1 Genesis Of Galois Theory

Definition 1.1 (Radical Extension). A field extension $K/F$ is radical if there is a tower of field extensions $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n = K$ where $F_{i+1} = F_i(\alpha_i)$, $\alpha_i^{r_i} \in F_i$ for some $r_i \in \mathbb{Z}^+$. 

2 Splitting Fields

Proposition-Definition 2.1 (Field Homomorphism). A map of fields $\sigma : F \rightarrow F'$ is a field homomorphism if it is a ring homomorphism. We also have:

(i) $\sigma$ is injective
(ii) $\sigma[x] : F[x] \rightarrow F'[x]$ is a ring homomorphism where 

$$\sigma[x](\sum_{i=1}^{n} f_i x^i) = \sum_{i=1}^{n} \sigma(f_i)x^i$$

Proposition 2.1. $K = F[x]/\langle p(x) \rangle$ is a field extension of $F$ via composite ring homomorphism $F \hookrightarrow F[x] \rightarrow F[x]/\langle p(x) \rangle$. Also $K = F(\alpha)$ where $\alpha = x + \langle p(x) \rangle$ is a root of $p(x)$. 

Proposition 2.2. Let $\sigma : F \rightarrow F'$ be a field isomorphism (a bijective field homomorphism). Let $p(x) \in F[x]$ be irreducible. Let $\alpha$ and $\alpha'$ be roots of $p(x)$ and $(\sigma p)(x)$ respectively (in appropriate field extensions). Then there is a field extension $\tilde{\sigma} : F(\alpha) \rightarrow F'(\alpha')$ such that:

(i) $\tilde{\sigma}$ extends $\sigma$, i.e. $\tilde{\sigma}|_F = \sigma$
(ii) $\tilde{\sigma}(\alpha) = \alpha'$

Definition 2.1 (Splitting Field). Let $F$ be a field and $f(x) \in F[x]$. A field extension $K/F$ is a splitting field for $f(x)$ over $F$ if:

*The following notes were based on Dr Daniel Chan’s MATH5725 lectures in semester 2, 2007.*
(i) $f(x)$ factors into linear polynomials over $K$

(ii) $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of $f(x)$ in $K$

**Note.** Consider tower of field extension $F \subseteq K \subseteq L$ and $f(x) \in F[x]$. If $L$ is a splitting field for $f(x)$ over $F$, then it is a splitting field for $K$. If $K$ is generated by roots of $f(x)$ then the converse also holds.

**Theorem 2.1.** Let $F$ be a field and $f(x) \in F[x]$. Then there is a splitting field $K$ of $f(x)$ over $F$.

**Theorem 2.2.** Let $\sigma : F \rightarrow F'$ be a field isomorphism and $f(x) \in F[x]$. Suppose $K, K'$ are splitting fields for $f(x)$ and $(\sigma f)(x)$ over $F$ and $F'$ respectively. Then there is an isomorphism of fields $\tilde{\sigma} : K \rightarrow K'$ which extends $\sigma$. This is referred to as the uniqueness of splitting fields.

### 3 Algebraic Closure

**Definition 3.1** (Algebraic Extension & Algebraic Closure). Some definitions.

(i) A field extension $K/F$ is algebraic over $F$ if every $\alpha \in K$ is algebraic over $F$

(ii) A field $K$ is algebraically closed if the only algebraic extension of $K$ is $K$ itself

(iii) $K$ is an algebraic closure of $F$ if it is an algebraic field extension of $F$ such that $K$ is algebraically closed

**Proposition 3.1.** Let $F \subseteq K \subseteq L$ be a tower field extensions then:

(i) $[L : F] = [L : K][K : F]$

(ii) $L/F$ is algebraic if and only if both $L/K$ and $K/F$ are algebraic

(iii) Finite field extensions are algebraic

(iv) If $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over $F$, then $K$ is finite over $F$

**Note.** If $\alpha$ is transcendental, then $[F(\alpha) : F] = \infty$ as irreducible polynomial with root $\alpha$ does not exist.

**Lemma 3.1.** Let $F$ be a field. There exists a set $S$ such that for any algebraic field extension $K/F$, $|K| < |S|$.

**Remark.** Either $K$ is countable or $|K| = |F|$.
Definition 3.2 (Splitting Field). A field extension $K/F$ is a splitting field for $\{f_i(x)\}_{i \in I}$ over $F$ if:

(i) every $f_i(x)$ factorises into linear factors over $K$

(ii) $K$ is generated is the field generated by $F$ and all the roots of all the $f_i(x)$'s

Remark. If $I$ is finite, $K$ is just the splitting field for $\prod_{i \in I} f_i(x)$.

Proposition 3.2. In field extension $K/F$, let $\{\alpha_j\}_{j \in J} \subseteq K$. The subfield of $K$ generated by $F$ and the $\alpha_j$'s is:

(i) intersection of all the subfields of $K$ containing $F$ and all the $\alpha_j$'s

(ii) union of all $F(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_n})$ where $\{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_n}\} \subseteq J$

Theorem 3.1. Let $F$ be a field and $\{f_i(x)\}_{i \in I} \subseteq F[x] - 0$.

(i) There exists a splitting field $K$ for $\{f_i(x)\}_{i \in I}$ over $F$

(ii) Suppose there is a field isomorphism $\sigma : F \longrightarrow F'$ and $K'$ is a splitting field for $\{(\sigma f_i)(x)\}_{i \in I}$ over $F'$. There is a field isomorphism $\tilde{\sigma} : K \longrightarrow K'$ which extends $\sigma$.

4 Field Automorphisms

Proposition-Definition 4.1 (Field Homomorphism Over $F$). Let $K$, $K'$ be field extensions of field $F$. We say a homomorphism $\sigma : K \longrightarrow K'$ fixes $F$ or $\sigma$ is a field homomorphism over $F$ if $\sigma(\alpha) = \alpha$ for any $\alpha \in F$. Such homomorphisms are linear over $F$. If furthermore $K = K'$ and $\sigma$ is an automorphism then we say $\sigma$ is a field automorphism over $F$.

