{Q}(\zeta) \arrow[dr, dash, "2"'] & & \mathbb{Q}(a) \subseteq \mathbb{R} \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

# 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 $X^2+X+1$.*
$X^3-2=(X-a)(X-a\zeta)(X-a\zeta^2)$

$$\begin{tikzcd}
\mathbb{Q}(a,\zeta) \arrow[d, dash, "6"] & \mathbb{Q}(\zeta)(a) \arrow[d, dash, "3"'] \\
\mathbb{Q} & \mathbb{Q}(\zeta) \arrow[d, dash, "2"'] \\
 & \mathbb{Q}
\end{tikzcd}$$

*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*

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

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

$\blacksquare$

## 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 $\phi$ extends to an isomorphism $\theta : F_1(a_1) \to F_2(a_2)$ such that $\theta(a_1) = a_2$.*

$$\begin{tikzcd} K_1 \arrow[d, no head] & K_2 \arrow[d, no head] \\ F(a_1) \arrow[r, dotted, "\exists\theta"] \arrow[d, no head] & F(a_2) \arrow[d, no head] \\ F_1 \arrow[r, "\theta"] & F_2 \end{tikzcd}$$

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

*Proof.*

$$
\begin{tikzcd}
F_1[X] \arrow[rrr, "\tilde{\phi}", "\cong"'] \arrow[dr, "q_1"] & & & F_2[X] \arrow[dl, "q_2"'] \\
& F_1[X]/\langle f_1 \rangle \arrow[r, "\psi", "\cong"'] \arrow[d, "p_1"', "\cong"] & F_2[X]/\langle f_2 \rangle \arrow[d, "p_2"', "\cong"] & \\
& F_1(a_1) \arrow[r, dotted, "p_2 \circ \psi \circ p_1^{-1}"] & F_2(a_2) & \\
F_1 \arrow[uuu, "\subseteq"] \arrow[rrr, "\theta", "\cong"'] & & & F_2[X] \arrow[uuu, "\subseteq"']
\end{tikzcd}
$$

■

**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 $\phi$ extends to an isomorphism $K_1 \to K_2$.*

$$
\begin{tikzcd}
K_1 \arrow[r, "\cong"] & K_2 \\
F_1 \arrow[u, "\subseteq"] \arrow[r, "\phi"] & F_2 \arrow[u, "\subseteq"']
\end{tikzcd}
$$

*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 $(M, \psi) \in \mathscr{M}$

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

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, $\psi$ extends to an isomorphism $\theta : M(a_1) \to M'(a_2)$.
Now $(M(a_2), \theta) \in \mathscr{M}$, contradicting that $(M, \psi)$ 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 $\phi$ 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 $X^2 + X + 1 : \zeta, \zeta^2$

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

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

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

# Lecture 7, 4/17/23

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

**Definition 0.7.**

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

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

  This will be an intermediate field.

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

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

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

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

- $L \in \text{Intermed}$ is <u>closed</u> if $\mathscr{F}(\mathscr{G}(L)) = L$. It is <u>stable</u> if $\phi(L) \subseteq L$ for all $\phi \in \text{Gal}(K : F)$. $H \in \text{SubGal}$ 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 $\phi \in \text{Gal}(K : F)$, so $\phi(L) = L$.
We have restriction map $\rho : \text{Gal}(K : F) \to \text{Gal}(L : F), \rho(\phi) = \phi|_L$. We have $\ker(\rho) = \text{Gal}(K : L)$

**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 $L \in \text{Intermed}$*

*(b) $H \subseteq \mathscr{G}\mathscr{F}(H)$ and $\mathscr{F}(H) = \mathscr{F}\mathscr{G}\mathscr{F}(H)$ for all $H \in \text{SubGal}$*

