4. Galois Theory of Polynomials

Recall: If $f(x) \in F[x]$ and $K$ is the splitting field over $F$, then the Galois group of $f(x)$ over $F$ is $G := \text{Gal}(K/F)$.

$G$ acts faithfully on the set $S$ of roots of $f(x)$, i.e., $G \to S_n$ (where $|S| = n$).

Exercise. If $f(x)$ is irreducible, then this action is transitive.
(This follows immediately from Prop 1.9: $\exists \phi: F(a) \to F(b)$...).

Def: A simple radical extension of $F$ is a field $K = F(a)$, where $a^\ell \in F$ for some $n \in \mathbb{N}$, i.e., $a$ is a root of $x^\ell - b \in F[x]$.

Example: If char $F \neq 2$ and $[K:F] = 2$, then $K/F$ is a simple radical extension (complete the square).

Consider $f(x) = x^2 - 1 \in F[x]$, let $K$ be the splitting field.

If char $F = p > 0$, suppose $p + n$ (so $f'(x) \neq 0$, i.e., $(f(x), f'(x)) = 1$).

Prop 3.2 $\Rightarrow$ $f(x)$ has $n$ distinct roots, called the roots of unity.

The $n$th roots of unity form a multiplicative subgroup of $K \setminus \{0\}$.

By Prop 3.7, it is cyclic.

The generators are the primitive $n$th roots of unity.

Note: There are $\phi(n)$ primitive roots of unity, where $\phi$ is Euler's totient function: $\phi(n) = |\{0 < k < n : (n,k) = 1\}|$. 
Remark: if \( w \) is a primitive \( n^{th} \) root of unity, then
* \( 1, w, w^2, \ldots, w^{n-1} \) are all the \( n^{th} \) roots of unity
* \( K = F(w) \), a simple radical extension
* \( 1 + w + w^2 + \ldots + w^{n-1} = 0 \) (actually \( w \) need not be primitive).

Prop 4.1: (a) If \( \text{char } F = p \| n \), then the Galois group of \( x^{n-1} \in F[x] \) is abelian.

(b) Moreover, if \( F = \mathbb{Q} \), the Galois group \( x^{n-1} \in F[x] \) is isomorphic to the multiplicative group \( (\mathbb{Z}/n\mathbb{Z})^\times \).

PF: (a) Take \( G = \text{Gal}(F(w)/F) \), \( w \) is a primitive \( n^{th} \) root of unity.
If \( \phi, \theta \in G \), then \( \phi(w) \) and \( \theta(w) \) are roots of \( F(x) \).
Therefore, \( \phi(w)^i = w^i \), \( \theta(w)^j = w^j \) for some \( i, j \).
Thus, \( \phi \theta(w) = w^{ij} = \theta \phi(w) \).
Since \( F(w) \) is simple, every \( \phi \in G \) is determined by \( \phi(w) \),
so \( \phi \theta = \theta \phi \implies G \) is abelian. \( \checkmark \)

(b) Check that \( (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \text{Gal}(\mathbb{Q}(w)/\mathbb{Q}) \)
\[ a \pmod{n} \longrightarrow \Gamma_a \text{ where } \Gamma_a(w) = w^a \]
is an isomorphism (Easy exercise). \( \checkmark \)

Def: The polynomial \( \Phi_n(x) = \prod_{i=1}^{\phi(n)} (x - w_i) \) where \( w_1, \ldots, w_{\phi(n)} \) are the primitive roots of unity, is the \( n^{th} \) cyclotomic polynomial.
Remark: If \( \eta \) is a root of \( f(x) = x^n - 1 \), then \( \eta \) is a primitive \( d^{th} \) root of unity, where \( |\eta| = d \) in \( K \setminus \{0, 1\} \), so \( d \mid n \) (Lagrange). Therefore, \( x^n - 1 = \prod_{d \mid n} \Phi_d(x) \), and so

\[
\Phi_n(x) = \frac{x^n - 1}{\prod \{ \Phi_d(x) : d \text{ proper divisor of } n \}}
\]

Example:

\[
\Phi_1(x) = x - 1 \\
\Phi_2(x) = \frac{x^2 - 1}{\Phi_1(x)} = \frac{x^2 - 1}{x - 1} = x + 1 \\
\Phi_3(x) = \frac{x^3 - 1}{\Phi_1(x)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 \\
\Phi_4(x) = \frac{x^4 - 1}{\Phi_1(x) \Phi_2(x)} = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1 \\
\Phi_5(x) = \frac{x^5 - 1}{\Phi_1(x)} = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x) \Phi_2(x) \Phi_3(x)} = x^2 - x + 1
\]

Fact: If \( f = \Phi_n \), then \( \Phi_n(x) \in \mathbb{Z}[x] \).

