1. Algebraic Extensions

1.1. Finite and Algebraic Extensions.

**Definition 1.1.1.** Let $1_F$ be the multiplicative unity of the field $F$.

1. If $\sum_{i=1}^{n} 1_F \neq 0$ for any positive integer $n$, we say that $F$ has *characteristic* 0.
2. Otherwise, if $p$ is the smallest positive integer such that $\sum_{i=1}^{p} 1_F = 0$, then $F$ has *characteristic* $p$. (In this case, $p$ is necessarily prime.)
3. We denote the characteristic of the field by $\text{char}(F)$. 

(4) The prime field of $F$ is the smallest subfield of $F$. (Thus, if $\text{char}(F) = p > 0$, then the prime field of $F$ is $\mathbb{F}_p \triangleq \mathbb{Z}/p\mathbb{Z}$ (the field with $p$ elements) and if $\text{char}(F) = 0$, then the prime field of $F$ is $\mathbb{Q}$.)

(5) If $F$ and $K$ are fields with $F \subseteq K$, we say that $K$ is an extension of $F$ and we write $K/F$. $F$ is called the base field.

(6) The degree of $K/F$, denoted by $[K : F] \triangleq \dim_F K$, i.e., the dimension of $K$ as a vector space over $F$. We say that $K/F$ is a finite extension (resp., infinite extension) if the degree is finite (resp., infinite).

(7) $\alpha$ is algebraic over $F$ if there exists a polynomial $f \in F[X] - \{0\}$ such that $f(\alpha) = 0$.

**Definition 1.1.2.** If $F$ is a field, then

$$F(\alpha) \triangleq \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F[X] \text{ and } g(\alpha) \neq 0 \right\},$$

is the smallest extension of $F$ containing $\alpha$. (Hence $\alpha$ is algebraic over $F$ if, and only if, $F[\alpha] = F(\alpha)$.)

In the same way,

$$F(\alpha_1, \ldots, \alpha_n) \triangleq \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : f, g \in F[X_1, \ldots, X_n] \text{ and } g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

$$= F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$$

is the smallest extension of $F$ containing $\{\alpha_1, \ldots, \alpha_n\}$.

**Definition 1.1.3.** If $K/F$ is a finite extension and $K = F[\alpha]$, then $\alpha$ is called a primitive element of $K/F$.

**Proposition 1.1.4.** For any $f \in F[X] - \{0\}$ there exists an extension $K/F$ such that $f$ has a root in $K$. (E.g., $K \triangleq F[X]/(g)$, where $g$ is an irreducible factor of $f$.)

**Theorem 1.1.5.** If $p(X) \in F[X]$ is irreducible of degree $n$, $K \triangleq F[X]/(p(X))$ and $\theta$ is the class of $X$ in $K$, then $\theta$ is a root of $p(X)$ in $K$, $[K : F] = n$ and $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is an $F$-basis of $K$. 
Remark 1.1.6. Observe that $F[\theta]$ (polynomials over $F$ evaluated at $\theta$), where $\theta$ is a root of an irreducible polynomial $p(X)$, is then a field. Observe that $1/\theta$ can be obtained with the extended Euclidean algorithm: if $d(X)$ is the gcd($X, p(X)$) and $d(X) = a(X) \cdot X + b(X) \cdot p(X)$, the $1/\theta = a(\theta)$.

**Definition 1.1.7.** If $\alpha$ is algebraic over $F$, then there is a unique monic irreducible over $F$ that has $\alpha$ as a root, called the irreducible polynomial (or minimal polynomial) of $\alpha$ over $F$, and we shall denote it $\text{min}_{\alpha,F}(X)$. [Note: $(\text{min}_{\alpha,F}(X)) = \ker \phi$, where $\phi : F[X] \to F[\alpha]$ is the evaluation map.]

**Corollary 1.1.8.** If $\alpha$ is algebraic over $F$, then $F(\alpha) = F[\alpha] \cong F[x]/(\text{min}_{\alpha,F})$, and $[F[\alpha] : F] = \deg \text{min}_{\alpha,F}$.

**Proposition 1.1.9.** If $K$ is a finite extension of $F$ and $\alpha$ is algebraic over $K$, then $\alpha$ is algebraic over $F$ and $\text{min}_{\alpha,K}(X) \mid \text{min}_{\alpha,F}(X)$.

**Definition 1.1.10.** Let $\phi : R \to S$ be a ring homomorphism. If $f(X) = a_nX^n + \cdots + a_1X + a_0$, then $f^\phi \overset{\text{def}}{=} \phi(a_n)X^n + \cdots + \phi(a_1)X + \phi(a_0) \in S[X]$. [Note that $f \mapsto f^\phi$ is a ring homomorphism.]

**Theorem 1.1.11.** Let $\phi : F \to F'$ be an isomorphism, and $f \in F[X]$ be an irreducible polynomial. If $\alpha$ is a root of $f$ in some extension of $F$ and $\alpha'$ is a root of $f^\phi$ in some extension of $F'$, then there exists an isomorphism $\Phi : F[\alpha] \to F'[\alpha']$ such that $\Phi(\alpha) = \alpha'$ and $\Phi|_F = \phi$.

**Definition 1.1.12.** $K/F$ is an algebraic extension if every $\alpha \in K$ is algebraic over $F$.

**Proposition 1.1.13.** If $[K : F] < \infty$, then $K/F$ is algebraic.

Remark 1.1.14. The converse is false. E.g., $\bar{\mathbb{Q}} \overset{\text{def}}{=} \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$ is an infinite algebraic extension of $\mathbb{Q}$. 
Proposition 1.1.15. If $L$ is a finite extension $K$ and $K$ is a finite extension of $F$, then
\[ [L : F] = [L : K] \cdot [K : F]. \]
Moreover, if $\{\alpha_1, \ldots, \alpha_n\}$ is an $F$-basis of $K$ and $\{\beta_1, \ldots, \beta_m\}$ is a $K$-basis of $L$, then $\{\alpha_i \cdot \beta_j : i \in \{1, \ldots, n\} \text{ and } j \in \{1, \ldots, m\}\}$ is an $F$-basis of $L$.

Definition 1.1.16. $\{\alpha_1, \ldots, \alpha_n\}$ generates $K/F$ if $K = F(\alpha_1, \ldots, \alpha_n)$ and $K/F$ is finitely generated. (Not necessarily algebraic!)

Proposition 1.1.17. $[K : F] < \infty$ if, and only if, $K$ is finitely generated over $F$ by algebraic elements.

Corollary 1.1.18. Let $K/F$ be an arbitrary extension, then
\[ E \overset{\text{def}}{=} \{\alpha \in K : \alpha \text{ is a algebraic over } F\}, \]
is a subfield of $K$ containing $F$.

Definition 1.1.19. If $F$ and $K$ are fields contained in the field $\mathcal{F}$, then the composite (or compositum) of $F$ and $K$ is the smallest subfield of $\mathcal{F}$ containing $F$ and $K$, and is denoted by $FK$.

Proposition 1.1.20. (1) In general, we have:
\[ FK = \left\{ \frac{\alpha_1 \beta_1 + \cdots + \alpha_m \beta_m}{\gamma_1 \delta_1 + \cdots + \gamma_n \delta_n} : \alpha_i, \gamma_i \in F; \beta_j, \delta_j \in K; \gamma_1 \delta_1 + \cdots + \gamma_n \delta_n \neq 0 \right\} \]
(2) If $K_1/F$ and $K_2/F$ are finite extensions, with $K_1 = F[\alpha_1, \ldots, \alpha_m]$ and $K_2 = F[\beta_1, \ldots, \beta_n]$, then $K_1 K_2 = F[\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n]$, and $[K_1 K_2 : F] \leq [K_1 : F] \cdot [K_2 : F]$.

Definition 1.1.21. Let $\mathcal{C}$ be a class of field extensions. We say that $\mathcal{C}$ is distinguished if the following three conditions are satisfied:

(1) Let $F \subseteq K \subseteq L$. Then, $L/F$ is in $\mathcal{C}$ if, and only if, $L/K$ and $K/F$ are in $\mathcal{C}$. 
(2) If $K_1$ and $K_2$ are extensions of $F$, both contained in $\mathcal{F}$, then if $K_1/F$ is in $\mathcal{C}$, then $K_1 K_2/K_2$ is also in $\mathcal{C}$.