**3.** *(a) $L \in \text{Intermed}$ is closed iff $L \in \text{Im}(\mathscr{F})$*

*(b) $H \in \text{SubGal}$ is closed iff $H \in \text{Im}(\mathscr{G})$*

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

*So there is a bijection between $\{$closed $L \in \text{Intermed}\}$ 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) $L = E(a_1, \dots, a_m)$. 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 $\phi_i(a) \neq \phi_j(a)$.
$\phi_i$ 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 $M = E(a_1, \dots, a_{m-1})$, $L = M(a_m)$. 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) $n = [J : H]$, $\phi_1(H), \dots, \phi_n(H)$ 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 $a_1, \dots, a_{n+1} \in L$, 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 $b = (b_1, \dots, b_n)$ 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 $j$s, so without loss of generality, $g = (b_1, \dots, b_k, 0, \dots, 0)$ where $b_1, \dots, b_k \neq 0$.
Without loss of generality, suppose $b_1 = 1$
We claim there exists $\ell$ 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 $i$, $0 = \sum_j \phi_i(a_j)b_j = \sum_j \phi_i(a_j)\phi_i(b_j) = \sum_i(\sum_j a_jb_j)$
Thus $\sum_j a_jb_j = 0$ for all $j$, as this is in both $\mathscr{F}(H), \mathscr{F}(J)$
This contradicts the linear independence of $a_is$ over $\mathscr{F}(J)$.
Thus there exists $\ell \in \{2, \dots, k\}$ such that $b_\ell \notin \mathscr{F}(J)$.
Permute $j = 2, \dots, k$ to get $\ell = 2$.
Now $b = \{1, \underbrace{b_2}_{\notin \mathscr{F}(J)}, \dots, b_j, 0, \dots, 0\}$
Thus there exists $\phi \in J$ such that $\phi(b_2) \neq b_2$.
So $\phi\phi_1(H), \dots, \phi\phi_n(H)$ 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 $b' = (1, \phi(b_2), \dots, \phi(b_k), 0, \dots, 0)$ 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)* $L \in \mathrm{Intermed}$ *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* $\mathscr{F}(H) \in \mathrm{Intermed}$ *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 $F = \operatorname{Fix}_K \operatorname{Gal}(K : F)$

**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.** $|\operatorname{Gal}(K : F)| = [K : F]$

*If so, for all $L \in \text{Intermed}, L \subseteq K$ is Galois.*

*Proof.* $[K : F] < \infty$ implies $\operatorname{Gal}(K : F)$ finite.
So all $H \in \text{SubGal}$ 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,

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

$3 \Rightarrow 1$

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

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

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 $L = \mathscr{F}\mathscr{G}(L) = \operatorname{Fix}_K \operatorname{Gal}(K : L)$. Thus $L \subseteq K$ is Galois.

■

**Example 0.8.** $F \subseteq K, [K : F] = 2, \operatorname{char} F \neq 2 \implies F \subseteq K$ Galois
Reason: $|\operatorname{Gal}(K : F)| = 2$.
$F = \mathbb{Q} \subseteq K = \mathbb{Q}(a, \zeta) \subseteq \mathbb{C}$, $a = \sqrt[3]{2} \in \mathbb{R}, \zeta =$root of $X^2 + X + 1$
There exists $\phi_{ij} \in \operatorname{Gal}(K : F)$ such that $\phi_{ij}(a) = a\zeta^i$ $(i = 0, 1, 2)$ and $\phi_{ij}(\zeta) = \zeta^j$ $(j = 1, 2)$
Therefore $|\operatorname{Gal}(K : F)| = 6 = [K : F]$.
For all $L \in$ 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 $\phi \in G = \operatorname{Gal}(K : F)$.
$\phi$ 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 $c_i \in \operatorname{Fix}_K(F) = F_1$, 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 $a \in L, \phi \in \operatorname{Gal}(K : F)$. $p_{a,F} \in F[X]$ 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 $L$.
$\phi$ 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*

$$\begin{tikzcd}\{\textit{intermediate fields of } F \subseteq K\} \arrow[r, bend right, "\mathscr{G}"'] & \{\textit{subgroups of } \mathrm{Gal}(K:F)\} \arrow[l, bend right, "\mathscr{F}"']\end{tikzcd}$$