Thm 4.2: The cyclotomic polynomial \( \Phi_n(x) \) in \( \mathbb{Q}[x] \) is monic, irreducible, in \( \mathbb{Z}[x] \), and has degree \( \phi(n) \).

Proof: It is clear that \( \Phi_n(x) \) is monic of degree \( \phi(n) \).

To show \( \Phi_n(x) \in \mathbb{Z}[x] \), use induction. Base case trivial. Assume it's true for all \( 1 \leq d < n \).

Then \( x^n - 1 = f(x) \Phi_n(x) \), where \( f(x) = \prod_{d \mid n, \text{d < n}} \Phi_d(x) \in \mathbb{Z}[x] \) is monic.
Clearly, \( f(x) \mid x^{p^n} - 1 \) in \( \mathbb{Q}(\omega)[x] \) (\( \omega \) a primitive \( n^{th} \) root of unity) and \( f(x), x^{p^n} - 1 \in \mathbb{Q}[x] \implies f(x) \mid x^{p^n} - 1 \) in \( \mathbb{Q}[x] \)
(by Euclidean Algorithm).

By Gauss' Lemma (Thm 3.13), \( f(x) \mid x^{p^n} - 1 \in \mathbb{Z}[x] \implies \Phi_n(x) \in \mathbb{Z}[x]. \)

Show \( \Phi_n(x) \) irreducible: Suppose that \( \Phi_n(x) = f(x)g(x) \),
where \( f(x), g(x) \in \mathbb{Z}[x] \) are both monic. (Goal: show one of them is \( 1 \)).

Let \( w \) be a primitive \( n^{th} \) root of unity, which is a root of \( f(x) \).
If \( p \nmid n \) is prime, then \( w^p \) is primitive, so \( w^p \) is a root of \( f(x) \) or \( g(x) \).

Suppose \( g(w^p) = 0. \) Then \( w \) is a root of \( g(x^p) \implies f(x) \mid g(x^p). \)
(since \( f(x) \) is the minimal poly for \( w \) over \( \mathbb{Q} \)).

Say \( g(x^p) = f(y)h(x), \) \( h(x) \in \mathbb{Z}[x]. \)
Reduce mod \( p: \) \( g(x^p) = (g(x))^p = \overline{f(x)} \overline{h(x)} \in \mathbb{F}_p[x]. \)

Since \( \mathbb{F}_p[x] \) is a UFD, \( \overline{f(x)} \) \& \( \overline{h(x)} \) have a common factor in \( \mathbb{F}_p[x]. \)
Note: \( \Phi_n(x) = f(x)g(x) \implies \overline{\Phi_n(x)} = \overline{f(x)} \overline{g(x)} \)
\( \implies \overline{\Phi_n(x)} \in \mathbb{F}_p[x] \) has a multiple root.
\( \Rightarrow x^{p^n} - 1 \) has a multiple root, since \( \overline{\Phi_n(x)} \mid x^{p^n} - 1. \)

Therefore, \( f(w^p) = 0. \)
Similarly, if \((n, a) = 1\), then \(w^n\) is a root of \(f(x)\).

\[\Rightarrow\] Every primitive \(n^{th}\) root of unity is a root of \(f(x)\).

\[\Rightarrow\] \(f(x) = \Phi_n(x)\) \(\triangleq \Phi_n(x) \triangleq \quad |\)

Thus, \(\Phi_n(x)\) is irreducible. \(\square\)

Prop 4.3: Suppose \(\text{char } F = p \not| n\), and \(\omega \in F\) is a primitive \(n^{th}\) root of unity, and \(0 \neq b \in F\). Then a splitting field \(K\) for \(f(x) = x^n - b\) over \(F\) is a simple radical extension of \(F\) and the Galois group \(G\) of \(f(x)\) is abelian.

pf: Let \(\alpha \in K\) be a root of \(f(x)\). The distinct roots are then \(\alpha, \alpha w, \alpha w^2, \ldots, \alpha w^{n-1}\), so \(K = F(\alpha)\), and \(\alpha^n = b + F\), so \(K/F\) is a simple radical extension. \(\checkmark\)

The proof that \(G\) is abelian is analogous to that in Prop 4.1 (but moreover, \(G\) is cyclic). \(\square\)

Def: \(K/F\) is an extension by radicals if there is a sequence \(F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n = K\) such that \(L_i/L_{i-1}\) is a simple radical extension.