(3) If $K_1$ and $K_2$ are extensions of $F$, both contained in $\mathcal{F}$, then if $K_1/F$ and $K_2/F$ are in $\mathcal{C}$, then $K_1 K_2/F$ is also in $\mathcal{C}$. [Note that this follows from the previous two.]

**Definition 1.1.22.** Let $\mathcal{C}$ be a class of field extensions. We say that $\mathcal{C}$ is *quasi-distinguished* if the following three conditions are satisfied:

1. Let $F \subseteq K \subseteq L$. Then, if $L/F$ is in $\mathcal{C}$ then $L/K$ in $\mathcal{C}$.

2. Same as (2) of distinguished.

3. Same as (3) of distinguished.

**Remark 1.1.23.** The above definition is *not* standard.

**Proposition 1.1.24.** The classes of algebraic extensions and finite extensions are distinguished.

### 1.2. Algebraic Closure

**Definition 1.2.1.** Let $K$ and $L$ be extensions of $F$.

1. An *embedding* (i.e., an injective homomorphism) $\phi : K \to L$ is *over* $F$ if $\phi|_F = \text{id}_F$.

2. If $E/K$ and $\psi : E \to L$ is also an embedding, we say that $\psi$ is *over* $\phi$, or is an *extension* of $\phi$, if $\psi|_K = \phi$.

**Remark 1.2.2.** Remember that if $\phi : F \to F'$ is field homomorphism, then $\phi$ is either injective or $\phi \equiv 0$.

**Definition 1.2.3.** An *algebraic closure* of $F$ is an algebraic extension $K$ in which any polynomial in $F[X]$ splits [i.e., can be written as a product of linear factors] in $K[X]$. We say that $F$ is *algebraically closed* if it is an algebraic closure of itself.
Lemma 1.2.4. Let $K/F$ be algebraic. If $\phi : K \to K$ is an embedding over $F$, then $\phi$ is an automorphism.

Lemma 1.2.5. Let $F$ and $K$ be subfields of $F$ and $\phi : F \to L$ be an embedding into some field $L$. Then $\phi(FK) = \phi(F) \phi(K)$.

Theorem 1.2.6. (1) For any field $F$, there exists an algebraic closure of $F$.
(2) An algebraic closure of $F$ is algebraically closed.

Definition 1.2.7. If $f(X) = \sum_{i=0}^{n} a_i X^i \in F[X]$, then the formal derivative of $f$ is $f'(X) = \sum_{i=0}^{n} i a_i X^{i-1}$.

Remark 1.2.8. The same formulas from calculus still hold (product rule, chain rule, etc.).

Lemma 1.2.9. Let $f \in F[X]$ and $\alpha$ a root of $f$. Then $\alpha$ is a multiple root if, and only if, $f'(\alpha) = 0$.

Lemma 1.2.10. Let $\phi : F \to F'$ be an embedding, $c, a_1, \ldots, a_k \in F$, and $f \overset{\text{def}}{=} c(X - a_1) \cdots (X - a_k) \in F[X]$. Then, $f^\phi(X) = \phi(c)(X - \phi(a_1)) \cdots (X - \phi(a_k))$.

Theorem 1.2.11. Let $f \in F[X]$ be an irreducible polynomial. If $f$ splits in $K$ as $f = c(X - \alpha_1)^{n_1} \cdots (X - \alpha_k)^{n_k}$, with the $\alpha_i$’s distinct, then $n_1 = \cdots = n_k$. [So, $f$ is a $n_1$-th power of a polynomial with simple roots.] Moreover, if $K'$ is any other field where $f$ splits, and $n$ is the common exponent above [e.g, $n = n_1$], we must have $f = c(X - \alpha'_1)^n \cdots (X - \alpha'_k)^n$ in $K'[X]$. [I.e., the number of distinct roots $k$ and the exponent $n$ are the same.]
Corollary 1.2.12. If \( f \in F[x] \) is irreducible and \( \text{char}(F) = 0 \) [or \( f' \neq 0 \)], then \( f \) has only simple roots [in any extension of \( F \)].

Theorem 1.2.13. (1) If \( \phi : F \rightarrow K \) is an embedding of \( F \), \( K \) is algebraically closed and \( \alpha \) is algebraic over \( F \), then the number of extensions of \( \phi \) to \( F[\alpha] \) is equal to the number of distinct roots of \( \min_{\alpha,F}(X) \).

(2) If \( K/F \) is an algebraic extension, \( \phi : F \rightarrow L \), with \( L \) algebraically closed, then there exists an extension \( \psi : K \rightarrow L \) of \( \phi \). Moreover, if \( K \) is also algebraically closed and \( L/\phi(F) \) is algebraic, then \( \psi \) is an isomorphism. [Hence the algebraic closure of a field is unique up to isomorphism, and we denote the algebraic closure of \( F \) by \( \bar{F} \).]

(3) If \( K/F \) is an algebraic extension and \( \bar{K} \) is an algebraic closure of \( K \), then it is also an algebraic closure of \( F \). Conversely, if \( \bar{F} \) is an algebraic closure of \( F \) and \( K' \) is the image of the embedding of \( K \) into \( \bar{F} \), then \( \bar{F} \) is an algebraic closure of \( K' \).

1.3. Splitting Fields.

Definition 1.3.1. \( K \) is a splitting field of \( f \in F[X] \) if \( f(X) \) splits in \( K \), but not in any proper subfield of \( K \). In particular if \( f \) splits in an extension of \( F \) as \( f = c(X - \alpha_1) \cdots (X - \alpha_n) \), then \( F[\alpha_1, \ldots, \alpha_n] \) is a splitting field of \( f \).

Theorem 1.3.2. If \( K_1/F \) and \( K_2/F \) are two splitting fields of \( f \in F[X] \) [or of the same families of polynomials] in different algebraic closure [so that they are distinct], then there exists an isomorphism between \( K_1 \) and \( K_2 \) over \( F \) [induced by the isomorphism of the algebraic closures].

Remark 1.3.3. If \( \bar{F} \) is an algebraic closure of \( F \) and \( \alpha_1, \ldots, \alpha_n \in \bar{F} \) are all the roots of \( f(X) \), then the splitting field of \( F \) is \( F[\alpha_1, \ldots, \alpha_n] \).

Definition 1.3.4. \( K \) is normal extension of \( F \) if it is algebraic over \( F \) and any embedding \( \phi : K \rightarrow \bar{K} = \bar{F} \) over \( F \) is an automorphism of \( K \).
Theorem 1.3.5. Let $F \subseteq K \subseteq \overline{F}$. The following are equivalent:

1. $K$ is normal.
2. $K$ is a splitting field of a family of polynomials.
3. Every polynomials in $F[X]$ that has a root in $K$, splits in $K[X]$.

Theorem 1.3.6. The class of normal extensions is quasi-distinguished [but not distinguished]. Also, if $K_1/F$ and $K_2/F$ are normal, then so is $K_1 \cap K_2/F$.

Proposition 1.3.7. If $[K : F] = 2$, then $K/F$ is normal.

Remark 1.3.8. 
1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}(\sqrt{2})$ are normal extensions, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.
2. $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$, where $\zeta_3 = e^{2\pi i/3}$, is normal, and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\zeta_3, \sqrt[3]{2})$, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

1.4. Separable Extensions.

Lemma 1.4.1. Let $\sigma : F \to L$ and $\tau : F \to L'$ be embeddings of $F$ into algebraically closed fields, and let $K/F$ be an algebraic extension. Then, the number [or cardinality] of extensions of $\sigma$ to $K$ is the same as the number of extensions of $\tau$ to $K$.

Definition 1.4.2. 
1. Let $K/F$ be a finite extension and $\overline{F}$ be an algebraic closure of $F$. Then, the separable degree of $K/F$ is
$$[K : F]_s \overset{\text{def}}{=} \text{number of embeddings } \phi : K \to \overline{F} \text{ over } F.$$ 
2. A polynomial $f \in F[X]$ is a separable polynomial if it has no multiple roots.
3. Let $\alpha$ be algebraic over $F$. Then $\alpha$ is separable over $F$ if $\text{min}_{\alpha, F}(X)$ is separable.
4. $K/F$ is a separable extension if every element of $K$ is separable over $F$.

