Chapter - 4 : Field Theory

Definition .71 *A field is a commutative division ring.*

In the context of a field F, a non-empty subset $S \subseteq F$ is considered a subfield if it is itself a field.

Definition .72 *A field F is classified as a prime field if it has no proper subfields.*

Example 1.19.2 *1. $\mathbb{Z}_p$ is a prime field for a prime number p. Here, $\mathbb{Z}_p \cong \frac{\mathbb{Z}}{<p>}$.*

2. Additionally, $\mathbb{Q}$ qualifies as a prime field.

Proposition .37 *Every prime field is either isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_q$ for some prime q.*

To elaborate, we define a (non-zero map) function $f : \mathbb{Z} \to P$, representing the given field, as

$$n \mapsto ne \ (e + e + \cdots n \ times),$$

where e is the unity of P. f is a homomorphism, and so the kernel of f is an ideal of $\mathbb{Z}$ (which is a PID), making $\ker f$ a principal ideal of $\mathbb{Z}$. Let $\ker f =< q >$ and so $\frac{\mathbb{Z}}{Kerf} \cong f(\mathbb{Z}) \subseteq P$.

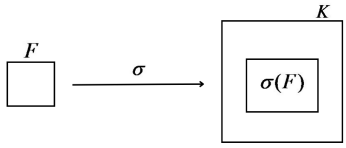
1. If $q = 0$, then $\mathbb{Z} \cong f(\mathbb{Z}) \subseteq P$ and P is with infinite characteristic. If $\mathbb{Q}'$ is a field of quotients of $f(\mathbb{Z})$, then $\mathbb{Q}' \subseteq P$, where P is a prime field. This implies $P = \mathbb{Q}'$. Furthermore, the field of quotients of $\mathbb{Z}$ is $\mathbb{Q}$, resulting in $\mathbb{Q} \cong \mathbb{Q}'$, and thus, $P = \mathbb{Q}'$ implies that P is isomorphic to $\mathbb{Q}$.

2. If $q \neq 0$ (since q cannot be 1, otherwise f is the zero map), we assert that q is prime. Assuming $q = ab$ (which implies that both a and b divide q), then $qe = q = (ae)(be) = 0$ (since $q \in Ker(f)$). This gives us $ae = 0$ or $be = 0$, i.e., $a \in Ker(f)$ or $b \in Ker(f)$, which leads to q dividing a or q dividing b leading to a contradiction ($q = a$ or $q = b$). ***Therefore, q is prime.***

Hence, $\frac{\mathbb{Z}}{<q>} \cong f(\mathbb{Z}) \subseteq P$. Since P is prime and $f(\mathbb{Z})$ its subfield, it follows that $f(\mathbb{Z}) = P$, hence $\frac{\mathbb{Z}}{<q>} \cong P$.

Definition .73 *The intersection of all subfields of a field F is called the prime subfield of F, which is the smallest subfield.*

Definition .74 *A field extension of a field F is a pair (K, σ), where K is a field and $\sigma : F \to K$ is a monomorphism.*



In particular, σ can be an identity map, making $F \subseteq K$ (a superset and the field itself) an extension of F. We denote $\sigma(F)$ also simply by F (as $F \cong \sigma(F)$). We define $\phi : F \times K \to K$, where F is a field and K is its extension, by $(\alpha, x) \mapsto \alpha x$, with $\alpha \in F$ and $x \in K$. This allows us to immediately see that:

1. *K is a vector space over F.*
2. *K has a basis and dimension over F.*

Definition .75 *The dimension of K as a vector space over F is called the degree of K over F, denoted as $[K : F]$.*

Example 1.19.3 *1. $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field extension of $\mathbb{Q}$ (why?). The set $\{1, \sqrt{2}\}$ forms a basis of $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$, resulting in $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.*

2. *$[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]] = 2$.*
3. *$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$*
4. *$[\mathbb{R} : \mathbb{Q}] = \infty$.*
5. *Let F be a field, and let K be the field of quotients of $F[x]$, where x is an indeterminate over F. For $\alpha_0, \alpha_1, \cdots, \alpha_n \in F$, assuming $\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n = 0$, it follows that $\alpha_i = 0$ for $0 \leq i \leq n$. In other words, the set $\{1, x, x^2, \cdots, x^n, \cdots\}$ will be an infinite independent set, leading to $[K : F] = \infty$.*

Example 1.19.4 *In 5^{th} and 1^{st} part above, K is an infinite extension of F, while $\mathbb{Q}[\sqrt{2}]$ is a finite extension of $\mathbb{Q}$.*