Def: A polynomial \(f(x) \in F[x]\) is solvable by radicals over \(F\) if there is an extension \(K/F\) by radicals such that \(f(x)\) splits in \(K[x]\).

This just means that we have a "formula" for the elements of \(K\), e.g., quadratic formula, cubic formula.
Fact: Over $\mathbb{Q}$, all degree-2, 3, and 4 polynomials are solvable by radicals, but not all degree-5 polynomials are. We will formalize and prove this using Galois theory.

**Def:** If $F \subseteq E \subseteq K$ and $F \subseteq L \subseteq K$, define the join of $E$ in $L$ to be $E \vee L = F(E \triangleleft L)$; i.e., "smallest subfield of $K$ containing $E$ and $L$".

**Def:** If $G$ is a group, and $J, H \subseteq G$, define the join of $J \vee H$ to be $J \vee H = \langle J \cup H \rangle$; i.e., "smallest subgroup of $G$ containing $J$ and $H$".

**Exercise:** Suppose $F \subseteq E, L \subseteq K$, and $J, H \subseteq G = \text{Gal}(K/F)$. Then:

1. $J(E \triangledown L) = J(E) \cap J(L)$ and $F(J \vee H) = F(J) \cap F(H)$
Prop 4.4: Suppose $F \leq K_1, K_2 \leq L$ and $K_i / F$ is an extension by radicals ($i = 1, 2$). Then $K_1 \vee K_2$ is an extension by radicals.

Pf: If $K_1 = F(a_1, \ldots, a_m)$ and $K_2 = F(b_1, \ldots, b_n)$, then
\[ K_1 \vee K_2 = F(a_1, \ldots, a_m, b_1, \ldots, b_n). \]

Prop 4.5: If $K / F$ is a separable extension by radicals, and $L / F$ is a Galois closure, then $L / F$ is a separable extension by radicals.

Pf: Recall: $L$ is a splitting field for $F = \{ m_i(x) \}$ over $F$, where $\{a_1, \ldots, a_n\}$ is an $F$-basis for $K$.

Set $G = \text{Gal}(L / F)$.

Prop 3.3 $\Rightarrow \{ \phi(a_i) : \phi \in G, 1 \leq i \leq n \}$ spans $L$ over $F$.

If $G = \{ \phi_1, \ldots, \phi_k \}$, set $K_i = \phi_i(K)$.

Then $L = K_1 \vee K_2 \vee \cdots \vee K_k$. Apply Prop 4.4.

Thm 4.6 (Galois): Suppose char $F = 0$, and $f(x)$ is solvable by radicals.

Then the Galois group of $f(x)$ is solvable.

Remark: The converse holds as well. (See Thm 4.10.)

Pf: Let $F = L_0 \leq L_1 \leq \cdots \leq L_k = K$ be a sequence of simple radical extensions, with $L_i = L_{i-1}(a_i)$, $a_i \in L_{i-1}$, such that there is a splitting field $L$ for $f(x)$ over $F$, $L \leq K$.

Prop 4.5 $\Rightarrow$ wlog we may assume that $K / F$ is Galois (otherwise just take $K$ to be the Galois closure).
Let $G = \text{Gal}(L/F)$, the Galois group of $F(x)$.

By FTGT, $\text{Gal}(L/F) \cong \text{Gal}(K/F)/\text{Gal}(K/L)$. 

By Thm 5.4 (Groups), $(G \text{ solvable } \iff N \text{ solvable }$ and $G/N \text{ solvable}$).

$\text{Gal}(K/F) \text{ solvable } \iff \text{Gal}(K/L) \text{ solvable }$,

and $\text{Gal}(L/F) \text{ solvable }$.

**We want to show Gal($L/F$) is solvable, thus it suffices to show that Gal($K/F$) is solvable.**

Set $n = n_1 n_2 \ldots n_k$ and let $M$ be the splitting field for $x^n - 1$ over $K$.

Let $w$ be a primitive $n_i$th root of unity in $M$ (i.e., $M = K(w)$).

Note: $F(w)$ contains all $n_i$th roots of unity for $1 \leq i \leq k$.

Since $K/F$ is Galois, $K$ is the splitting field for some $g(x)$ over $F$.

Clearly, $M$ is a splitting field for $(x^{n_i} - 1)g(x)$ over $F$.

Therefore, $M/F$ is Galois.

By FTGT, $\text{Gal}(K/F) \cong \text{Gal}(M/F)/\text{Gal}(M/K)$.

and $\text{Gal}(M/K) \text{ solvable } \iff \text{Gal}(M/L) \text{ solvable }$ and $\text{Gal}(K/F) \text{ solvable }$.