Remark 1.4.3. If $\phi : F \to L$ is embedding of $F$ and $L$ is algebraic closed, then
$$[K : F]_s = \text{number of extensions } \psi : K \to L \text{ of } \phi.$$
Theorem 1.4.4. If $L/K$ and $K/F$ are algebraic extensions, then

$$[L : F]_s = [L : K]_s \cdot [K : F]_s.$$  

Moreover, if $[L : F] < \infty$, then

$$[L : F]_s \leq [L : F],$$

and $K/F$ is separable if, and only if, $[L : F]_s = [L : F]$.

Theorem 1.4.5. If $K = F[\{\alpha_i : i \in I\}]$, where $I$ is a set of indices and $\alpha_i$ is separable over $F$ for all $i \in I$, then $K/F$ is separable.

Theorem 1.4.6. The class of separable extensions is distinguished.

Proposition 1.4.7. Let $K$ be a finite extension of $F$ inside $\bar{F}$. Then the smallest extension of $K$ which is normal over $F$ is $L \overset{\text{def}}{=} \phi_1(K)\ldots\phi_n(K)$, where $\{\phi_1, \ldots, \phi_n\}$ are all the embeddings of $K$ into $\bar{F}$ over $F$. (The $\phi_i(K)$'s are called the conjugates of $K$.) Moreover, if $K/F$ is separable, then $L$ is also separable over $F$.

Definition 1.4.8.  

(1) The field $L$ in the proposition above is called the normal closure of $K/F$.

(2) Let

$$F^s \overset{\text{def}}{=} \text{compositum of all separable extensions of } F.$$  

$F^s$ is called the separable closure of all $F$.

(3) If $K = F[\alpha]$, then $K$ is said to be a simple extension of $F$.

Theorem 1.4.9 (Primitive Element Theorem). If $[F : F] < \infty$, then $K/F$ has a primitive element if, and only if, there are finitely many intermediate fields (i.e., fields $L$ such that $F \subseteq L \subseteq K$). Moreover, if $K/F$ is (finite and) separable, then $K/F$ has a primitive element.

Lemma 1.4.10. If $f \in F[X]$ is irreducible, then $f$ has distinct roots if, and only if, $f'(X)$ is a non-zero polynomial.
Proposition 1.4.11.  

(1) $\alpha$ is separable over $F$ if, and only if, $(\min_{\alpha,F})' \neq 0$.

(2) If $\text{char}(F) = 0$, then any extension of $F$ is separable.

(3) Let $\text{char}(F) = p > 0$. Then $\alpha$ is inseparable over $F$ if, and only if, $\min_{\alpha,F} \in F[X^p]$. (And thus, $\min_{\alpha,F}$ is a $p$-power in $\bar{F}[X]$.)

1.5. Inseparable Extensions.

Definition 1.5.1. An algebraic extension $K/F$ is inseparable if it is not separable. (Note that if $K/F$ is inseparable, then $\text{char}(F) = p > 0$.)

Proposition 1.5.2. If $F[\alpha]/F$ is finite and inseparable, then $\min_{\alpha,F}(X) = f(X^{p^k})$, where $p = \text{char}(F)$ [necessarily positive], for some positive integer $k$ and separable and irreducible polynomial $f \in F[X]$. Moreover, $[F[\alpha] : F]_s = \deg f$, $[F[\alpha] : F] = p^k \cdot \deg f$, and $\alpha^{p^k}$ is separable over $F$.

Corollary 1.5.3. If $K/F$ is finite, then $[K : F]_s | [K : F]$. If $\text{char}(F) = 0$, then the quotient is 1, and if $\text{char}(F) = p > 0$, then the quotient is a power of $p$.

Definition 1.5.4. Let $K/F$ be a finite algebraic extension. The inseparable degree of $K/F$ is $[K : F]_i \overset{\text{def}}{=} \frac{[K : F]}{[K : F]_s}$.

Proposition 1.5.5. Let $K/F$ be a finite algebraic extension. Then:

(1) $K/F$ is separable if, and only if, $[K : F]_i = 1$;

(2) if $E$ is an intermediate field, then $[K : F]_i = [K : E]_i \cdot [E : F]_i$.

Definition 1.5.6.  

(1) Let $\alpha$ be algebraic over $F$, with $\text{char}(F) = p$. We say that $\alpha$ is purely inseparable over $F$ if $\alpha^{p^n} \in F$ for some positive integer $n$. [Thus, $\min_{\alpha,F} | X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}$.

(2) An algebraic [maybe infinite] extension $K/F$ is a purely inseparable extension if $[K : F]_s = 1$. 
Proposition 1.5.7. An element $\alpha$ is purely inseparable if, and only if, $\min_{\alpha,F}(x) = x^{p^n} - a$ for some positive integer $n$ and $a \in F$. [Observe that $a = \alpha^{p^n}$.]

Proposition 1.5.8. Let $K/F$ be an algebraic extension. The following are equivalent:

1. $K/F$ is purely inseparable [i.e., $[K:F]_s = 1$].
2. All elements of $K$ are purely inseparable over $F$.
3. $K = F[\alpha_i : i \in I]$, for some set of indices $I$, with $\alpha_i$ purely inseparable over $F$.

Proposition 1.5.9. The class of purely inseparable extensions is distinguished.

Definition 1.5.10. (1) Let $F$ be a field and $G$ be a subgroup of $\text{Aut}(F)$. Then:

$$F^G \overset{\text{def}}{=} \{ \alpha \in F : \phi(\alpha) = \alpha, \forall \phi \in G \},$$

is the fixed field of $G$. (Note: it is a field.)

(2) The extension $K/F$ is a Galois extension if it is normal and separable. In this case, the Galois group of $K/F$, denoted by $\text{Gal}(K/F)$ is the group of automorphisms of $K$ over $F$ [i.e., automorphisms of $K$ which fix $F$].

Remark 1.5.11. If $K/F$ is Galois, then $\text{Gal}(K/F)$ is equal to the set of embeddings of $K$ into $\bar{K}$. Also, if $K/F$ is finite, then $K/F$ is Galois if, and only if, $|\text{Aut}_F(K)| = [K:F]$, and so $|\text{Gal}(K/F)| = [K:F]$.

Remark 1.5.12. Note that for any field extension $K/F$ we have a group of automorphisms over $F$, which we denote by $\text{Aut}_F(K)$. But, usually, the notation $\text{Gal}(K/F)$ is reserved for Galois extensions only. [A few authors do use $\text{Gal}(K/F)$ for $\text{Aut}_F(K)$, though.]

Proposition 1.5.13. Let $K/F$ be an algebraic extension. Then

$$K' \overset{\text{def}}{=} \{ x \in K : x \text{ is separable over } F \}$$

is a field [equal to the compositum of all separable extensions of $F$ that are contained in $K$]. [So, it is clearly the maximal separable extension of $F$ contained in $K$.] Then, $K'/F$ is separable and $K/K'$ is purely inseparable.
Corollary 1.5.14. (1) $K/F$ is separable and purely inseparable, then $K = F$.
(2) If $\alpha$ is separable and purely inseparable over $F$, then $\alpha \in F$.

Corollary 1.5.15. If $K/F$ is normal, then the maximal separable extension of $F$ contained in $K$ [i.e., the $K'$ in the proposition above] is normal over $F$. [Hence, $K'/F$ is Galois.]

Corollary 1.5.16. If $F/E$ and $K/E$ are finite, with $F, K \subseteq F$, with $F/E$ separable and $K/E$ purely inseparable, then

$$[FK : K] = [F : E] = [FK : E],$$

$$[FK : F] = [K : E] = [FK : E].$$

Definition 1.5.17. Let $F$ be a field [or a ring] of characteristic $p$, with $p$ prime. The Frobenius morphism of $F$ is the map

$$\sigma : F \to F,$$

$$x \mapsto x^p.$$

Corollary 1.5.18. Let $K/F$ be a finite extension in characteristic $p > 0$ and $\sigma$ be the Frobenius.

(1) If $K^\sigma F = K$, then $K/F$ is separable, where

$$K^\sigma = \sigma(K) = \{\sigma(x) : x \in K\}.$$

(2) If $K/F$ is separable, then $K^{\sigma^n} F = K$ for any positive integer $n$.