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

# Lecture 11, 4/24/23

*Proof.* We will now prove the Main Theorem of Galois Theory.
Part 1 follows from the Little theorem. This implies all intermediate fields are closed and all subgroups of $\mathrm{Gal}(K : F)$ are closed.
2 and 3 follow from prop 5 on page 13 of this document.
Now for 4.
By the Little Theorem, $L \subseteq K$ is Galois.
By a previous prop, we know $F \subseteq L$ is Galois iff $L$ is stable. By another one, we know $L = \mathscr{F}\mathscr{G}(L)$ is stable iff $\mathrm{Gal}(K : L) \trianglelefteq \mathrm{Gal}(K : F)$
Assume $L$ is stable, let $a \in L \setminus F$. $F \subseteq K$ Galois implies there exists $\phi \in \mathrm{Gal}(K : F)$ such that $\phi(a) = a$.
By stability, $\phi$ restricts to a map in $\mathrm{Gal}(L : F)$ and $\phi|_L(a) \neq a$.
Thus $F \subseteq L$ is Galois.
The last step is left as an exercise.

■

**Definition 0.9.** For $F$ a field, $F[X]$ a polynomial ring, $f \in F[X]$.

- Let $F \subseteq K$ be a field extension. We say that $a \in K \setminus F$ is a multiple root of $f$ if $(X - a)^2 \mid f$ in $K[X]$.

  As an exercise, suppose that $K \subseteq L$ is a field extension, $f, g \in K[X]$ polynomials. Then $f \mid g$ in $K[X]$ iff $f \mid g$ in $L[X]$.

- $a$ is a simple root of $f$ if it's not a multiple root.
- If $f$ is irreducible, then $f$ is separable over $F$ if $f$ has no multiple roots in any extension field.
- If $f$ arbitrary, $f$ is separable over $F$ if all irreducible factors of $f$ are separable over $F$.

Now let $F \subseteq K$ be a field extension.

- Suppose $a \in K$ is algebraic over $F$. Then $a$ is separable over $F$ if $p_{a,F}$ is separable over $F$.
- Let $F \subseteq K$ be algebraic. $F \subseteq K$ is separable if each $a \in K$ is separable over $F$.
- $F \subseteq K$ is normal if each polynomial over $F$ with a root in $K$ splits over $K$.

Note: $F \subseteq K$ a field extension. If $F \subseteq K$ is algebraic and Galois, it is separable and normal.

**Example 0.9.** Let $[K : F] = 2$. If char $F \neq 2$, then $K$ is separable over $F$.
Say $a \in K$, $p_{a,F} = X^2 + bX + c$.
$a^2 + ba + c = 0$.
Suppose $p_{a,F} = (X - d)^2 = X^2 - 2d + d^2$.
Then $-2d = b \in F$, so $d \in F$. Contradiction.
Thus $[K : F] = 2$ implies $F \subseteq K$ is normal.

**Definition 0.10.** Let $R$ be a ring, and $f \in R[X]$ a polynomial.
$f = \sum_{i=0}^{n} r_i X^i, r_i \in R$.
Define $f' = \sum_{i=1}^{n} i r_i X^{i-1}$, the formal derivative.
Exercise: show the product rule holds. That is, $(fg)' = f'g + fg'$.

# Lecture 12, 4/26/23

## Separability criterion

**Theorem 0.14.** *Let $F$ be a field, $f \in F[X]$ a polynomial.*

*(a) $f$ has no multiple roots in any extension field iff $\gcd(f, f') = 1$*

*(b) If $f$ is irreducible, then $f$ is separable over $F$ iff $f' \neq 0$.*

*Exercise: for $f, g \in F[X] \subseteq K[X], \gcd(f, g) = 1$ in $F[X]$ iff $\gcd(f, g) = 1$ in $K[X]$.*

*Proof.*

(a) $\Rightarrow$ Suppose $\gcd(f, f') \neq 1$. There exists $g \in F[X]$ of degree at least 1 such that $g \mid f$ and $g \mid f'$.
Let $K \supseteq F$ be a splitting field for $g$.
Let $a \in K$ be a root of $g$. Thus $f = (X - a)h$ in $K[X]$, $f' = h + (X - a)h'$.
$(X - a) \mid g$, $g \mid f'$ implies $(X - a) \mid h$.
So $(X - a)^2 \mid f$ in $K[X]$.