**Suffices to show that Gal($M/K$) is solvable.**

Let $M_0 = F$, $M_1 = F(w)$, $M_2 = M_1(q_1)$, $\ldots$, $M_{k+1} = M_k(q_k) = M$. 


We now have the chain of subfields
\[ F \leq F(w) \leq F(w, a_i) \leq F(w, a_i, a_{i+1}) \leq \cdots \leq F(w, a_i, \ldots, a_k) = M, \]
\[ \text{i.e. } L_0 \leq L_1 \leq L_2 \leq \cdots \leq L_k = M, \]
\[ \text{i.e. } M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_k = M. \]

**Key:** Each \( M_{i+1} = M_i(a_i) \) contains a root \( a_i \) of \( X^{n_i} - b_i \) and the \( n_i \)th roots of unity.

\[ \Rightarrow \text{ Each } M_{i+1} = M_i(a_i) \text{ contains all roots of } X^{n_i} - b_i \]
\[ \Rightarrow M_{i+1}/M_i \text{ is Galois.} \]

**Prop. 4.3** \( \Rightarrow \text{Gal}(M_{i+1}/M_i) \text{ is abelian.} \)

Define \( H_0 = \text{Gal}(M/F) \)
\[ H_i = \text{Gal}(M/M_i) \leq \text{Gal}(M/F), \text{ etc.} \]

Note: \( M/M_i \) and \( M_{i+1}/M \) are Galois

Apply FTGT:
\[ \text{Gal}(M/M_{i+1}) = H_{i+1} \leq \text{Gal}(M/M_i) = H_i \]
and \( H_i/H_{i+1} \leq \text{Gal}(M_{i+1}/M_i) \) which is abelian.

By definition, \( \text{Gal}(M/F) \) is solvable
\[ \Rightarrow \text{Gal}(M_{i+1}/F) \text{ is solvable} \]
\[ \Rightarrow \text{Gal}(M_{i+1}/F) \text{ is solvable.} \]
Example: Let \( F(x) = x^5 + 5x^3 - 20x^2 + 5 \in \mathbb{Q}[x] \), which is irreducible by Eisenstein \((p=5)\).

By calculus, \( F(x) \) has exactly 3 real roots \( a_1, a_2, a_3 \).

Let \( a_4, a_5 \) be the complex (conjugate) roots.

Let \( K \subseteq \mathbb{C} \) be a splitting field for \( F(x) \) over \( \mathbb{Q} \).

Then \( 5 \mid [K: \mathbb{Q}] = |G| \Rightarrow G \) contains a "5-cycle" \( \sigma \) (Cauchy).

Also, by Thm 3.5(c), complex conjugation restricted to \( K \) is a \( \mathbb{Q} \)-automorphism, fixing \( a_1, a_2, a_3 \), and \( a_4 \leftrightarrow a_5 \).

This element \( \tau \) is a "2-cycle" of \( G \).

Basic group theory fact: Any 3-cycle and 2-cycle generate \( S_5 \).

Therefore, \( G \cong S_5 \), which is not solvable \((S_5 \cong A_5 \cong 1; A_5 \) is simple but not abelian\).

Thus, \( F(x) \) is not solvable by radicals.

Similarly, any degree-\( p \) polynomial \((\text{prime } p \neq 5)\) with exactly \( p-2 \) real roots is not solvable by radicals.

For the converse of Thm 4.6, we need some more tools.

Def: Suppose \( F \) contains a primitive \( n^{th} \) root of unity, and \( K=F(a) \) is a simple Galois extension, \([K:F]=n\), and \( G=\text{Gal}(K/F)=\langle \phi \rangle \) has order \( n \). If \( w \in F \) is an \( n^{th} \) root of unity, then define the Lagrange resolvent of \( w \) and \( a \) to be

\[
L(w, a) = a + W\phi(a) + W^2\phi^2(a) + \ldots + W^{n-1}\phi^{n-1}(a),
\]
Exercise: \( \Phi(L(w, a)) = L(w, \Phi(a)) = w^i L(w, a) \).

Cor: \( \Phi(L(w, a)^n) = \Phi(L(w, a))^n = (w^i L(w, a))^n = L(w, a)^n \)

* i.e., \( L(w, a)^n \) is fixed by every \( \phi \in \text{Gal}(k|F) \)

\[ \Rightarrow L(w, a)^n \in F. \]

Prop 4.7: Suppose \( w \in F \) is a primitive \( n^{th} \) root of unity

\[ K = F(a) \] a Galois extension with \( [K:F] = n \), and cyclic Galois group \( G = \text{Gal}(K|F) = \langle \phi \rangle \).