Definition .76 *Let $S \subseteq K$, where K is a field. A subfield K' of K is said to be generated by S, denoted by $< S >$, if $S \subseteq K'$ and if L is a subfield of K such that $S \subseteq L$, then $K' \subseteq L$, i.e., K' is the smallest subfield containing S (denoted as $K' =< S >$), and it is the intersection of all subfields of K containing S.*

(Note the round brackets): If K is a field extension of F, then the subfield of K generated by $F \cup S$ is referred to as the subfield of K generated by S over F and denoted as $F(S)$, i.e., $F(S) = \langle F \cup S \rangle$. If $S = \{a_1, a_2, \ldots, a_n\}$, then $F(S) = F(a_1, a_2, \ldots, a_n)$. If $S = \{a\}$ (singleton), we simply write $F(a)$.

Yes, there is a distinction between $F[a]$ and $F(a)$. To clarify, $F(a)$ is, as defined earlier, a field. In contrast, $F[a]$ represents the set of polynomials over F with the indeterminate a and forms a ring generated by $F \cup \{a\}$. It's important to emphasize that $F[a]$ is a subset of $F(a)$.

Proposition .38 *If K is an extension of L, and L is an extension of F, then K is an extension of F. Moreover, $[K : F] = [K : L][L : F]$.*

Proof: *Let $[K : L] = n$ and $[L : F] = m$. Since K is an extension of L with degree n, there exist n linearly independent elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ such that $K = L(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Similarly, since L is an extension of F with degree m, there exist m linearly independent elements $\beta_1, \beta_2, \ldots, \beta_m \in L$ such that $L = F(\beta_1, \beta_2, \ldots, \beta_m)$. Combining these two results, we have:*

$$K = L(\alpha_1, \alpha_2, \ldots, \alpha_n) = (F(\beta_1, \beta_2, \ldots, \beta_m))(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

By the distributive property, this is equivalent to:

$$K = F(\beta_1\alpha_1, \beta_1\alpha_2, \ldots, \beta_m\alpha_n)$$

The elements $\beta_i\alpha_j$ are all in K, so we can conclude that K is an extension of F. Furthermore, $[K : L] = n$ and $[L : F] = m$, so the product rule for degrees of field extensions gives:

$$[K : F] = [K : L][L : F] = n \cdot m$$

Thus, we have proven that K is an extension of F and that $[K : F] = [K : L][L : F]$, as desired. ■

Definition .77 *A field is said to be finitely generated over F if there exist a finite number of elements $a_1, a_2, \ldots, a_n$ in K such that $K = F(a_1, a_2, \ldots, a_n)$.*

Definition .78 *If K is generated by a single element over F, i.e., $K = F(a)$ for some $a \in K$, then K is called a simple extension of F.*

Example 1.19.5 *$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ is a simple extension of $\mathbb{Q}$.*

Note 28 *Consider $a \in K$. $F(a)$ is a subfield of K generated by a over F, i.e.,*

1. *All powers of a are allowed.*
2. *All elements of F are allowed.*

Thus, we have the combination $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n \in F(a)$ for all $\alpha_i \in F$ and $a \in K$. Clearly, $F[a] \subseteq F(a)$. Therefore, the field of quotients of $F[a]$ is also contained in $F(a)$ (as it will be the smallest), denoted as T. That is, $T \subseteq F(a)$. Since $F \subseteq T$ and $a \in T$ (since T is a field), we have $F(a) \subseteq T$. This implies $T = F(a)$, so $F(a)$ is the field of quotients of $F[a]$.

In general, $F(S)$ is the field of quotients of $F[S]$, where S is the subring of K generated by $F \cup S$.

Definition .79 *An element $a \in K$ is said to be a root of $p(x) \in F[x]$ if $p(a) = 0$.*

Definition .80 *An element $a \in K$ is said to be algebraic over F if a is a root of a non-zero polynomial $f(x) \in F[x]$.*

Definition .81 *K is called an algebraic extension of F if* $\forall\ a \in K$, *a is algebraic over F, meaning* $\exists\ f(x) \in F[x]$ *for all* $a \in K$ *such that* $f(a) = 0$.

Definition .82 *A polynomial is monic if its leading coefficient is 1.*

Theorem .49 *If* $a \in K$ *is algebraic over F, then* $\exists$ *a unique monic polynomial* $p(x) \in F[x]$ *such that*

1. $p(a) = 0$
2. $\forall\ f(x) \in F[x]$, *if* $f(a) = 0$, *then* $p(x) | f(x)$.