Proposition-Definition 4.2 (Galois Group). Let $K/F$ be a field extension of $F$. Let $G$ be the set of field automorphisms of $K$ over $F$. Then $G$ is a group when endowed with composition as group multiplication. It is called the Galois group of $K/F$ and is denoted by $\text{Gal}(K/F)$.

Lemma 4.1. Let $f(x) \in F[x]$. $K/F$ is a field extension and $\alpha \in K$ is a root of $f(x)$. Let $\sigma : K \longrightarrow K'$ be a field homomorphism over $F$. Then $\sigma(\alpha)$ is also a root of $f(x)$.

Remark. Any field homomorphism $\sigma : F(\alpha_1, \alpha_2, \ldots, \alpha_n) \longrightarrow K$ over $F$ is determined by values $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$ since $\sigma$ fixes $F$.

Corollary 4.1. Let $K$ be a splitting field for $f(x) \in F[x]$ over field $F$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be roots of $f(x)$, so that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then any $\sigma \in G = \text{Gal}(K/F)$ permutes the roots of $\alpha_1, \alpha_2, \ldots, \alpha_n$ and so gives an injective group homomorphism $G \longrightarrow \text{Perm}\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \cong S_n$.

Lemma 4.2. Let $F$ be a field and $f(x) \in F[x]$. Let $K$ the splitting field for $f(x)$ over $F$. Suppose $\alpha$ and $\alpha'$ are roots of an irreducible factor $f_0(x)$ of $f(x)$ over $F$. Then there is a $\sigma \in G = \text{Gal}(K/F)$ such that $\sigma(\alpha) = \alpha'$. In particular, $G$ acts transitively on roots of $f_0(x)$. 

3
5 Fixed Fields

**Proposition-Definition 5.1** (Fixed Field). The fixed field of $G$ in $K$ is $K^G = \{\alpha \in K : \sigma(\alpha) = \alpha, \text{ for any } \sigma \in G\}$ and it is a subfield of $K$.

**Definition 5.1** (Prime Maps). Let $K/F$ be a field extension. $G = K/F$. We define two maps, both called prime. 
\{subgroups of $G$\} $\longleftrightarrow$ \{intermediate fields of $K/F$\}; $H \mapsto H' = K^H$; $K_0 \mapsto K'_0 = \text{Gal}(K/K_0)$.

**Lemma 5.1.** Let $H_1, H_2, \ldots$ denote subgroups of $G$ and $K_1, K_2, \ldots$ the intermediate fields of $K/F$. Priming reverses inclusions:

(i) $H_1 \subseteq H_2 \implies H'_1 \supseteq H'_2$

(ii) $K_1 \subseteq K_2 \implies K'_1 \supseteq K'_2$

**Lemma 5.2.** $H_1 \subseteq H''_1$ and $K_1 \subseteq K''_1$.

**Definition 5.2** (Closed Subsets). We $H_1$ is a closed subgroup of $G$ if $H_1 = H''_1$ and $K_1$ is a closed intermediate field of $K/F$ of $K_1 = K''_1$. The closure of $H_1$ and $K_1$ are $H''_1$ and $K''_1$ respectively.

**Lemma 5.3.** $H'_1 = H'''_1$ and $K'_1 = K'''_1$.

**Theorem 5.1.** Priming induces a well defined bijection \{closed subgroups of $G$\} $\longleftrightarrow$ \{closed intermediate fields of $K/F$\}; $H \mapsto H' = K^H$; $K_0 \mapsto K'_0 = \text{Gal}(K/K_0)$.

6 Two Technical Results

**Theorem 6.1.** Let $K_1 \leq K_2$ be intermediate fields. Then $[K_1' : K_2'] \leq [K_2 : K_1] = n$ if $n < \infty$.

**Lemma 6.1.** Let $\sigma, \tau \in K'_1$ then $\sigma K'_2 \neq \tau K'_2$ (distinct cosets) $\implies \sigma(\alpha) \neq \tau(\alpha)$, i.e. $[K_1' : K_2'] \leq \text{number of distinct } \sigma'$s $\leq n$.

**Lemma 6.2.** Let $\sigma, \tau \in G$ be such that $\sigma H_1 = \tau H_1$. Then for any $\alpha \in H'_1$, we have $\sigma(\alpha) = \tau(\alpha)$.

**Remark.** As a result, given any left coset $C \subseteq H_1 \subseteq G$ and $\alpha \in H'_1$, we can unambiguously define $C(\alpha) = \sigma(\alpha)$ where $\sigma$ is any element of $C$.

**Theorem 6.2.** Let $H_1 \leq H_2 \leq G$. Suppose $n = [H_2 : H_1] < \infty$. Then $[H'_1 : H'_2] \leq [H_1 : H_2]$.
7 Galois Correspondence

**Corollary 7.1.** Two corresponding results.

(i) Let $H_1 \leq H_2 \leq G$. If $H_1$ is closed and $[H_2 : H_1] < \infty$ then $H_2$ is closed and $[H_2 : H_1] = [H'_1 : H'_2]$

(ii) Given intermediate fields $K_1 \leq K_2 \leq K$. Supposed $K_1$ is closed and $[K_2 : K_1] < \infty$ then $K_2$ is closed and $[K_2 : K_1] = [K'_1 : K'_2]$

**Definition 7.1 (Galois Extension).** An algebraic field extension $K/F$ is Galois if $F$ is closed, i.e. $F = F'' = K^{\text{Gal}(K/F)}$.

**Proposition 7.1.** Let $K/F$ be a finite field extension.

(i) $G = \text{Gal}(K/F)$ is finite

(ii) $K/F$ is Galois $\implies [K : F] = |G|$

(iii) If $|G| \geq [K : F]$ then $K/F$ is Galois

**Theorem 7.1 (Fundamental Theorem Of Galois Theory).** Let $K/F$ be a finite Galois extension and $G = \text{Gal}(K/F)$.

(i) There are inverse bijections $\{\text{subgroups of } G\} \leftrightarrow \{\text{intermediate fields of } K\}$; $H \mapsto H' = K^H$; $K_0 \mapsto K'_0 = \text{Gal}(K/K_0)$

(ii) For intermediate field $K_0$, $K/K_0$ is Galois with Galois group $\text{Gal}(K/K_0) = K'_0$

**Note.** In fact, we can show that all intermediate fields of a Galois extension are closed. So are the subgroups of the corresponding Galois group.