Remark 1.5.19. (1) If $K = F[\alpha_1, \ldots, \alpha_m]$, then $K^{\sigma^n} F = F[\alpha_1^{p^n}, \ldots, \alpha_m^{p^n}]$.
(2) Notice that if $K/F$ is an algebraic extension, we can always have an intermediate field $K'$ such that $K'/F$ is separable and $K/K'$ is purely inseparable, but not always we can have a $K''$ such that $K''/F$ is purely inseparable and $K/K''$ is separable. [For example, take $F = \mathbb{F}_p(s,t)$, with $p > 2$, and $K = F[\alpha]$, where $\alpha$ is a root of $X^p - \beta$ and $\beta$ is a root of $X^2 - sX + t$.]

The next proposition states that if $K/F$ is normal, then there is such a $K''$. 
Proposition 1.5.20. Let $K/F$ be normal and $G \overset{\text{def}}{=} \text{Aut}_F(K)$ [where $\text{Aut}_F(K)$ is the set of automorphisms of $K$ over $F$] and $K^G$ be the fixed field of $G$ [as in Definition 1.5.10]. Then $K^G/F$ is purely inseparable and $K/K^G$ is separable. [Hence, $K/K^G$ is Galois.]

Moreover, if $K'$ is the maximal separable extension of $F$ contained in $K$, then $K = K' K^G$ and $K' \cap K^G = F$.

Definition 1.5.21. A field $F$ is a perfect field if either $\text{char}(F) = 0$ or $\text{char}(F) = p > 0$ and the Frobenius $\sigma : F \to F$ is onto [or equivalently, every element of $F$ has a $p$-th root]. [Note that $\sigma$ is always injective, so $\sigma$ is, in in this case, an automorphism of $F$.]

Proposition 1.5.22. Every algebraic extension of a perfect field $F$ is both perfect and separable over $F$.

1.6. Finite Fields.

Theorem 1.6.1. If $F$ is a field with $q$ [finite] elements, then:

1. $\text{char}(F) = p > 0$ and so $\mathbb{F}_p \subseteq F$;
2. $q = p^n$ for some positive integer $n$;
3. $F$ is the splitting field of $X^q - X$ (over $\mathbb{F}_p$);
4. any other field with $q$ elements is isomorphic to $F$, and in a fixed algebraic closure of $\mathbb{F}_p$, there exists only one field with $q$ elements, usually denoted by $\mathbb{F}_q$;
5. there exists $\xi \in F$, such that $F^\times = \langle \xi \rangle$;
6. for any positive integer $r$, there is a unique field with $p^r$ elements in a fixed algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$, which is the unique extension of $\mathbb{F}_p$ of degree $r$ in $\bar{\mathbb{F}}_p$.

Proposition 1.6.2. Any algebraic extension of a finite field Galois [i.e., it is both normal and separable].
Proposition 1.6.3. The set of automorphisms of $\mathbb{F}_{p^r}$ is $\{\text{id}, \sigma, \sigma^2, \ldots, \sigma^{r-1}\}$, where $\sigma$ is the Frobenius map. [Note that these are all automorphisms, and they are automorphisms over $\mathbb{F}_p$.]

Proposition 1.6.4. $\mathbb{F}_{p^s}$ is an extension of $\mathbb{F}_{p^r}$ if, and only if, $r \mid s$. In this case, the set of embeddings of $\mathbb{F}_{p^s}$ into $\overline{\mathbb{F}}_p$ over $\mathbb{F}_{p^r}$ [or equivalently, since normal, the set of automorphisms of $\mathbb{F}_{p^s}$ over $\mathbb{F}_{p^r}$] is $\{\text{id}, \sigma^r, \sigma^{2r}, \ldots, \sigma^{s-r}\}$, where $\sigma$ is the Frobenius map. [In other words, $\text{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_{p^r}) = \langle \sigma^r \rangle$.]

Proposition 1.6.5. The algebraic closure $\overline{\mathbb{F}}_p$ is $\bigcup_{r>0} \mathbb{F}_{p^r}$. [Note that any finite union is contained in a single finite field.]

2. Galois Theory

2.1. Galois Extensions.

Proposition 2.1.1. Galois extensions form a quasi-distinguished class, and if $K_1/F$ and $K_2/F$ are Galois, then so is $K_1 \cap K_2/F$.

Theorem 2.1.2. Let $K/F$ be a Galois extension and $G \overset{\text{def}}{=} \text{Gal}(K/F)$. Then

1. $K^G = F$;
2. if $E$ is an intermediate field ($F \subseteq E \subseteq K$), then $K/E$ is also Galois;
3. the map $E \mapsto \text{Gal}(K/E)$ is injective.

Corollary 2.1.3. Let $K/F$ be a Galois extension and $G \overset{\text{def}}{=} \text{Gal}(K/F)$. If $E_i$ is an intermediate field and $H_i \overset{\text{def}}{=} \text{Gal}(K/E_i)$, for $i = 1, 2$, then:

1. $H_1 \cap H_2 = \text{Gal}(K/E_1E_2)$;
2. if $H = \langle H_1, H_2 \rangle$ [i.e., $H$ is the smallest subgroup of $G$ containing $H_1$ and $H_2$], then $K^H = E_1 \cap E_2$.

Corollary 2.1.4. Let $K/F$ be separable and finite, and $L$ be the normal closure of $K/F$ [i.e., the smallest normal extension of $F$ containing $K$]. Then $L/F$ is finite and Galois.
Lemma 2.1.5. Let $K/F$ be a separable extension such that for all $\alpha \in K$, $[F[\alpha] : F] \leq n$, for some fixed $n$. Then $[K : F] \leq n$.

Theorem 2.1.6 (Artin). Let $K$ be a field, $G$ be a subgroup of $\text{Aut}(K)$ with $|G| = n < \infty$, and $F \overset{\text{def}}{=} K^G$. Then $K/F$ is Galois and $G = \text{Gal}(K/F)$ (and $[K : F] = n$).

Corollary 2.1.7. Let $K/F$ be Galois and finite and $G \overset{\text{def}}{=} \text{Gal}(K/F)$. Then, for any subgroup $H$ of $G$, $H = \text{Gal}(K/K^H)$.

Remark 2.1.8. The above corollary is not true if the extension is infinite! The map $H \mapsto K^H$ is not injective! For example, $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is Galois, the cyclic group $H$ generated by the Frobenius is not the Galois group, and yet $K^H = \overline{\mathbb{F}}_p$.

Lemma 2.1.9. Let $K_1$ and $K_2$ be two extensions of $F$ with $\phi : K_1 \to K_2$ an isomorphism over $F$. Then $\text{Aut}_F(K_2) = \phi \circ \text{Aut}_F(K_1) \circ \phi^{-1}$.

Theorem 2.1.10. Let $K/F$ be a Galois extension and $G \overset{\text{def}}{=} \text{Gal}(K/F)$. If $E$ is an intermediate extension, then $E/F$ is normal [and thus Galois] if, and only if, $H \overset{\text{def}}{=} \text{Gal}(K/E)$ is a normal subgroup of $G$. In this case, $\phi \mapsto \phi|_E$ induces an isomorphism between $G/H$ and $\text{Gal}(E/F)$.

Definition 2.1.11. An extension $K/F$ is an Abelian extension (resp., a cyclic extension) if it is Galois and $\text{Gal}(K/F)$ is Abelian (resp., cyclic).

Corollary 2.1.12. If $K/F$ is Abelian (resp., cyclic), then for any intermediate field $E$, $K/E$ and $E/F$ are Abelian (resp., cyclic).

Theorem 2.1.13 (Fundamental Theorem of Galois Theory). Let $K/F$ be finite and Galois, with $G \overset{\text{def}}{=} \text{Gal}(K/F)$. The results above gives: the map

$$
\{\text{subgroups of } G\} \longrightarrow \{\text{intermediate fields of } K/F\}
$$

$$
H \longmapsto K^H
$$
is a bijection with inverse

$$\{\text{intermediate fields of } K/F \} \longrightarrow \{\text{subgroups of } G\}$$

$$E \longmapsto \text{Gal}(K/E).$$

Moreover an intermediate field $E$ is Galois if, and only if, $H \overset{\text{def}}{=} \text{Gal}(K/E)$ is normal in $G$, and $\text{Gal}(E/F) \cong G/H$, induced by $\phi \mapsto \phi|_E$.