Hint(s): *Let* $t(x)$ *be a polynomial for a such that* $t(a) = 0$. *Convert* $t(x)$ *to a monic polynomial by multiplying with the inverse of its leading coefficient. Let* $p(x) = \alpha_n^{-1} t(x)$. *Choose* $t(x)$ *to be of the smallest degree such that* $t(a) = 0$, *then* $p(x)$ *will have the same property. For any* $f(x) \in F[x]$ *with* $f(a) = 0$, *write* $f(x) = q(x)p(x) + r(x)$. *It follows that* $r(a) = 0$ *or* $deg(r(x)) < deg(p(x))$. *Thus,* $f(a) = q(a)p(a) + r(a) \Rightarrow r(a) = 0$ *(since* $f(a) = 0$*), implying the existence of* $r(x)$ *such that* $deg(r(x)) < deg(p(x))$ *and* $r(a) = 0$, *which is not possible. Therefore,* $r(x) = 0$, *resulting in* $p(x) | f(x)$. *The uniqueness of* $p(x)$ *can be proven (as an exercise).*

Definition .83 *The monic polynomial of smallest degree in* $F[x]$ *for an algebraic element* $a \in K$ *is called the minimal polynomial of a over F.*

The degree of the minimal polynomial of a is called the degree of a over $\mathbb{F}$, *which is* $n = [F(a) : F]$, *equal to the degree of the minimal polynomial of a, indicating that a is algebraic over F with degree n.*

Example 1.19.6 1. *The minimal polynomial of* $\sqrt{3}$ *over* $\mathbb{Q}$ *is* $x^2 - 3$, *so* $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

2. *The minimal polynomial of* $(2)^{\frac{1}{3}}$ *over* $\mathbb{Q}$ *is* $x^3 - 2$.

Proposition .39 *Let R be a ring.* $[F(a) : F]$ *is finite if and only if a is algebraic over F.*

Proof: $F(a)$ *is a vector space over F of dimension n. Any* $(n+1)$ *vectors in* $F(a)$ *will be linearly dependent, which means* $1, a, a^2, \cdots, a^n$ *are linearly dependent. This implies that* $\exists\ \alpha_0, \alpha_1, \cdots, \alpha_n \in F$ *such that* $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n = 0$. *Thus, a is a root of the polynomial* $\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in F[x]$, *making a algebraic over F.*

Conversely, suppose a is algebraic, and let $p(x)$ *be its minimal polynomial with* $deg(p(x)) = n$. *For any non-zero element* $f(a) = \alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1} a^{n-1} \in F[a]$ *(since* a^i *for* $i \geq n$ *can be expressed as a combination of* $1, a, a^2, \ldots, a^{n-1}$ *due to* $p(a) = 0$*), we have* $p(x) \nmid f(x)$ *(because the degree of* $f(x)$ *is less than that of* $p(x)$*). Since* $p(x)$ *is minimal, there exist* $A(x)$ *and* $B(x) \in F(x)$ *such that* $A(x)p(x) + B(x)f(x) = 1$. *It follows that* $B(a)f(a) = 1$, *resulting in* $(f(a))^{-1} = B(a)$. *Thus,* $F[a]$ *is a field, implying* $F(a) = F[a]$. *Furthermore,* $1, a, \ldots, a^{n-1}$ *is a linearly independent set that spans* $F(a)$.

Proposition .40 *Every finite extension of a field is an algebraic extension.*

Remark 8 *The converse of the above proposition may not be true. An algebraic extension may not necessarily be a finite extension.*

Example 1.19.7 *Let A be a field of algebraic numbers over* $\mathbb{Q}$, *meaning A is an algebraic extension of* $\mathbb{Q}$. *However, A is not a finite field extension of* $\mathbb{Q}$.

Remark 9 *If* $F \subseteq F_1 \subseteq K$, *and* $a \in K$ *is algebraic over F, then a is also algebraic over* F_1 *since* $F \subseteq F_1$. *If* $p(x)$ *is the minimal polynomial of a in* $F[x]$, *and* $p_1(x)$ *is the minimal polynomial of a in* $F_1[x]$, *then* $p_1(x) | p(x) \in F_1[x]$. *This implies that* $deg(p_1(x)) \leq deg(p(x))$. *Also,* $[F(a) : F] = deg(p(x))$ *and* $[F_1(a) : F_1] = deg(p_1(x))$, *so* $[F_1(a) : F_1] \leq [F(a) : F]$.