**Theorem 7.2.** Let $K$ be a field and $G$ be a finite group of field automorphisms of $K$. If $F = K^G$ then $K/F$ is Galois and the Galois group is $G$, i.e. $K/K^G$ is Galois with Galois group $G$.

8 Normality

**Definition 8.1 (Normal Extension).** $K$ is a splitting field over $F$ if it is the splitting field of some family of polynomials over $F$. We say also in this case that $K/F$ is normal.

**Proposition 8.1.** Let $K/F$ be a Galois extension with Galois group $G$.

(i) Let $\alpha \in K$ and $p(x) \in F[x]$ be its minimal polynomial. Then $p(x)$ factorises over $K$

(ii) $K$ is the splitting field of $\{f_i\}$ over $F$ where $f_i$ ranges over the minimum polynomials of all $\alpha \in K$
Lemma 8.1. Let $K/F$ be an algebra extension and $\sigma : K \rightarrow K$ be a field homomorphism over $F$. Then $\sigma$ is an isomorphism.

Proposition 8.2. Let $K$ be the splitting field of $\{f_i\}$ over $F$. Given field extension $L$ of $K$ and field homomorphism $\sigma : K \rightarrow L$ over $F$, we have $\sigma(K) = K$. This is referred to as the stability of splitting fields.

Remark. Let $K/F$ be a Galois extension with Galois group $G = \text{Gal}(K/F)$. $G$ acts on $\{\text{intermediate fields of } K/F\}$ by $K_1 \mapsto \sigma(K_1)$ where $\sigma \in G$ and on $\{\text{subgroups of } G\}$ by conjugation, i.e. $H \mapsto \sigma H \sigma^{-1}$.

Proposition 8.3. Let $\sigma \in G$.

(i) If $K_1$ is an intermediate field then $(\sigma(K_1))' = \sigma K_1 \sigma^{-1}$

(ii) For $H \leq G$, $\sigma(H') = (\sigma H \sigma^{-1})'$

Theorem 8.1. Let $K/F$ be a finite Galois extension. Let $G$ be the Galois group $\text{Gal}(K/L)$. If $L$ is an intermediate field then $L/F$ is Galois if and only if $L' = \text{Gal}(K/L) \subseteq G$ is a normal subgroup. In this case $\text{Gal}(L/F) = G/L'$.

Note. So for a Galois extension, we have a bijection between Galois subfields and normal subgroups.

9 Separability

Proposition-Definition 9.1 (Inseparability). Let $K/F$ be a field extension. Suppose $\text{char}(F) \neq p$. We say $\alpha \in K$ is purely inseparable over $F$ if there is some $n \geq 1$ with $\alpha^{p^n} \in F$. In this case, $\text{Gal}(F(\alpha)/F) = 1$.

Definition 9.1 (Derivative). Let $F$ be a field. We can define derivatives as

$$f'(x) = \frac{df}{dx} = \sum_{j=0}^{n} f_{j}x^{j-1} \in F[x]$$

if $f(x) = \sum_{j=0}^{n} f_{j}x^{j} \in F[x]$

Remark. The following properties of the derivative holds for $f, g \in F[x]$:

(i) $(f + g)' = f' + g'$

(ii) $(fg)' = fg' + f'g$

(iii) $\alpha$ is a multiple root of $f(x) \in F[x]$ if and only if $0 = f(\alpha) = f'(\alpha)$
Definition 9.2 (Separable Degree). Let $K/F$ be a finite field extension. Its separable degree is $[K : F]_S = \text{number of field homomorphisms } \sigma : K \rightarrow F$ over $F$.

Proposition-Definition 9.2 (Separability). Let $f(x) \in F[x]$ be irreducible. The following are equivalent.

(i) In the splitting field $L$ of $f(x)$ over $F$, $f(x)$ factorises into distinct linear factors

(ii) $f'(x) \neq 0$

(iii) $[F(\alpha) : F] = [F(\alpha) : F]_S$ where $\alpha$ is a root of $f(x)$

(iv) $f(x)$ and $\alpha$ are separable over $F$

Definition 9.3 (Separability). A field extension $K/F$ is separable if every $\alpha \in K$ is separable over $F$.

Theorem 9.1. Let $K \supseteq L \supseteq F$ be a tower of finite field extensions. Then:

(i) $[K : F]_S = [K : L]_S[L : F]_S$

(ii) $[K : F]_S \leq [K : F]$ with equality occurring if and only if $K/F$ is separable

Remark. In fact, suppose $\sigma_i : K \rightarrow F$ are distinct homomorphisms over $L$ and $\tau_j : L \rightarrow F$ distinct homomorphisms over $F$. We can then extend $\tau_j$ to $\overline{\tau_j} : L \rightarrow F$. It follows that $\overline{\tau_j}\sigma_i$ are all the distinct homomorphisms from $K \rightarrow F$.

Corollary 9.1. Two results.

(i) Consider finite field extensions $K/L$, $L/F$. Then $K/F$ is separable if and only if $K/L$ and $L/F$ are separable

(ii) If a field $K$ is generated over $F$ by separable elements $\{\alpha_i\}$ then $K/F$ is separable

10 Criterion For Galois

Lemma 10.1. Let $K/F$ be a Galois extension. Let $L \subseteq K$ be a splitting field of some $f(x) \in F[x]$ over $F$, then $L/F$ is Galois.

Theorem 10.1. $K/F$ is a Galois extension if and only if $K$ is separable splitting field over $F$.

Proposition 10.1. The following are equivalent.

(i) $K/F$ is a normal extension, i.e. $K$ is a splitting field over $F$ for some family of polynomials
(ii) For any \( \alpha \in K \) if \( f_\alpha(x) \) is its minimal polynomial over \( F \) then \( f_\alpha(x) \) factorises linearly over \( K \).