**Remark 2.1.14.** Note that the maps $H \mapsto K^H$ and $E \mapsto \text{Gal}(K/E)$ are inclusion reversing, i.e., $H_1 \leq H_2$ implies $K^{H_1} \supseteq K^{H_2}$, and if $E_1 \subseteq E_2$, then $\text{Gal}(K/E_1) \supseteq \text{Gal}(K/E_2)$.

**Theorem 2.1.15 (Natural Irrationalities).** Let $K/F$ be a Galois extension and $L/F$ be an arbitrary extension, with $K, L \subseteq \mathcal{F}$ [so that we can consider the compositum $LK$]. Then $LK$ is Galois over $L$ and $K$ is Galois over $K \cap L$. Moreover, if $G \overset{\text{def}}{=} \text{Gal}(K/F)$ and $H \overset{\text{def}}{=} \text{Gal}(KL/L)$, then for any $\phi \in H$, $\phi|_K \in G$ and $\phi \mapsto \phi|_K$ is an isomorphism between $H$ and $\text{Gal}(K/K \cap L)$.

**Corollary 2.1.16.** If $K/F$ is finite and Galois and $L/F$ is an arbitrary extension, then $[KL : L] \mid [K : F]$.

**Remark 2.1.17.** The above theorem does not hold for if $K/F$ is not Galois. For example, $F \overset{\text{def}}{=} \mathbb{Q}$, $K \overset{\text{def}}{=} \mathbb{Q}(\sqrt[3]{2})$ and $L \overset{\text{def}}{=} \mathbb{Q}(\zeta_3 \sqrt[3]{2})$, where $\zeta_3 = e^{2\pi i/3}$.

**Theorem 2.1.18.** Let $K_1/F$ and $K_2/F$ be Galois extensions with $K_1, K_2 \in \mathcal{F}$. Then $K_1K_2/F$ is Galois. Moreover, if $G \overset{\text{def}}{=} \text{Gal}(K_1K_2/F)$, $G_1 \overset{\text{def}}{=} \text{Gal}(K_1/F)$, $G_2 \overset{\text{def}}{=} \text{Gal}(K_2/F)$ and

$$\Phi : G \rightarrow G_1 \times G_2$$

$$\phi \mapsto (\phi|_{K_1}, \phi|_{K_2}),$$

then $\Phi$ is injective and if $K_1 \cap K_2 = F$, then $\Phi$ is an isomorphism.

**Corollary 2.1.19.** If $K_i/F$ is Galois and $G_i \overset{\text{def}}{=} \text{Gal}(K_i/F)$ for $i = 1, \ldots, n$ and $K_{i+1} \cap (K_1 \ldots K_i) = F$ for $i = 1, \ldots, (n-1)$, then $\text{Gal}(K_1 \ldots K_n/F) = G_1 \times \cdots \times G_n$. 
Corollary 2.1.20. Let $K/F$ be finite and Galois, with $G \overset{\text{def}}{=} \text{Gal}(K/F) = G_1 \times \cdots \times G_n$, $H_i \overset{\text{def}}{=} G_1 \times \cdots \times G_{i-1} \times 1 \times G_{i+1} \times \cdots \times G_n$ and $K_i \overset{\text{def}}{=} K^H_i$. Then $K_i/F$ is Galois with $\text{Gal}(K_i/F) \cong G_i$, $K_{i+1} \cap (K_1 \ldots K_i) = F$ and $K = K_1 \ldots K_n$.

Corollary 2.1.21. Abelian extensions are quasi-distinguished [see Definition 1.1.22]. Moreover, if $K$ is an Abelian extension of $F$ and $E$ is an intermediate field, then $E/F$ is also Abelian. [Hence, intersections of Abelian extensions are also Abelian.]

Remark 2.1.22. Observe that, as with Galois extensions [and Abelian extensions are Galois by definition], we do not always have that if $K/E$ and $E/F$ are Abelian, then $K/F$ is Abelian. For example, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are Abelian (since they are degree two extensions), but $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is not even Galois [since $X^4 - 2$ does not split in $\mathbb{Q}(\sqrt{2})$].

2.2. Examples and Applications.

Definition 2.2.1. The Galois group of a separable polynomial $f \in F[X]$ is the Galois group of the splitting field of $f$ over $F$. We will denote it by $G_f$ or $G_{f,F}$.

Proposition 2.2.2. (1) Let $f \in F[X]$ be a [not necessarily separable or irreducible] polynomial, $K$ be its splitting field, and $n$ be the number of distinct roots of $f$ [in $K$]. Then, $G \overset{\text{def}}{=} \text{Aut}_F(K)$ is a subgroup of the symmetric group $S_n$, seen as permutations of the roots of $f$. [In particular, any $\sigma \in G$ is determined by its values on the roots of $f$, and hence, if $\sigma \in G$ fixes all roots of $f$, then $\sigma = \text{id}_K$.]

(2) If $f \in F[X]$ is irreducible [but not necessarily separable] and $K$, $n$, and $G$ are as above, then $G$ is a transitive subgroup of $S_n$ [i.e., for all $i, j \in \{1, \ldots, n\}$, there is $\sigma \in G$ such that $\sigma(i) = j$].

(3) Let $K/F$ be Galois [and hence separable] with $G \overset{\text{def}}{=} \text{Gal}(K/F)$, $\alpha \in K$, $\mathcal{O} \overset{\text{def}}{=} \{\sigma(\alpha) : \sigma \in G\}$ be the orbit of $\alpha$ by the action of $G$ in $K$. Then, $\mathcal{O}$ is finite, say, $\mathcal{O} = \{\alpha_1, \ldots, \alpha_k\}$, and

$$\min_{\alpha, F} = (x - \alpha_1) \cdots (x - \alpha_k).$$

(4) Let $K/F$ be finite and Galois with $G \overset{\text{def}}{=} \text{Gal}(K/F)$, and let $\alpha \in K$. Then, $K = F[\alpha]$ if, and only if, the orbit of $\alpha$ by $G$ has exactly $[K : F]$ elements.

Proposition 2.2.3 (Quadratic Extensions).

(1) If $\text{char}(F) \neq 2$ and $[K : F] = 2$, then there exists an $a \in F$ such that $K = F[\alpha]$, with $\min_{\alpha,F} = X^2 - a$. Also, $\text{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z}$ and the non-identity element is such that $\phi(\alpha) = -\alpha$.

(2) If $f \in F[X]$ is a quadratic separable polynomial, then the splitting field of $F$ has degree two over $F$, $G_f \cong \mathbb{Z}/2\mathbb{Z}$ and the non-zero element of $G_f$ is takes a root of $f$ to the other root.

Definition 2.2.4. Let $f \in F[X]$, such that

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i).$$

Then the discriminant of $f$ is defined as

$$\Delta_f = \Delta \overset{\text{def}}{=} \prod_{i<j}(\alpha_i - \alpha_j)^2.$$ 

Proposition 2.2.5. For any $f \in F[X]$, $\Delta_f \in F$. In particular if $f = aX^2 + bX + c$, then $\Delta_f = b^2 - 4ac$ and if $f = X^3 + aX + b$, then $\Delta_f = -4a^3 - 27b^2$.

Proposition 2.2.6 (Cubic Extensions and Polynomials).

(1) If $[K : F] = 3$, then for any $\alpha \in K - F$, we have $K = F[\alpha]$.

(2) If $\text{char}(F) \neq 3$ and $f \in F[X]$ is irreducible of degree 3, say $f(X) = X^3 + aX^2 + bX + c$, then the splitting field of $f$ is the same as the splitting field of the polynomial $\tilde{f}(X) \overset{\text{def}}{=} f(X - a/3) = X^3 + \tilde{a}X + \tilde{b}$. [Hence $G_f = G_{\tilde{f}}$.]

(3) If the splitting field of a separable $f \in F[X]$ is of degree 3, then $G_f \cong \mathbb{Z}/3\mathbb{Z}$ and if $\alpha_1, \alpha_2, \alpha_3$ are the distinct roots of $f$, then $G_f = \langle \phi \rangle$, where $\phi(\alpha_1) = \alpha_2$ and $\phi(\alpha_2) = \alpha_3$ and $\phi(\alpha_3) = \alpha_1$. Note that in this case, $G_f \cong A_3$, where $A_n$ is the alternating subgroup of $S_n$ [i.e., the subgroup of even permutations].
(4) If the splitting field of a separable \( f \in F[X] \) is not of degree 3, then \( G_f \cong S_3 \) [and hence \( G_f \) can permute the roots of \( f \) in all possible ways].