$\Leftarrow$ Suppose $f$ has a multiple root $a$ in an extension field $K$.
$f = (X - a)^2 g, g \in K[X]$.
$f' = 2(X - a)g + (X - a)^2 g'$.
Thus $(X - a) \mid f' \implies \gcd(f, f') = 1$.

(b) $\Rightarrow$ Since $f$ is separable, $\gcd(f, f') = 1$ by (a). Thus $f' \neq 0$.

$\Leftarrow$ Suppose $f$ is not separable. Then $g = \gcd(f, f') \neq 1$ by (a).
So $\deg g \geq 1$, $g \mid f, g \mid f'$.
Since $f$ is irreducible, $g$ is a scalar times $f$.
So $\deg f = \deg g \leq \deg f < \deg g$. Unless $f' = 0$, this is a contradiction.
So $f' = 0$.

∎

**Corollary 0.15.** *If* $\operatorname{char} F = 0$*, all polynomials over* $F$ *are separable. Therefore, all algebraic field extensions of* $F$ *are separable.*

*Proof.* If $\operatorname{char} F = 0$, then there is no $\mathbb{Z}$-torsion, so the formal derivative can't possibly be zero unless the degree of $f$ is 0.

∎

**Theorem 0.16.** *Let* $F \subseteq K$ *be an algebraic field extension. Then the following are equivalent:*

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

**2.** $F \subseteq K$ *is separable and* $K$ *is a splitting field over* $F$ *for some set of polynomials in* $F[X]$.

**3.** $K$ *is a splitting field over* $F$ *for some set of separable polynomials in* $F[X]$.

*Proof.*

(1) $\Rightarrow$ (2)

Already done.

## $(2) \Rightarrow (3)$

Let $K$ be a splitting field over $F$ for a set of polynomials $S \subsetneq F[X]$. Let $S'$ be a collection of all the monic irreducible polynomial factors in $S$. Clearly, $K$ is also a splitting field of $S'$ over $F$.
$f \in S^1$ splits over $K$, implying $f$ has a root $a \in K$.
$f = p_{a,F}$, so $F \subseteq K$ implies $f$ separable over $F$.

## $(3) \Rightarrow (1)$

Let $K$ be a splitting field over $F$ for some set $S$ of separable polynomials.
Stepq 1: $[K : F] < \infty$.
For $n = 1$, this is trivial.
Suppose $n > 1$. Then $F \subseteq K \Rightarrow$ the polynomials cannot all split over $F$.
So there exists $g \in S$ that does not split over $F$.
Thus, $g$ has a monic irreducible factor $f \in F[X]$ such that $\deg f \geq 2$.
Let $a \in K$ be a root of $f$.
Thus $f = p_{a,F}, a \neq F$.
$L = F(a) \supsetneq F$.
So $[K : L] < n$ by the tower rule.
This implies