**Theorem 10.2.** Let \( K/F \) be an algebraic extension. For \( \alpha \in K \), let \( f_\alpha(x) \in F[x] \) be its minimal polynomial over \( F \). Let \( L \supseteq K \) be the splitting field of \( \{ f_\alpha(x) \}_\alpha \) over \( F \). So in particular \( L \supseteq K \).

(i) If \( L_1 \) is a subfield of \( K \) such that \( L_1/F \) is normal and \( L_1 \supseteq K \) then \( L_1 \supseteq L \).

(ii) If \( K/F \) is separable, so is \( L/F \), i.e. \( L/F \) is Galois.

(iii) If \( K/F \) is finite, so is \( L/F \) and \( L \) is a splitting field of a single polynomial \( f(x) \in F[x] \) over \( F \).

**Note.** 10.2 (i) implies that \( L \) is the smallest splitting field containing \( K \) over \( F \). For (iii), the single polynomial \( f(x) \) is given by \( f(x) = \prod_{i=1}^{n} f_{\alpha_i}(x) \) where \( K = F(\alpha_1, \alpha_2, \ldots, \alpha_n) \).

**Definition 10.1 (Normal & Galois Closures).** The field \( L \) in Theorem 10.2 is called the normal closure of \( K \) over \( F \). If \( K/F \) is separable, then we also call \( L \) the Galois closure of \( K \) over \( F \).

**Remark.** In a field of characteristic 0, where separability is guaranteed, you can always embed a finite extension in a finite Galois extension, i.e. Theorem 10.2 (iii).

## 11 Radical Extensions

**Proposition 11.1.** Let \( F \) be a field of characteristic \( p \) and \( n \geq 2 \) be such that \( p \nmid n \). The group of roots of unity in \( F^\times \) is \( \mu_n \cong \mathbb{Z}/n\mathbb{Z} \).

**Lemma 11.1.** Let \( p \) be a prime and \( F \) be a field with all the \( p \) roots of unity. For \( \alpha \in F \), let \( K = F(\sqrt[p]{\alpha}) \). Then:

(i) \( K/F \) is a splitting field for \( x^p - \alpha \) over \( F \).

(ii) If \( \operatorname{char}(F) \neq p \) and \( \sqrt[p]{\alpha} \notin F \) then \( K/F \) is Galois with Galois group \( \operatorname{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z} \).

(iii) If \( \operatorname{char}(F) = p \) or \( \sqrt[p]{\alpha} \in F \) then \( \operatorname{Gal}(K/F) = 1 \).

**Lemma 11.2.** Let \( p \) be a prime and \( F \) be a field. Let \( K \) be the splitting field of \( x^p - 1 \) over \( F \). Then \( \operatorname{Gal}(K/F) \) is abelian. In fact, \( K = F(\omega) \) where \( \omega^p = 1 \).

**Definition 11.1 (Solvability).** Let \( G \) be a group. A normal chain of subgroups is a sequence of the form \( 1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G \). We say \( G \) is solvable if there exists such a chain of normal subgroups with \( G_{i+1}/G_i \) of cyclic prime order or trivial.

**Theorem 11.1.** Consider tower of field extensions \( F = F_0 \leq F_1 \leq F_2 \leq \ldots \leq F_n = K \) where \( F_{i+1} = F_i(\sqrt[p_i]{\alpha_i}) \) for some prime \( p_i \) and \( \alpha_i \in F_i \). Suppose \( K/F \) is Galois and \( F \) contains all \( p_i \)th roots of unity. Then \( G = \operatorname{Gal}(K/F) \) is solvable.
12 Solvable Groups

Proposition 12.1. Let $G$ be a finite group and $N \trianglelefteq G$. Then $G$ is solvable if and only if $N$ and $G/N$ are both solvable.

Proposition 12.2. A finite group $G$ is solvable if and only if there is a normal chain of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ with all $G_{i+1}/G_i$ abelian.

Definition 12.1 (Commutator Group). Let $G$ be a group and $g, h \in G$. The commutator of $g$ and $h$ is $[g, h] = g^{-1}h^{-1}gh$. The commutator subgroup of $G$ is the group generated by all $[g, h]$ as $g, h$ ranges over $G$. It is denoted by $[G, G]$.

Proposition 12.3. Let $G$ be a group.

(i) $[G, G] \trianglelefteq G$

(ii) $G/[G, G]$ is abelian

(iii) Given any $N \trianglelefteq G$ with $G/N$ abelian, we have $N \geq [G, G]$, i.e. $G/[G, G]$ is the largest abelian quotient group

Definition 12.2 (Derived Series). Let $G$ be a finite group. Its derived series is the normal chain of subgroups $G = G^{(0)} \triangleright G^{(1)} \triangleright \ldots$ where $G^{(r+1)} = [G^{(r)} : G^{(r)}]$.

Corollary 12.1. A finite group $G$ is solvable if and only if in the derived series $G^{(r)} = 1$ for some $r < \infty$.

Theorem 12.1. Let $n \geq 5$.

(i) $[A_n : A_n] = A_n$

(ii) $A_n$ and $S_n$ are not solvable

13 Solvability By Radicals

Lemma 13.1. Let $L$ be a Galois closure of a separable radical extension then $L$ is radical.

Theorem 13.1. Let $K/F$ be a field extension which embeds in separable radical extension $L/F$ in the sense that we have a tower of field $F \leq K \leq L$. Then $G = \text{Gal}(K/F)$ is solvable.

Definition 13.1 (Solvability). Let $F$ be a field and $f(x) \in F[x]$ be irreducible. The Galois group of $f(x)$ is $\text{Gal}(K/F)$ where $K$ is the splitting field of $f(x)$ over $F$. We say $f(x)$ is solvable by radicals if $K/F$ embeds in a separable radical extension $L/F$ as in Theorem 13.1, i.e. $\text{Gal}(K/F)$ solvable.

Corollary 13.1. For $p(x), F, K$ as in Definition 13.1. The Galois group of $p(x)$ over $F$ is $S_n = \text{Gal}(K/F)$. If $n \geq 5$, $p(x)$ is not solvable by radicals as $S_n$ is not.
14 A Polynomial Not Solvable By Radicals

**Lemma 14.1.** Fix $p$ a prime. Let $\sigma, \tau \in S_p$ be a p-cycle and a 2-cycle respectively. Then the subgroup generated by $\sigma, \tau$ is $S_p$.