(5) Let \( f = \prod_{i=1}^{3}(X - \alpha_i) \in F[X] \) and
\[
\delta \overset{\text{def}}{=} (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).
\]
[Thus, \( \delta^2 = \Delta_f \).] If \( f \) is irreducible in \( F[X] \), \( \Delta_f \neq 0 \) [i.e., \( f \) is separable] and \( \text{char}(F) \neq 2 \), then \( G_f \cong S_3 \) if, and only if, \( \delta \not\in F \) [or equivalently, \( \Delta_f \) is not a square in \( F \)]. [Note that if \( \delta \not\in F \), then \( F(\sqrt[n]{\delta})/F \) is a degree two extension contained in the splitting field of \( f \).]

**Examples 2.2.7.** From the above, we can deduce:

(1) If \( f \overset{\text{def}}{=} X^3 - X + 1 \in \mathbb{Q}[X] \), then \( \Delta_f = -23 \), and hence \( G_f = S_3 \).

(2) If \( f \overset{\text{def}}{=} X^3 - 3X + 1 \in \mathbb{Q}[X] \), then \( \Delta_f = 81 \), and hence \( G_f = \mathbb{Z}/3\mathbb{Z} \).

**Example 2.2.8.** If \( f = X^4 - 2 \in \mathbb{Q}[X] \), then \( G_f \cong D_8 \), the dihedral group of 8 elements. More precisely, if \( \phi \in \text{Gal}(\mathbb{Q}[\sqrt[4]{2}, i]/\mathbb{Q}[i]) \) such that \( \phi(\sqrt[4]{2}) = \sqrt[4]{2}i \) and \( \psi \in \text{Gal}(\mathbb{Q}[\sqrt[4]{2}, i]/\mathbb{Q}[\sqrt[4]{2}]) \) such that \( \psi(i) = -i \) [i.e., \( \psi \) is the complex conjugation], then
\[
G_f = \langle \phi, \psi : \phi^4 = \text{id}, \psi^2 = \text{id}, \psi \circ \phi = \phi^3 \circ \psi \rangle
= \{ \text{id}, \phi, \phi^2, \phi^3, \psi, \phi \circ \psi, \phi^2 \circ \psi, \phi^3 \circ \psi \}.
\]

**Proposition 2.2.9.** Let \( E \) be a field, \( t_1, \ldots, t_n \) be algebraically independent variables over \( E \), \( s_1, \ldots, s_n \) be their elementary symmetric functions, \( F \overset{\text{def}}{=} E(s_1, \ldots, s_n) \) and \( K \overset{\text{def}}{=} E(t_1, \ldots, t_n) \). Then \( \min_{t_i,F} = \prod_{i=1}^{n}(X - t_i) \) and \( \text{Gal}(K/F) \cong S_n \).

**Theorem 2.2.10** (Fundamental Theorem of Algebra). \( \mathbb{C} \) is the algebraic closure of \( \mathbb{R} \).

**Lemma 2.2.11.** If \( G \subseteq S_p \), with \( p \) prime, and \( G \) contains a transposition and a \( p \)-cycle, then \( G = S_p \).
Proposition 2.2.12. If $f \in \mathbb{Q}[X]$ is irreducible, $\deg f = p$, with $p$ prime, and if $f$ has exactly two complex roots, then $G_f \cong S_p$.

Example 2.2.13. As an application of the proposition above, let $f \overset{\text{def}}{=} X^5 - 4X + 2 \in \mathbb{Q}[X]$. Then $G_f \cong S_5$. In fact, one can use the above proposition to prove that for every prime $p$ there is a polynomial $f_p \in \mathbb{Q}[X]$ such that $G_{f_p, \mathbb{Q}} = S_p$. [One can get all $S_n$, in fact, but it is harder.]

Theorem 2.2.14. Let $f \in \mathbb{Z}[X]$ be a monic separable polynomial, $p$ be a prime that does not divide the discriminant of $f$, and $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ be the reduction modulo $p$ of $f$ [i.e., obtained by reducing the coefficients]. Then, there is a bijection between the roots of $f$ and the roots of $\bar{f}$, denoted by $\alpha \mapsto \bar{\alpha}$, and an injection $i : G_f \to G_{\bar{f}}$, such that, if $\phi \in G_f$ and $\bar{\alpha}_i$ and $\bar{\alpha}_j$ are roots of $\bar{f}$, with $\phi(\bar{\alpha}_i) = \bar{\alpha}_j$, then $i(\phi)(\alpha_i) = \alpha_j$.

In particular, if $\phi \in G_f$, then $G_f$ has an element [namely $i(\phi)$] that has the same cycle structure [seen as a permutation] as $\phi$ itself. [E.g., if $\phi$ as a permutation is a product of a two-cycle, a 4-cycle and a 7-cycle [all disjoint], then $i(\phi)$ is also a product of a two-cycle, a 4-cycle and a 7-cycle [all disjoint] in $G_f$.]

Example 2.2.15. As an application of the theorem above, one can prove that $f \overset{\text{def}}{=} X^5 - X - 1 \in \mathbb{Z}[X]$ is such that $G_f = S_5$, by reducing $f$ modulo 5 and modulo 2.

2.3. Roots of Unity.

Definition 2.3.1.

(1) A $n$-th root of unity in a field $F$ is a root of $X^n - 1$ in $F$. A root of unity [with no $n$ specified] is a root of unit for some $n$.

(2) The set of all roots of unity form an Abelian group, denoted by $\mu(F)$ or simply $\mu$.

(3) The set of $n$-th roots of unity in $F$ is a cyclic group denoted by $\mu_n(F)$ or simply $\mu_n$.

(4) If $\operatorname{char}(F) \nmid n$, then $|\mu_n| = n$ and a generator of $\mu_n$ is called a primitive $n$-th root of unity.
Proposition 2.3.2. (1) If \( \text{char}(F) = p > 0, n = p^r m, \) and \( p \nmid m \), then \( \mu_n(F) = \mu_m(F) \) [and so \( |\mu_n(F)| = m \)].

(2) If \( \gcd(n, m) = 1 \), then \( \mu_n \times \mu_m \cong \mu_{nm} \) and the isomorphism is given by \( (\zeta, \zeta') \mapsto \zeta \zeta' \). [In particular, if \( \zeta_n \) and \( \zeta_m \) are primitive \( n \)-th and \( m \)-th roots of unity, then \( \zeta_n \zeta_m \) is a primitive \( nm \)-th root of unity.]

Proposition 2.3.3. Let \( F \) be a field such that \( \text{char}(F) \nmid n \), and \( \zeta_n \) a primitive \( n \)-th root of unity. Then \( F[\zeta_n]/F \) is Galois. If \( \phi \in \text{Gal}(F[\zeta_n]/F) \), then \( \phi(\zeta_n) = \zeta_n^{i(\phi)} \), for some \( i(\phi) \in (\mathbb{Z}/n\mathbb{Z})^\times \) and this map \( \iota : \text{Gal}(F[\zeta_n]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times \) is injective. Thus, \( \text{Gal}(F[\zeta_n]/F) \) is Abelian.

Remark 2.3.4. Note that \( \text{Gal}(F[\zeta_n]/F) \) is not necessarily cyclic. For example, \( \text{Gal}(\mathbb{Q}[\zeta_8]/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \).

Definition 2.3.5. We say that \( K/F \) is a cyclotomic extension if there exists a root of unity \( \zeta \) over \( F \) such that \( K = F[\zeta] \). [Careful: in Lang, an extension is cyclotomic if there exists a root of unity \( \zeta \) over \( F \) such that \( K \subseteq F[\zeta] \!).]

Definition 2.3.6. Let \( \varphi : \mathbb{Z} \to \mathbb{Z} \) denote the Euler phi-function, which is defined as
\[
\varphi(n) \overset{\text{def}}{=} |\{ m \in \mathbb{Z} : 0 < m < n \text{ and } \gcd(m, n) = 1 \}|.
\]

Theorem 2.3.7. If \( \zeta_n \) is a primitive \( n \)-th root of unity in \( \mathbb{Q} \), then \( [\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n) \) and the map \( \iota : \text{Gal}(F[\zeta_n]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times \) [as in Proposition 2.3.3] is an isomorphism.