**1.** $K$ is a splitting field for $S$ over $L$.

**2.** All polynomials in $S$ are separable over $L$.

By induction, this implies that $L \subseteq K$ is Galois.
So $|\operatorname{Gal}(K : L)| = [K : L]$.
Let $G = \operatorname{Gal}(K : F)$, $H = \operatorname{Gal}(K : L)$.
$|G| = |H|[G : H]$.
$[K : F] = [K : L][L : F]$.
$[L : F] = \deg p_{a,F} = \deg f = m$.
By prop 5 on page 13, we know $[G : H] \leq [L : F]$.
$f$ has $m$ distinct roots in $K$, say $a_1, \ldots, a_m$.
By the Extension Lemma, there exist $F$-automorphisms $\phi_i : F(a) \to F(a_i)$ such that $\phi_i(a) = a_i$.
Let $K$ be a splitting field for $S$ over $F(a)$ and $F(a_i)$.
By uniqueness of splitting fields, there exists isomorphisms $\psi_i : K \to K$ extending $\phi_i$.
$\psi_i \in G$.
$\psi_j^{-1}\psi_i(a) = \psi_j^{-1}(a_i) \neq \psi_j^{-1}(a_j) =$
Thus $\psi_j^{-1}\psi_i \notin H$ if $i \neq j$.
So $\psi_i H \neq \psi_j H$.

Thus $[G : H] \geq m$.
So $[G : H] = m$, i.e. $|G| = [K : F]$, so $F \subseteq K$ is Galois.

# Lecture 14, 4/28/23

We continue the proof.
For (3) $\Rightarrow$ (1), we have shown step 1, $[K : F] < \infty$.
Now for step 2: $[K : F]$ arbitrary.
Let $K = F(R)$, where $R = \{\text{all roots in } K \text{ of polynomials in } S\} = \bigcup_{\text{finite } T \subseteq S} R_T = \{\text{all roots in } K \text{ of polynomials in } T\}$
$K = \bigcup_{\text{finite } T \subseteq S} F(R_T)$.
$F(R_T)$ is a splitting field for $T$ over $F$.
Thus $[F(R_T) : F] < \infty$.
By step 1, $F(R_T)$ is Galois over $F$.
Look at $a \in K \setminus F$.
There exists a finite set $T \subseteq S$ such that $a \in F(R_T)$.
There exists $\phi \in \text{Gal}(F(R_T) : F)$ such that $\phi(a) = a$.
$K$ is a splitting field for $S$ over $F(R_T)$.
By uniqueness of splitting fields, $\phi$ extends to an isomorphism $\psi : K \to K$.
$\psi \in \text{Gal}(K : F), \psi(a) = \phi(a) \neq a$.
Thus $F \subseteq K$ is Galois.

■

**Theorem 0.17.** *Let $F \subseteq K$ be an algebraic field extension. Let $\overline{K}$ be an algebraic closure of $K$. The following are equivalent:*

**1.** *$F \subseteq K$ normal*

**2.** *$K$ is a splitting field for some set $S$ of polynomials over $F$.*

**3.** *$K$ is a stable intermediate field of $F \subseteq \overline{K}$.*

*Proof.*

## (1) $\Rightarrow$ (2)

$S = \{p_{a,F} \mid a \in K\}$.
By normality, all $p_{a,F}$ split over $K$. $K = \{\text{roots of } p \in S \text{ in } K\}$.
Therefore $K$ is a splitting field for $S$ over $F$.

$(2) \Rightarrow (3)$

Let $\phi \in \text{Gal}(\overline{K} : F)$.
Let $K = F(R)$, where $R = \{\text{roots in } K \text{ of } f \in S\}$.
For all $f \in S, \phi$ permutes roots of $f$ in $K$.
Therefore $\phi(R) \subseteq R$, implying $\phi(K) \subseteq F(R) = K$.

$(3) \Rightarrow (1)$

Let $f \in F[X]$ be irreducible with a root $a \in K$. We want to show $f$ splits over $\overline{K}$.
Let $a_1, \ldots, a_r$ be the roots of $f$ in $\overline{K}$.
For all $i$, $p_{a,F}$ =constant times $f = p_{a_i,F}$.
By the Extension Lemma, there exists $F$-isomorphism $\phi_i : F(a) \to F(a_i)$ such that $\phi_i(a) = a_i$.
Since $\overline{K}$ is an algebraic closure of $F$, it is also an algebraic closure of $F(a)$ and $F(a_i)$.
By uniqueness of algebraic closures, $\phi_i$ extends to an isomoprhism $\psi_i : \overline{K} \to K$, $\phi_i \in \text{Gal}(\overline{K} : F)$
By stability, $\psi_i(K) \subseteq K$, implying $a_i \in K$.
Thus $f$ splits over $K$, i.e. $F \subseteq K$ is normal.