**Proposition 14.1.** Let $f(x) \in \mathbb{Q}[x]$ be irreducible of degree $p$. Suppose $f(x)$ has exactly two non-real roots. Then the Galois group of $f(x)$ is $G = S_p$. Thus $f(x)$ is not solvable by radicals if $p \geq 5$.

**Theorem 14.1.** Let $K/F$ be a finite separable extension then $K = F(\alpha)$ for some $\alpha \in K$. In particular, $\alpha$ is such that $[F(\alpha) : F]$ is maximum.

**Theorem 14.2** (Fundamental Theorem Of Algebra). $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$ is algebraically closed.

**Lemma 14.2.** Let $P$ be any 2-group. There is a chain of subgroups $P = P_0 \leq P_1 \leq P_2 \leq \ldots \leq 1$ with $[P : P_i] = 2^i$.

15 Traces & Norms

**Definition 15.1** (Trace & Norm). Let $K/F$ be a finite field extension of degree $n$. Let $\alpha \in K$ and multiplication by $\alpha$ be $m_\alpha : K \rightarrow K$ an $F$-linear map. Represent $m_\alpha$ by the $n \times n$ matrix over $F$, $M_\alpha$. We define the trace of $\alpha$ to be $\text{tr}_{K/F}(\alpha) = \text{tr}(M_\alpha)$ and the norm of $\alpha$ to be $N_{K/F}(\alpha) = \det(M_\alpha)$.

**Notation.** For finite field extension $L/F$, let $G_{L/F}$ be the set of field homomorphisms $L \rightarrow \overline{L}$, so that $|G_{L/F}| = [L : F]_S$.

**Proposition 15.1.** Let $K/F$ be a finite separable extension. Then for $\alpha \in K$, we have
\[
\text{tr}(\alpha) = \sum_{\sigma \in G_{K/F}} \sigma(\alpha) \quad \text{and} \quad N(\alpha) = \prod_{\sigma \in G_{K/F}} \sigma(\alpha)
\]

**Theorem 15.1.** Let $F, K$ be fields. Consider distinct field homomorphisms $X_1, X_2, \ldots, X_n : F \rightarrow K$. These are linearly independent over $F$, i.e. there are $a_1, a_2, \ldots, a_n \in K$ with $a_1X_1(\alpha) + a_2X_2(\alpha) + \ldots + a_nX_n(\alpha) = 0$ for all $\alpha \in F$ then all the $a_i$’s are zero.

**Corollary 15.1.** Let $K/F$ be a finite separable extension. Then there exists an element $\alpha \in K$ with $\text{tr}_{K/F}(\alpha) = 1$.
16 Cyclic Extensions

Definition 16.1 (Cyclic Extension). A Galois extension is cyclic if its Galois group is either cyclic or abelian.

Theorem 16.1 (Hilbert’s Theorem 90). Let $K/F$ be a cyclic extension of degree $n$ with Galois group $G = \langle \sigma \rangle$. Then $\alpha \in K$ satisfies $N(\alpha) = 1$ if and only if $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in K$.

Theorem 16.2. Let $K/F$ be a cyclic extension of degree $n$. Suppose $\text{char} F \nmid n$ and $F$ contains all $n$th roots of 1. Then $K = F(\beta)$ where $\beta$ has a minimal polynomial $x^n - b$ over $F$. In particular, we have $\beta$ is such that $\omega = \frac{\beta}{\sigma(\beta)}$, where $\omega^n = 1$.

Theorem 16.3. Let $K/F$ be a cyclic extension of degree $n$ and with Galois group $G = \langle \sigma \rangle$. Then $\alpha \in K$ satisfies $\text{tr}(\alpha) = 0$ if and only if $\alpha = \beta - \sigma(\beta)$.

Theorem 16.4. Let $K/F$ be a Galois extension of prime degree $p = \text{char}(F)$. Then $K = F(\beta)$ where $\beta$ has minimum polynomial $x^p - x - b$ over $F$. In particular, we have $\beta$ is such that $1 = \beta - \sigma(\beta)$.

Note. In Theorem 16.4, $[K : F] = p$, prime. So $|G| = p$ and $G$ is cyclic of degree $p$. Thus $K/F$ is also cyclic of degree $p$.

17 Solvable Extension

Definition 17.1 (Solvable Extension). Let $K/F$ be a finite separable extension. We say $K/F$ is solvable if its Galois closure has solvable Galois group.

Theorem 17.1. Let $F$ be a field of characteristic 0. Then any solvable extension $K/F$ embeds in a radical extension.

Lemma 17.1. Suppose $K$ and $F$ as in Theorem 17.1. Let $n = |G|$ where $G = \text{Gal}(K/F)$. Let $K_1$ and $F_1$ be obtained from $K$ and $F$ respectively by adjoining all $n$th roots of unity. Then $G_1 = \text{Gal}(K_1/F_1)$ is also solvable.

Remark. Theorem 17.1 is false if $\text{char}(F) > 0$ since there are cyclic extensions of degree $p$ which cannot be constructed by adjoining $p$th roots (since $x^p - a = (x - \sqrt[p]{a})^p$ is not separable). But if we only assume $K/F$ finite and separable in Theorem 17.1, we do have another version of the theorem provided in our tower of field extensions, we allow not just adjoining $p$th roots but also roots of $x^p - x - a$. 

11
18 Finite Fields

Proposition 18.1. Let $K$ be a finite field and $p$ prime.

(i) $\text{char}(K) = p > 0$

(ii) $|K| = p^{[K:F_p]}$

(iii) $K$ is a subfield of $\mathbb{F}_p$

Proposition-Definition 18.1 (Frobenius Norm). Let $K$ be a field of characteristic prime $p$. The Frobenius homomorphism is the map $\phi : K \rightarrow K; x \mapsto x^p$.