Corollary 2.3.8. If \( \zeta_m \) and \( \zeta_n \) are a primitive \( m \)-th root of unity and primitive \( n \)-th root of unity, respectively, with \( \gcd(m, n) = 1 \), then \( \mathbb{Q}[\zeta_m] \cap \mathbb{Q}[\zeta_n] = \mathbb{Q} \),

Remark 2.3.9. If \( m = \text{lcm}(n_1, \ldots, n_r) \), and \( \zeta_{n_i} \) is a primitive \( n_i \)-th root of unity for \( i = 1, \ldots, r \), then \( \mathbb{Q}[\zeta_{n_1}] \cdots \mathbb{Q}[\zeta_{n_r}] = \mathbb{Q}[\zeta_m] \).
Definition 2.3.10. Let $n$ be a positive integer not divisible by $\text{char}(F)$. The polynomial
\[
\Phi_n(X) \overset{\text{def}}{=} \prod_{\zeta \text{ prim. } n\text{-th root of 1 in } F} (X - \zeta)
\]
is called the $n$-th cyclotomic polynomial [over $F$].

Proposition 2.3.11.

(1) $\deg \Phi_n = \varphi(n)$.

(2) If $\zeta_n$ is a primitive $n$-th root of unity, then $\Phi_n(X) = \min_{\zeta_n, \mathbb{Q}}(X)$.

(3) If $\zeta_n$ is a primitive $n$-th root of unity, then
\[
\Phi_n(X) = \prod_{\phi \in \text{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})} (X - \phi(\zeta_n))
\]

(4) $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

(5) If $\text{char}(F) = 0$, then $\Phi_n \in \mathbb{Z}[X]$ for all $n$. If $\text{char}(F) = p > 0$, then $\Phi_n \in \mathbb{F}_p[X]$ for all $n$ [not divisible by $p$].

Proposition 2.3.12.

(1) If $p$ is prime, then $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

(2) If $p$ is prime, then $\Phi_p(X) = \Phi_p(X^{p-1})$.

(3) If $n = p_1^{r_1} \cdots p_s^{r_s}$, with $p_i$’s distinct primes, then $\Phi_n(X) = \Phi_{p_1^{r_1-1}} \cdots p_s^{r_s-1}$

(4) If $n > 1$ is odd, then $\Phi_{2n}(X) = \Phi_n(-X)$.

(5) If $p \nmid n$, with $p$ an odd prime, then $\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$.

(6) If $p \mid n$, with $p$ prime, then $\Phi_{pn}(X) = \Phi_n(X^p)$.

Remark 2.3.13. It is not true that for all $n$, the coefficients of $\Phi_n(X)$ are either 0, 1 or $-1$. The first $n$ for which this fails is $105 = 3 \cdot 5 \cdot 7$.

Theorem 2.3.14 (Dirichlet’s Theorem of Primes in Arithmetic Progression). If $\gcd(a, r) = 1$, there are infinitely many primes in the arithmetic progression
\[
a, a + r, a + 2r, a + 3r, \ldots
\]
Theorem 2.3.15. Given a finite Abelian group $G$, there exists an extension $F/\mathbb{Q}$ such that $\text{Gal}(F/\mathbb{Q}) = G$.

Theorem 2.3.16 (Kronecker-Weber). If $F/\mathbb{Q}$ is finite and Abelian, then there exists a cyclotomic extension $\mathbb{Q}[\zeta]/\mathbb{Q}$ such that $F \subseteq \mathbb{Q}[\zeta]$.

2.4. Linear Independence of Characters.

Definition 2.4.1. Let $G$ be a monoid [i.e., a “group” which might not have inverses] and $F$ be a field. A character of $G$ in $F$ is a homomorphism $\chi : G \to F^\times$. The trivial character is the map constant equal to 1.

Let $f_i : G \to F$ for $i = 1, \ldots, n$. We say that the $f_i$'s are linearly independent if

$$\alpha_1 f_1 + \ldots + \alpha_n f_n = 0, \quad \alpha_i \in F,$$

then $\alpha_i = 0$ for all $i$.

Remarks 2.4.2. (1) If $K/F$ is a field extension and $\{\phi_1, \ldots, \phi_n\}$ are the embedding of $K$ over $F$, then we can think of $\phi_i|_{K^\times}$ as characters of $K^\times$ in $K$.

(2) If one says only a character in $G$ (without mention of the field), one usually means a character from $G$ in $\mathbb{C}^\times$ or even in

$$S^1 \overset{\text{def}}{=} \{\zeta \in \mathbb{C} : |\zeta| = 1\}.$$

Theorem 2.4.3 (Artin). If $\chi_1, \ldots, \chi_n$ distinct characters of $G$ in $F$, then they are linearly independent.

Corollary 2.4.4. Let $\alpha_1, \ldots, \alpha_n$ be distinct elements of a field $F^\times$. If $a_1, \ldots, a_n \in F$ such that for all positive integer $r$ we have

$$a_1 \alpha_1^r + \cdots + a_n \alpha_n^r = 0,$$

then $a_i = 0$ for all $i$.

Corollary 2.4.5. For any extension $K/F$, the set $\text{Emb}_{K/F}$ is linearly independent over $K$. 
2.5. Norm and Trace.

**Definition 2.5.1.** Let $K/F$ be a finite extension, with $[K : F]_s = r$ and $[K : F]_i = p^\mu$.

[So, char($F$) = $p$ or $[K : F]_i = 1$.] Let $\text{Emb}_{K/F} = \{\phi_1, \ldots, \phi_n\}$ and $\alpha \in K$:

1. The norm of $\alpha$ from $K$ to $F$ is

$$N_{K/F}(\alpha) \overset{\text{def}}{=} \prod_{i=1}^{n} \phi_i(\alpha^{p^\mu}) = \left( \prod_{i=1}^{n} \phi_i(\alpha) \right)^{[K:F]_i}.$$ 

2. The trace of $\alpha$ from $K$ to $F$ is

$$\text{Tr}_{K/F}(\alpha) \overset{\text{def}}{=} [K : F]_i \cdot \sum_{i=1}^{n} \phi_i(\alpha).$$

**Remark 2.5.2.** Note that if $K/F$ is inseparable, then $\text{Tr}_{K/F}(\alpha) = 0$.

**Lemma 2.5.3.**

1. Let $K/F$ be a finite extension, and $\text{Emb}_{K/F} = \{\phi_1, \ldots, \phi_n\}$ be the set of embeddings of $K$ over $F$. If $L/K$ is an algebraic extension and $\psi : L \to \bar{F}$ is an embedding over $F$, then

$$\{\psi \circ \phi_1, \ldots, \psi \circ \phi_n\} = \text{Emb}_{K/F}.$$ 

2. Let $F \subseteq K \subseteq L$ be field extensions. Let

$$\text{Emb}_{K/F} = \{\phi_1, \ldots, \phi_r\},$$

and

$$\text{Emb}_{L/K} = \{\psi_1, \ldots, \psi_s\}.$$ 

If $\bar{\phi}_i : \bar{F} \to \bar{F}$ is an extension of $\phi_i$ to $\bar{F}$ (which exists since $\bar{F}/F$ is algebraic), then

$$\text{Emb}_{L/F} = \{\bar{\phi}_i \circ \psi_j : i \in \{1, \ldots, r\} \text{ and } j \in \{1, \ldots, s\}\}.$$ 

3. Let $K/F$ be a separable extension. If $\alpha \in K$ is such that $\phi(\alpha) = \alpha$ for all embeddings $\phi \in \text{Emb}_{K/F}$, then $\alpha \in F$.

**Theorem 2.5.4.** Let $L/F$ be a finite extension.

1. For all $\alpha \in K$, $N_{K/F}(\alpha), \text{Tr}_{K/F}(\alpha) \in F$. 

(2) If \([K : F] = n\) and \(\alpha \in F\), then \(N_{K/F}(\alpha) = \alpha^n\) and \(\text{Tr}_{K/F}(\alpha) = n \cdot \alpha\).