■

**Theorem 0.18.** *Let $F \subseteq K$ be an aglebraic field extension. $F \subseteq K$ is Galois iff it is both separable and normal.*

*Proof.* Previous 2 theorems.

■

**Definition 0.11.** Let $F \subseteq K$ be an algebraic field extension. A <u>normal closure of $K$ over $F$</u> is an extension field $L \supseteq K$ such that

- $F \subseteq L$ is normal.
- $L$ is minimal.

**Theorem 0.19.** *Let $F \subseteq K$ be an algebraic field extension.*

**1.** *There exists a normal closure $L$ for $F$ over $K$, and $F \subseteq L$ is algebraic.*

**2.** *$L$ is unique up to $K$-isomorphim.*

**3.** *If $[K : F] < \infty$, then $[L : F] < \infty$.*

**4.** *If $F \subseteq K$ is separable, then $F \subseteq L$ is Galois.*

*Proof.* exercise

■

**Definition 0.12.** A field $F$ is perfect if every algebraic extension field of $F$ is separable over $F$.

**Example 0.10.** Anything with $\operatorname{char} F = 0$ is perfect. $\mathbb{F}_2(Y)$ is not perfect, and indeed $\mathbb{F}_p(Y)$ is not perfect for any prime $p$.

**Example 0.11.** Any finite field is perfect. Say $F$ a field, $\operatorname{char} F = p > 0$. $F \to F$, $a \mapsto a^p$, the Frobenius map on $F$.

# Lecture 14, 5/1/23

*Frobenius map:* $\phi_F : F \to F$, $f(x) = x^p$.

**Theorem 0.20.** *Let $F$ be a field. Then the following are equivalent:*

**1.** *$F$ is perfect*

**2.** *All extension fields of finite degree over $F$ are separable over $F$.*

**3.** *Every irreducible polynomial in $F[X]$ is separable over $F$.*

**4.** *Either* $\operatorname{char} F = 0$, *or* $\operatorname{char} F = p$, *and $\phi_F$ is surjective.*

*Proof.*

$(1) \Rightarrow (2)$

Done

$(2) \Rightarrow (3)$

Chose $p \in F[X]$ irreducible. Then there exists an extension field $K = F(a) \supseteq F$ such that $[K : F] < \infty$,$p(a) = 0$.
$K \supseteq F$ is separable, so $p = p_{a,F}$ is separable over $F$.

$(3) \Rightarrow (1)$

Done

(4) $\Rightarrow$ (3)

Assume char $F = p > 0$.
Choose $f \in F[X]$ irreducible. Suppose $f$ is not separable over $F$.
Exercise: $f = g(X^p)$ for some $g \in F[X]$.
$g = \sum_{i=0}^{n} c_i X^i, c_i \in F$.
there exists $b_i \in F$ such that $b_i^p = c_i$.
Thus,

$$\begin{aligned} f &= g(X^p) \\ &= \sum_{i=0}^{n} c_i X^{pi} \\ &= \sum_{i=0}^{n} b_i^p X^{pi} \\ &= \left( \sum_{i=0}^{n} b_i X^i \right)^p \end{aligned}$$

This contradicts that $F$ is irreducible. Thus $f$ is separable.