(i) This is a field homomorphism

(ii) If $K$ is finite or is $\mathbb{F}_p$ then $\phi$ is an automorphism

Lemma 18.1. Let $K$ be a field with $p^n$ elements, $n$ a positive integer. Then any $\alpha \in K$ is a root of $x^{p^n} - x = 0$. Equivalently if $\phi$ is Frobenius homomorphism, $\phi^n(\alpha) = \alpha$. In particular, $\phi^n$ is the identity on $K$.

Theorem 18.1. Let $\phi : \mathbb{F}_p \rightarrow \mathbb{F}_p$ be the Frobenius homomorphism.

(i) The fixed field $\mathbb{F}_{p^n} = \mathbb{F}_p(\phi^n)$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$

(ii) $|\mathbb{F}_{p^n}| = p^n$

(iii) If $K$ is a subfield of $\mathbb{F}_p$ with $p^n$ elements then $K = \mathbb{F}_{p^n}$

(iv) $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a cyclic of degree $n$ and has Galois group $\langle \phi \rangle = \mathbb{Z}/n\mathbb{Z}$

(v) $\mathbb{F}_p/\mathbb{F}_p$ is Galois

Note. Galois group of $\mathbb{F}_p/\mathbb{F}_p$ is not $\langle \phi \rangle$.

Corollary 18.1. Two useful facts.

(i) The subfields of $\mathbb{F}_{p^n}$ are those of the form $\mathbb{F}_{p^d}$, $d \mid n$

(ii) $\mathbb{F}_{p^n}/\mathbb{F}_{p^d}$ is cyclic of degree $\frac{n}{d}$

Remark. The lattice of finite subfields of $\mathbb{F}_p$ is just the lattice of positive integers ordered by divisibility, i.e. if $n$, $l$ are positive integers with lowest common multiple $m$, greatest common divisor $d$, the smallest subfield containing $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^l}$ is $\mathbb{F}_{p^m}$, while $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^l} = \mathbb{F}_{p^d}$. 

12
19 Topological Groups

Definition 19.1 (Topological Group). A topological group is a group $G$ endowed with a topology such that:

(i) Multiplication map $\mu : G \times G \to G$ is continuous

(ii) The inverse map $\eta : G \to G; \ g \mapsto g^{-1}$ is also continuous

Proposition 19.1. Let $G$ be a topological group.

(i) For $g \in G$, left and right multiplication by $g$ are bi-continuous

(ii) If $U \subseteq G$ is open then $gU$ is open for every $g \in G$

(iii) Let $U \subseteq G$ be an open subgroup then $U$ is closed

Proposition 19.2. Let $\{G_\alpha\}_{\alpha \in A}$ be a set of topological groups. Then $G = \prod_\alpha G_\alpha$ endowed with the product topology is a topological group.

Notation. Consider data of:

(i) A partial ordered set $(A, \leq)$

(ii) For each $\alpha \in A$, a group $G_\alpha$

(iii) For each $\alpha, \beta \in A$, with $\alpha \leq \beta$, a group homomorphism $\phi_{\alpha \beta} : G_\alpha \to G_\beta$ such that for all $\alpha \leq \beta \leq \gamma$, $\phi_{\alpha \gamma} = \phi_{\beta \gamma} \phi_{\alpha \beta}$

\[ G_\alpha \xrightarrow{\phi_{\alpha \gamma}} G_\gamma \]
\[ \phi_{\alpha \beta} \quad \phi_{\beta \gamma} \]
\[ G_\beta \]

Definition 19.2 (Direct & Inverse Systems). The above data are said to be:

(i) An inverse system of groups if for any $\beta, \gamma \in A$, there is some $\alpha \in A$ with $\alpha \leq \beta, \alpha \leq \gamma$

(ii) A direct system of groups if for any $\beta, \gamma \in A$, there is some $\delta \in A$ with $\delta \geq \beta, \delta \geq \gamma$

Proposition-Definition 19.1 (Inverse Limit). Let $\{G_\alpha\}$ be an inverse system of groups as in Definition 19.2. Let $G = \{(g_\alpha) \in \prod_\alpha G_\alpha : \phi_{\alpha \beta}(g_\alpha) = g_\beta\}$. Then $G$ is a subgroup of $\prod_\alpha G_\alpha$ called the inverse limit of the inverse system $\{G_\alpha\}$ and denoted $\lim_{\alpha \in A} G_\alpha$. 
**Proposition 19.3.** Let \((G_\alpha, \phi_{\alpha\beta})\) be an inverse system of groups and \(G = \lim_{\alpha \in A} G_\alpha \leq \prod_\alpha G_\alpha\). Let \(\pi_\alpha : G \to G_\alpha\) be the natural projection \((g_\alpha) \mapsto g_\alpha\). Suppose \(H\) is a group and for each \(\alpha \in A\), we have a group homomorphism \(\psi_\alpha : H \to G_\alpha\) satisfying \(\psi_\beta = \phi_{\alpha\beta} \circ \psi_\alpha\) whenever \(\alpha \leq \beta\). Then there is a unique group homomorphism \(\psi\) such that \(\pi_\alpha \circ \psi = \psi_\alpha\) for all \(\alpha \in A\).

\[
\begin{array}{ccc}
H & \xrightarrow{\psi_\beta} & G_\beta \\
\downarrow{\psi_\alpha} & \nearrow{\phi_{\alpha\beta}} & \\
G_\alpha & \nearrow{\pi_\alpha} & G
\end{array}
\]

**Remark.** This is the universal property of inverse limits.

**Definition 19.3** (Pro-Finite Group). A pro-finite group \(G\) is a group that is isomorphic to an inverse limit of an inverse system \(\{G_\alpha\}\) of finite groups, i.e. all \(G_\alpha\) are finite.

**Lemma 19.1.** Let \(G = \lim_{\alpha \in A} G_\alpha \leq \prod_\alpha G_\alpha\) be a pro-finite group with \(G_\alpha\) finite.

1. \(G \leq \prod_\alpha G_\alpha\) is closed
2. \(G\) is compact
3. The open subgroups are the closed subgroups of finite index

## 20 Infinite Galois Extensions

**Lemma 20.1.** Let \(K/F\) be a Galois extension with Galois group \(G\). Let \(L\) be an intermediate field with \(L/F\) Galois too. Then the restriction map \(\rho : G = \text{Gal}(K/F) \to \text{Gal}(L/F); \sigma \mapsto \sigma|_L\) is a well defined group homomorphism with kernel \(L' = \text{Gal}(K/L)\). Also \(\rho\) is surjective.