Then for some \( i \), \( L(w^i, a) \in K \setminus F \).

Pf: Recall that \( \sum_{i=0}^{n-1} w^i = 0 \). (See Remark, p. 2).

\[ \sum_{i=0}^{n-1} L(w^i, a) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} w^i \phi^j(a) = \sum_{j=0}^{n-1} \phi^j(a) \sum_{i=0}^{n-1} (w^i)^j = 0 \]

Exercise: Rearrangement

\[ = \phi^0(a) \sum_{i=0}^{n-1} (w^o)^j = an. \]

Since \( F \) contains a primitive \( n^{th} \) root of unity, \( \text{char } F \) \( \neq n \), so \( an \neq 0 \) \( \Rightarrow na \in K \setminus F \).

Therefore, at least one \( L(w^i, a) \in K \setminus F \). \( \blacksquare \)

Prop 4.8: Suppose \( p \in \mathbb{Z} \) is prime and \( F \) contains a \( p^{th} \) root of unity, and \( K/F \) is Galois with \( [K:F] = p \).

Then \( K/F \) is a simple radical extension.

Pf: Since \( [K:F] \) is prime, \( K = F(a) \) for any \( a \in K \setminus F \), and \( G = \text{Gal}(K|F) \) is cyclic \( (|G| = [K:F] = p) \).

By Prop 4.7, \( \exists \) Lagrange resolvent \( b \in K \setminus F \).

By Exercise, \( b^p = c \in F \), i.e., \( b \) is a root of \( x^p - c \in F[x] \).
Prop 4.9: Suppose \( f(x) \in F[x] \) has Galois group \( G \) over \( F \), and \( E \mid F \) is any extension field. Then the Galois group of \( f(x) \) over \( E \) is isomorphic to a subgroup of \( G \).

Pf: Let \( L \mid E \) be a splitting field for \( f(x) \), with roots \( a_1, \ldots, a_n \). Then \( K = F(a_1, \ldots, a_n) \) is a splitting field for \( f(x) \) over \( F \).

If \( \phi \in \text{Gal}(L \mid E) \), then \( \phi \) permutes \( a_1, \ldots, a_n \), so \( \phi(K) = K \)
and \( \phi = 1_K \iff \phi(a_i) = a_i \forall i \iff \phi = 1_L \in \text{Gal}(L \mid E) \).

Thus, \( \exists \text{ Gal}(L \mid E) \xrightarrow{\phi} \text{Gal}(K \mid F) \)

Thus 4.10 (Galois): Suppose \( \text{char } F = 0 \), \( f(x) \in F[x] \), and the Galois group of \( f(x) \) is solvable. Then \( f(x) \) is solvable by radicals over \( F \).

Pf: Let \( K \) be a splitting field for \( f(x) \) over \( F \), set \( G = \text{Gal}(K \mid F) \) and say \( [K : F] = n \).

Let \( L \mid K \) be a splitting field for \( x^n - 1 \), with \( L \) a primitive \( n \)th root of unity.

Set \( E = F(w) \), and so clearly \( L \mid E \) is a splitting field for \( f(t) \).

Set \( H = \text{Gal}(L \mid E) \)

Prop 4.9 \( \Rightarrow H \xrightarrow{\phi} G = \text{Gal}(K \mid F) \).

\( G \) solvable (by assumption) \( \Rightarrow H \) solvable.
By Thm 5.3 (Groups), \( H \) has a subnormal series \( H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_k = 1 \) with abelian factors, and we can assume that \( H_{i-1}/H_i \) is cyclic of prime order \( p_i \) (by refinement).

Since \( E \subseteq L_i \), set \( L_i = F H_i \), so

\[ E = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = L, \quad [L_i : L_{i-1}] = p_i. \]

Since \( \text{Gal}(L/L_i) = H_i \supset H_{i-1} = \text{Gal}(L/L_{i-1}) \),

\( L_i/L_{i-1} \) is Galois, and \( L_{i-1} \) contains a primitive \( p_i \)-th root of unity (which is a power of \( w \)).

By Prop 4.8, \( L_i/L_{i-1} \) is a simple radical extension, \( i=1, \ldots, k \).

Thus, \( L/E \) (i.e., \( L_k/L_0 \)) is an extension by radicals.

Since \( F = E(w) \), \( L/F \) is also an extension by radicals.

\( \square \)

Cor (of Thms 4.6, 4.10): Suppose \( \text{char } F = 0 \) and \( f(x) \in F[x] \).

Then \( f(x) \) is solvable by radicals iff the Galois group of \( F(x) \) is solvable.