**Corollary 0.21.** *Any finite field is perfect.*

**Lemma 3.** *Let $F$ be any field. Then any finite subgroup $G \subseteq F^*$ is cyclic.*

*Proof.* Since $G$ is abelian, $G$ is a direct product of its Sylow subgroups, which must all be normal.
By the Chinese Remainder Theorem, it is enough to show all Sylow subgroups are cyclic.
Without loss of generality, $G$ is in a $p$-group for some prime $p$.
$M = \{m \geq 0 \mid p^m = \text{order of an element in } G\}$.
$n = \max(M)$, so there exists $x \in G$ such that $|x| = p^n$.
For all $g \in G, |g| \mid p^n$, so $g^{p^n} = 1$.
Therefore all $g \in G$ are roots of $X^{p^n} - 1$.
So $|G| \leq p^n$, implying $G = \langle x \rangle$ ∎

**Corollary 0.22.** *Any extensions of finite fields is simple.*

*Proof.* Say $F \subseteq K$ is an extension of finite fields. $K^\times = \langle x \rangle$ for some $x \in K$.
Thus $K = F(x)$.

**Theorem 0.23.** *(Steinitz's Theorem)*
*Let $F \subseteq K$ be a field extension, $[K : F] < \infty$. Then following are equivalent:*

**1.** *$K \supseteq F$ is simple.*

**2.** *There exist only finitely many intermediate fields of $F \subseteq K$.*

*Proof.* (1) $\Rightarrow$ (2)

$K = F(a)$ for some $a \in K$. Let $\mathscr{L} = \text{Intermed}(F \subseteq K)$, $\mathscr{P} = \{$monic polynomials in $K[X]$ that divide $p_{a,F}\}$.
Define $\mu : \mathscr{L} \to \mathscr{P}$ by $\mu(L) = p_{a,L}$.
We claim $\mu$ is injective.
To prove this claim, we prove if $L \in \mathscr{L}$, then $L = F(\text{coefficients of } p_{a,L})$.
Say $p_{a,L} = \sum_{i=0}^{n} c_i X^i, c_i \in L$.
Let $L' = F(c_0, \ldots, c_n) \subseteq L$.
$p_{a,L'} \mid p_{a,L}$ in $L'[X]$.
$p_{a,L} \mid p_{a,L'}$ in $L[X]$.
Thus $p_{a,L} = p_{a,L'}$.
$[K : L] = [L(a) : L] = \deg p_{a,L} = \deg p_{a,L'} = [L'(a) : L'] = [K : L']$.
By the tower rule, $[L : F] = [L' : F]$, i.e. $L = L'$.
This implies that $\mu$ is injective.
Thus $\mathscr{L}$ is finite.

(2) $\Rightarrow$ (1)

Without loss of generality, suppose $K$ is infinite.
So $F$ must be infinite. Let $K = F(a_1, \ldots, a_m)$. Suppose $F \subseteq K$ is not simple.
Choose $i < m$ minimal such that $F(a_1, \ldots, a_{i+1})$ is not simple over $F$.
Then $F(a_1, \ldots, a_i) = F(a)$ for some $a$.
$F(a_1, \ldots, a_i, a_{i+1}) = F(a, b)$ where $b = a_{i+1}$.
For all $c \in F$, set $L_c = F(a + cb)$.
Claim: $L_c \neq L_{c'}$ when $c \neq c'$.
Why? Suppose $F(a + cb) = L_c = L_{c'} = F(a + c'b)$.
Then $a + c'b \in F(a + cb)$, so $(c - c')b \in L_c$.
$c - c' \in F$, so $b \in L_c$.
Thus $a \in L_c$.
So $L_c = F(a, b)$
contradiction
Thus we have infintely many intermediate fields, a contradiction.

■

# Lecture ?????, 5/3/23

**Corollary 0.24.** *Let $F \subseteq K$ be a seperable field extension with $[K : F] < \infty$. Then $F \subseteq K$ has to be a simple extension.*

*Proof.* Let $L$ be a normal closure for $K$ over $F$. $[L : F] < \infty$, so $L$ is Galois over $F$. So {intermed fields of $F \subseteq L$} is in bijection with { subgroups of $\underbrace{\mathrm{Gal}(L : F)}_{\text{finite}}$}

So there are only finitely many intermediate fields for $F \subseteq K$. So by Steinitz, we are done. ■

Let $F$ be a finite field.