**Notation.** \(K/F\) is a Galois field extension. We have the following setup for an inverse system of finite Galois groups.

1. \(A\) = set of subfields \(K_\alpha\) of \(K\) such that \(K_\alpha/F\) is finite Galois. Order \(A\) by inclusion. \(K/F\) is algebraic. This is a direct system. Why? Let \(L\) be the smallest field containing \(K_\beta, K_\gamma \in A\). Then \(L\) is finite being finitely generated by algebraic elements. And Galois closure of \(L\) is also finite over \(F\).

2. Apply the Galois correspondence with \(N_\alpha = \text{Gal}(K/K_\alpha)\). If \(N_\beta \subseteq N_\alpha\), there is a natural map \(\phi_{\alpha\beta} : G/N_\beta \to G/N_\alpha; gN_\beta \mapsto gN_\alpha\) or \(\text{Gal}(K_\beta/F) \to \text{Gal}(K_\alpha/F); \sigma \mapsto \sigma|_{K_\alpha}\). Note \(\text{Gal}(K_\alpha/F)\) is finite, so this is an inverse system of finite groups.
Theorem 20.1. Let $K/F$ be a Galois extension with Galois group $G$. Then $G \cong \varprojlim_{\alpha \in A} \text{Gal}(K_{\alpha}/F)$, where $K_{\alpha}$ is a subfield of $K$ such that $K_{\alpha}$ is finite Galois. In particular, $G$ is pro-finite.

Proposition-Definition 20.1 (Separable Closure). Let $F$ be a field and $F^{\text{sep}} = \text{set of elements in } F \text{ which are separable over } F$.

(i) $F^{\text{sep}}$ is a field

(ii) $F^{\text{sep}}/F$ is Galois. $F^{\text{sep}}$ is called the separable closure of $F$

Definition 20.1 (Absolute Galois Group). Let $F$ be a field. the absolute Galois group of $F$ is $\text{Gal}(F^{\text{sep}}/F)$.

Note. $\text{Gal}(F_{p}/F_{p}) = \text{Gal}(F_{p}^{\text{sep}}/F_{p}) = \hat{\mathbb{Z}}$ as we have a correspondence between $F_{p}^{m}/F_{p}$ and $\mathbb{Z}/m\mathbb{Z}$.

21 Infinite Galois Groups

Notation. Let $G = \varprojlim_{\alpha \in A} G_{\alpha}$ be a pro-finite group with all $G_{\alpha}$ finite. Let $\pi_{\alpha} : G \longrightarrow G$ be the natural projection map. Note $\{1_{G_{\alpha}}\} \leq G_{\alpha}$ is open. Thus $U_{\alpha} = \ker(\pi_{\alpha}) = \pi_{\alpha}^{-1}(1)$ is an open subgroup of $G$. It is often called the fundamental open neighbourhood of 1.

Proposition 21.1. With the above notation.

(i) The $U_{\alpha}$ form a basis of open neighbourhood of 1, i.e. if $U$ is an open neighborhood of 1 then $U \supseteq U_{\alpha}$ for some $\alpha$

(ii) For $\sigma \in G$, the $\{\sigma G_{\alpha}\}$ form a basis of open neighbourhoods

(iii) $G$ is Hausdorff, so in particular points are closed

Note. In topological spaces, $\{1\}$ closed implies Hausdorff.

Lemma 21.1. Let $K/F$ be a Galois extension with Galois group $G$. Let $L$ be a an intermediate field of $K/F$.

(i) Then $L' = \text{Gal}(K/L) \leq G$ is topologically closed

(ii) The subspace topology on $L'$ is the same as that coming from its structure as a pro-finite group, i.e. from $G$

Theorem 21.1. Let $K/F$ be a Galois extension. There are inverse bijections with Galois group $G$. \{topologically closed subgroups $H \leq G\} \longleftrightarrow \{\text{intermediate fields } L\}; \quad H \longleftrightarrow H' = K^{H}; \quad L \longleftrightarrow L' = \text{Gal}(K/L)$. 
22 Inseparability

Proposition 22.1. Let $K/F$ be a field extension where $\text{char}(F) = p > 0$.

(i) The following are equivalent

(a) $\alpha \in K$ is purely inseparable over $F$, i.e. $\alpha^{p^n} \in F$ for some $n \geq 0$
(b) $\alpha$ is the only root of its minimal polynomial $f(x) \in F[x]$
(c) $[F(\alpha) : F]_S = 1$

(ii) In particular if $\alpha \in K$ is both separable and purely inseparable over $F$ then $\alpha \in F$

Proposition-Definition 22.1 (Maximal Separable Sub-Extension). Let $F$ be a field of characteristic $p > 0$. Let $K/F$ be a field extension. The intermediate field $L = K \cap F^{\text{sep}}$ of all elements in $K$ which are separable over $F$ is such that $K/L$ is purely inseparable. $L$ is called the maximal separable sub-extension.

Proposition-Definition 22.2 (Maximal Purely Inseparable Sub-Extension). Let $K/F$ be a field extension. The set of elements in $K$ which are purely inseparable over $F$ forms a field called the maximal purely inseparable sub-extension.

Theorem 22.1. Let $F$ be a field of characteristic $p > 0$ and $K/F$ is a normal extension with Galois group $G = \text{Gal}(K/F)$. Let $L_{\text{sep}} = \text{maximal separable sub-extension}$ and $L_{\text{pi}} = \text{maximal purely inseparable sub-extension}$.