(3) \(N_{K/F}|_{K^\times} : K^\times \to F^\times\) is a [multiplicative] group homomorphism and \(\text{Tr}_{K/F} : K \to F\) is an [additive] group homomorphism.

(4) If \(K\) is an intermediate field, then
\[
N_{L/F} = N_{K/F} \circ N_{L/K},
\]
\[
\text{Tr}_{L/F} = N_{K/F} \circ \text{Tr}_{L/K}.
\]

(5) If \(L = F(\alpha)\), where \(\min_{\alpha,F}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0\), then
\[
N_{L/F}(\alpha) = (-1)^n a_0, \quad \text{Tr}_{L/F}(\alpha) = -a_{n-1}.
\]

**Corollary 2.5.5.** If \(F \subseteq F(\alpha) \subseteq K\), with \([K : F] = n\), \(\min_{\alpha,F}(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0\), and \([L : F(\alpha)] = e\), then
\[
N_{L/F}(\alpha) = (-1)^n a_0^e, \quad \text{Tr}_{L/F}(\alpha) = (-a_{d-1})^e.
\]

**Remark 2.5.6.** \(\text{Tr}_{K/F} : K \to F\) is an \(F\)-linear map.

### 2.6. Cyclic Extensions.

**Theorem 2.6.1** (Hilbert’s Theorem 90 – multiplicative form). Let \(K/F\) be a cyclic extension of degree \(n\) and \(\text{Gal}(K/F) = \langle \sigma \rangle\). Then, \(\beta \in K\) is such that \(N_{K/F}(\beta) = 1\) if, and only if, there exists \(\alpha \in K^\times\) such that \(\beta = \alpha/\sigma(\alpha)\).

**Theorem 2.6.2.** Let \(F\) be a field such that \(F\) contains a primitive \(n\)-th root of unity for some fixed \(n\) not divisible by \(\text{char}(F)\).

1. If \(K/F\) is cyclic of degree \(n\), then \(K = F[\alpha]\) where \(\alpha\) is a root of \(X^n - a\), for some \(a \in F\). [In particular, \(\min_{\alpha,F} = X^n - a\).]

2. Conversely, if \(a \in F\) and \(\alpha\) is a root of \(X^n - a\), then \(F[\alpha]/F\) is cyclic, its degree, say \(d\), is a divisor of \(n\), and \(\alpha^d \in F\).

**Remark 2.6.3.** Note that, by linear independence of characters, if \(K/F\) is separable, then \(\text{Tr}_{K/F}\) is not constant equal to zero.
Theorem 2.6.4 (Hilbert’s Theorem 90 – additive form). Let $K/F$ be a cyclic extension of degree $n$ and $\text{Gal}(K/F) = \langle \sigma \rangle$. Then, $\beta \in K$ is such that $\text{Tr}_{K/F}(\beta) = 0$ if, and only if, there exists $\alpha \in K^\times$ such that $\beta = \alpha - \sigma(\alpha)$.

Theorem 2.6.5 (Artin-Schreier). Let $F$ be a field of characteristic $p > 0$.

1. If $K/F$ is cyclic of degree $p$, then $K = F[\alpha]$ where $\alpha$ is a root of $X^p - X - a$, for some $a \in F$. [In particular, $\text{min}_{\alpha,F}(X^p - X - a)$.

2. Conversely, if $a \in F$ and $f \overset{\text{def}}{=} X^p - X - a$, then either $f$ splits completely in $F$ or is irreducible over $F$. In the latter case, if $\alpha$ is a root of $f$, then $F[\alpha]/F$ is cyclic of degree $p$.

2.7. Solvable and Radical Extensions.

Definition 2.7.1. A finite extension $K/F$ is a solvable extension if it is separable and the normal closure $L$ of $K/F$ [which is then finite Galois over $F$] is such that $\text{Gal}(L/F)$ is a solvable group.

Remark 2.7.2. Note that for a finite separable extension $K/F$ to be solvable, it suffices that there exists some finite Galois extension of $F$ containing $K$ with its Galois group solvable.

Proposition 2.7.3. The class of solvable extensions is distinguished.

Definition 2.7.4. (1) A finite extension $K/F$ is a repeated radical extension if there is a tower:

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = K,$$

such that $F_i = F_{i-1}[\alpha_i]$, where $\alpha_i$ is either a root of a polynomial $X^n - a$, for some $a \in F_{i-1}$ and with $\text{char}(F) \nmid n$, or a root of $X^p - X - a$, for some $a \in F_{i-1}$, where $p = \text{char}(F)$. [Note that $\alpha_i$ might then be a root of unity.]

(2) A finite extension $K/F$ is a radical extension if there is $L \supseteq K$ such that $L/F$ is repeated radical.
Remark 2.7.5. Note that, by definition, if $K$ is the splitting field of a separable polynomial $f \in F[X]$, then the roots of $f$ are given by radicals [i.e., $f$ is solvable by radicals] if, and only if, $K$ is radical.

**Proposition 2.7.6.** The class of radical extensions is distinguished.

**Theorem 2.7.7.** Let $K/F$ be separable. Then, $K/F$ is solvable if, and only if, it is radical.

Remark 2.7.8. This allows us to determine when a polynomial can be solved by radicals simply by looking at its Galois group!

**Theorem 2.7.9.** For $n = 2, 3, 4$ [and $\text{char}(F) \neq 2, 3$] there are formulas for solving [general] polynomial equations of degree $n$ by means of radicals. For $n \geq 5$, there aren’t.

**Theorem 2.7.10.** Suppose that $f \in \mathbb{Q}[X]$ is irreducible and splits completely in $\mathbb{R}$. If any root of $f$ lies in a real repeated radical extension of $\mathbb{Q}$, then $\deg f = 2^r$ for some non-negative integer $r$.

Remark 2.7.11. Note that the above theorem tells us that we cannot replace radical by repeated radical in trying to express all roots of a polynomials in terms of radicals. For example, the polynomial $f = X^3 - 4X + 2$ splits completely in $\mathbb{R}$ and is solvable. So, we can write its roots in terms of radicals [since its radical], but we must have complex numbers to write them in terms of radicals [since is not repeated radical by the theorem above]. More precisely, if

$$\alpha \overset{\text{def}}{=} \sqrt[3]{\frac{111}{9}} - 1, \quad \text{and} \quad \zeta_3 \overset{\text{def}}{=} \frac{\sqrt{3}}{2} - \frac{1}{2},$$

then the [all real] roots of $f$ are

$$\alpha + \frac{4}{3\alpha}, \quad \alpha \zeta_3 + \frac{4}{3\alpha \zeta_3}, \quad \alpha \zeta_3^2 + \frac{4}{3\alpha \zeta_3^2}.$$  

[We cannot rewrite the above roots only using radicals of real numbers!]
Abelian extension, 15
algebraic, 2
algebraic closure, 5
algebraic extension, 3
algebraically closed, 5
Artin-Schreier Theorem, 26

base field, 2

character, 23
characteristic 0, 1
characteristic p, 1
composite, 4
compositum, 4
conjugates, 9
cyclic extension, 15
cyclotomic extension, 21
cyclotomic polynomial, 22
degree, 2
Dirichlet’s Theorem of Primes in Arithmetic Progression, 22
discriminant, 18
distinguished, 4
embedding, 5
Euler phi-function, 21
extension, 2, 5

finite extension, 2
finitely generated, 4
fixed field, 11
formal derivative, 6
Frobenius morphism, 12
Fundamental Theorem of Algebra, 19
Fundamental Theorem of Galois Theory, 15

Galois extension, 11
Galois group, 11
Galois group of a separable polynomial, 17
generates, 4

Hilbert’s Theorem 90 – additive form, 26
Hilbert’s Theorem 90 – multiplicative form, 25

infinite extension, 2
inseparable, 10
intermediate fields, 9
irreducible polynomial, 3

Kronecker-Weber Theorem, 23

linearly independent, 23

minimal polynomial, 3
monoid, 23

Natural Irrationalities, 16

norm, 24
normal closure, 9
normal extension, 7

orbit, 17
over, 5

perfect field, 13
prime field, 2
primitive n-th root of unity, 20
primitive element, 2
Primitive Element Theorem, 9
purely inseparable, 10
purely inseparable extension, 10

quasi-distinguished, 5

radical extension, 26
repeated radical extension, 26
root of unity, 20