- $\operatorname{char} F = p > 0$, so the prime field of $F$ is isomorphic to $\mathbb{F}_p$.
- If $n = [F : \mathbb{F}_p]$, then $F \cong \mathbb{F}_p^n$ as vector spaces, so $|F| = p^n$.
- $\phi_F$ is an $\mathbb{F}_p$-automorphism of $F$, with $\phi_F$ given by $x \mapsto x^p$.
- $F$ is perfect, because $\phi_F$ is surjective.
- $F^*$ is cyclic.

How can we build fields of order $p^2$? Well, we can adjoin the root of a quadratic. For $p = 2$, consider $X^2 + X + 1 \in \mathbb{F}_2[X]$. For $p = 3$, $X^2 + 1 \in \mathbb{F}_3[X]$. For $p = 5$, $X^2 + 2 \in \mathbb{F}_2[X]$.
Indeed for any odd $p$, $\{x^2 \mid x \in \mathbb{F}_p^*\} \subsetneq \mathbb{F}_p$. So there is some $k \in \mathbb{F}_p^*$ such that $X^2 - k \in \mathbb{F}_p[X]$ is irreducible.
Look at $g = X^{p^n} - X \in \mathbb{F}_p, g' = -1$. Then $\gcd(g, g') = 1$, so $g$ is seperable over $\mathbb{F}_p$. Likewise for $f = X^{p^n-1} - 1$.

**Theorem 0.25.** *Let $p$ be a prime, $n \in \mathbb{N}$. Assume there exists a field $F$ of order $p^n$. Then*

1. *$F$ is a splitting field over $\mathbb{F}_p$ of $X^{p^n - X}$ or $X^{p^n-1} - 1$. $\mathbb{F}_p \subseteq F$ is Galois,* $\mathrm{Gal}(F : \mathbb{F}_p) = \langle \phi_F \rangle$, $[F : \mathbb{F}_p] = n$.
2. *Let $K \supseteq F$ be an extension field of finite degree. Then $|K| = p^{dn}$, $F \subseteq K$ Galois,* $\mathrm{Gal}(K : F) = \langle \phi_K^n \rangle$

*Proof.* $\operatorname{char} F = p$, $[F : \mathbb{F}_p] = n$.

**1.** $|F^*| = p^n - 1$, $a^{p^n} = 1$ for all $a \in F^*$, so $a^{p^n} = a$ for all $a \in F$.

So all $a \in F$ are roots of $g = X^{p^n} - X \in \mathbb{F}_p[X]$.

So $g$ splits over $F$ and is seperable over $\mathbb{F}_p$. This tells us that $F$ is a splitting field for $g$ over $\mathbb{F}_p$. Therefore $F$ is Galois over $\mathbb{F}_p$.

$|\operatorname{Gal}(F : \mathbb{F}_p)| = n$, $\phi_F : x \mapsto x^p$, $\phi_F^n : x \mapsto x^{p^n}$, so $\phi_F^n = \mathrm{Id}_F$.

For $1 \leq j < n$:

$$\{a \in F \mid \phi_f^j(a) = a\} = \underbrace{\{\text{roots in } F \text{ of } X^{p^j} = X\}}_{\text{size } \leq p^j < |F|}$$

so $\phi_F^j \neq \mathrm{Id}_F$, so $|\phi_F| = n$ and $\operatorname{Gal}(F : \mathbb{F}_p) = \langle \phi_F \rangle$.

**2.** $|K| = |F|^d = p^{dn}$. $\mathbb{F}_p \subseteq K$ is Galois by 1, so $F \subseteq K$ is Galois.

So $|\operatorname{Gal}(K : F)| = d$. $\phi_K : K \to K, x \mapsto x^p$.

For all $a \in F, a = a^{p^n} = \phi_K^n(a)$, so $\phi_F^n \in \operatorname{Gal}(K : F)$, and $|\phi_K| = nd$, so $|\phi_K^n| = d = |\operatorname{Gal}(K : F :)|$, so it follows that $\operatorname{Gal}(K : F) = \langle \phi_K^n \rangle$

■