(i) $K/K^G$ is Galois with Galois group $G$

(ii) $L_{\text{pi}} = K^G$

(iii) $L_{\text{sep}}/F$ is Galois

(iv) $L_{\text{sep}} \cap L_{\text{pi}} = F$

(v) The smallest subfield containing $L_{\text{sep}}$ and $L_{\text{pi}}$ is $K$

(vi) The restriction map $\phi : \text{Gal}(K/L_{\text{pi}}) \longrightarrow \text{Gal}(L_{\text{sep}}/F)$ is a well defined group isomorphism

\[ \begin{array}{ccc}
K & \xmapsto{\phi} & L_{\text{sep}} \\
\xleftarrow{\text{separable}} & & \xleftarrow{\text{purely inseparable}} \\
L_{\text{pi}} & \xleftarrow{\text{purely inseparable}} & L_{\text{sep}} \\
\xleftarrow{\text{inseparable}} & & \xleftarrow{\text{separable}} \\
F & & 
\end{array} \]

Corollary 22.1. A field $F$ of characteristic $p \geq 0$ is perfect if Frobenius homomorphism $\phi : F \longrightarrow F$ is surjective, i.e. automorphism. Also fields of characteristic 0 are said to be perfect too. Any finite extension $K/F$ of a perfect field $F$ is separable.
23 Duality

Definition 23.1 (Torsion). Let $A$ be an abelian group and $m$ be a positive integer. An element $a \in A$ is $m$-torsion if $ma = 0$. We say $A$ is $m$-torsion if every element in $A$ is $m$-torsion. We say $A$ is torsion if every element of $A$ has finite order.

Proposition-Definition 23.1 (Set Of Group Homomorphisms). Let $G$ be a group and $A$ an abelian group. Let $\text{Hom}(G, A)$ be the set of group homomorphism $\phi : G \to A$. This is an abelian group when endowed with addition $(\phi_1 + \phi_2)(g) = \phi_1(g) + \phi_2(g)$, $g \in G$, $\phi_1, \phi_2 \in \text{Hom}(G, A)$ and $\phi_1(g), \phi_2(g) \in A$.

Definition 23.2 (Dual). Let $G$ be a torsion abelian group. Then the dual of $G$ is $G^\wedge = \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$.

Note. $A^\wedge \times B^\wedge = (A \times B)^\wedge$ with bijection $(\phi, \psi) \mapsto \rho$ where $\rho(a, b) = \phi(a) + \psi(b)$.

Definition 23.3 (Perfect Pairing). Let $A$, $B$ be torsion abelian groups. A pairing between $A$, $B$ is a function $\psi : A \times B \to \mathbb{Q}/\mathbb{Z}$ such that:

(i) $\psi(a, \cdot), \psi(\cdot, b)$ are group homomorphisms for all $a \in A$ and $b \in B$

(ii) if $\psi(a, \cdot) = 0 \implies a = 0$ and $\psi(\cdot, b) = 0 \implies b = 0$ then $\psi$ is said to be perfect

Proposition 23.1. Let $A$, $B$ be finite abelian groups and $\psi : A \times B \to \mathbb{Q}/\mathbb{Z}$ a perfect pairing between them. Then $A \cong B^\wedge$. In particular, the bijection is given by $a \mapsto \psi(a, \cdot)$.

Notation. Fix positive integer $m$. Let $F$ be a field of characteristic not dividing $m$ and such that $F \geq \mu_m$. Note that $|\mu_m| = m$. Kummer theory classifies abelian extensions of $F$ with $m$-torsion Galois groups. Here are some examples:

1. Let $F^{sm} = \{\alpha^m : \alpha \in F^*\}$. $F$ abelian $\implies F^{sm} \leq F^*$ and $F^*/F^{sm}$ is an $m$-torsion abelian group.

2. Let $a \in F^*/F^{sm}$, say $a = \alpha F^{sm}$. We define $\sqrt[m]{a}$ to be any $m$th root of $a$, i.e. $\sqrt[m]{\alpha F^{sm}}$. Note $\sqrt[m]{a}$ is well defined up to scalar multiple by some scalar $\beta \in F^*$. Why? Changing choices of $m$th root $\alpha$ changes $\sqrt[m]{\alpha}$ by an element of $\mu_m \subseteq F^*$. Changing $\alpha$ to $\alpha \beta^m$ where $\beta \in F^*$, i.e. changes $\sqrt[m]{\alpha}$ by $\beta$.

3. Let $J \leq F^*/F^{sm}$. Define $F(\sqrt[m]{J})$ to be the splitting field over $F$ of the family of polynomials $\{x^m - \alpha : \alpha F^{sm} \in J\}$. This is generated over $F$ by $\sqrt[m]{a}$, $a \in J$.

Proposition 23.2. For $J \leq F^*/F^{sm}$, $F(\sqrt[m]{J})/F$ is Galois.

Proposition 23.3. Let $J \leq F^*/F^{sm}$. Let $\sigma \in \text{Gal}(F(\sqrt[m]{J})/F)$, $a \in J$. Then $\psi(\sigma, a) = \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}} \in \mu_m$ and is independent of the choice of the $m$th root of $a$.

Proposition 23.4. For $J \leq F^*/F^{sm}$. $G = \text{Gal}(F(\sqrt[m]{J})/F)$ is a $m$-torsion abelian.
24  Kummer Theory

**Notation.** Fix positive integer $m$ and field of characteristic not dividing $m$ such that $F$ contains all $m$ mth root of unity. Let $J \leq F^*/F^{*m}$ and $G = \text{Gal}(F(\sqrt[m]{J})/F)$. We have a well defined map $\psi : G \times J \rightarrow \mu_m; (\sigma, a) \mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}$. Note also that $\mu_m \cong \mathbb{Z}/m\mathbb{Z} \cong \frac{1}{m}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$.

**Theorem 24.1.** The map $G \times J \xrightarrow{\psi} \mu_m \hookrightarrow \mathbb{Q}/\mathbb{Z}$ is a perfect pairing. If $J$ is finite then $\text{Gal}(F(\sqrt[m]{J})/F) \cong J^\wedge \cong J$.

**Theorem 24.2.** For positive integer $m$ and field of characteristic not dividing $m$ such that $F$ contains all $m$ mth root of unity, there is a bijection:

(i) \{subgroups $J \leq F^*/F^{*m}$\} $\longleftrightarrow$ \{abelian extensions of $F$ with m-torsion Galois group\} 

(considered up to isomorphisms of subfields of $F$); $J \longleftrightarrow F(\sqrt[m]{J})$

(ii) finite groups correspond to finite extensions