Theorem .50 *If L is an algebraic extension of K and K is an algebraic extension of F, then L is an algebraic extension of F.*

Proof: *Let* $a \in L$ *(we will prove that a is algebraic over F). Since L is an algebraic extension of K, we have* $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$ *for some* $\alpha_i \in K$. *Define* $F_0 = F$ *and* $F_i = F_{i-1}(\alpha_i)$. *Using the earlier remark, we find that* $[F_i : F_{i-1}] \leq [F(\alpha_i) : F]$, *which is finite. Therefore,* $[F_i : F_{i-1}]$ *is finite. Since* $[F_n : F] = [F_n : F_{n-1}] \cdots [F_1 : F]$, *we conclude that* $[F_n : F]$ *is finite. Now,* $\alpha_i \in F_n = F[\alpha_1, \alpha_2, \cdots, \alpha_n]$. *Also, a is algebraic over* F_n, *so* $[F_n(a) : F_n]$ *is finite. This implies* $[F_n(a) : F] = [F_n(a) : F_n][F_n : F]$, *and therefore* $[F_n(a) : F]$ *is finite. Thus,* $F_n(a)$ *is an algebraic*

extension of F, and hence a is algebraic over F (since $a \in F_n(a)$). As a is an arbitrary element of L, we conclude that L is an algebraic extension of F.

Exercise 60 *Show that the set of all elements in K (field) which are algebraic over F forms a subfield of K containing F. In this case, no element of K is algebraic over S if $a \notin S$.*

Proof: *Since $\alpha \in F$, we have $x - \alpha \in F(x)$. Furthermore, $F \subseteq S$, where S is the set of all elements of K that are algebraic over F. Also, if $a, b \in S$, then $[F(a) : F]$ and $[F(b) : F]$ are finite, implying that $F(a,b)$ is an algebraic extension. This shows that $a - b \in F(a,b)$, and thus $a - b$ is algebraic over F. Similarly, ab^{-1} and so S is a field containing F.*

Moreover, let S_1 be the set of all elements of K that are algebraic over S. Since S_1 is a subfield of K that contains S (as shown earlier), and S_1 is an algebraic extension of S (since S is an algebraic extension of F), we have $S_1 \subseteq S$. However, $S \subseteq S_1$, so we conclude that $S = S_1$.

Exercise 61 *If a and b are algebraic over K, then*

1. *$a \pm b$ and ab are algebraic over F*
2. *$0 \neq b$ and ab^{-1} are algebraic over F*

Definition .84 *If S is the largest possible algebraic extension of F in K, then S is called algebraically closed with respect to K (i.e., S has no proper algebraic extension in K). S is called the algebraic closure of F relative to K (if K is an algebraic extension of F, then $S = K$).*

Define $\sigma : F[x] \to F[a]$ by $\sigma(f(x)) = f(a)$, where $a \in K$ is algebraic over F and $p(x)$ is its minimal polynomial. Then $\ker\sigma =< p(x) >$. Since σ is onto and a homomorphism, we have $\frac{F[x]}{\ker\sigma} \cong F[a]$. This means that the field extension $\frac{F[x]}{<p(x)>} \cong F(a)$ can be constructed (as $F(a) = F[a]$).

Example 1.19.8 *Let $F = F_2$ and $p(x) = x^2 + x + 1$. If $\omega \in F_4 = \{1, \omega, \omega^2, 0\}$ and $p(x)$ is the minimal polynomial of ω, then $F_4 \cong \frac{F_2[x]}{<x^2+x+1>} = \{a + bx : a, b \in F_2\} = \{0, 1, x, 1 + x\}$ with the property $1 + x + x^2 = 0$.*

Theorem .51 *If any two elements a and b of K have the same minimal polynomial $p(x)$ over F, then there exists an isomorphism σ of $F(a)$ onto $F(b)$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in F$ and $\sigma(a) = b$.*

Hint(s): *Let $\eta_1 : \frac{F[x]}{<p(x)>} \cong F(a)$ and $\eta_2 : \frac{F[x]}{<p(x)>} \cong F(b)$. Choose $\sigma = \eta_2\eta_1^{-1}$ such that $\sigma(\alpha) = \eta_2\eta_1^{-1}(\alpha) = \eta_2(\alpha) = \alpha$ for all $\alpha \in F$, and $\sigma(a) = \eta_2\eta_1^{-1}(a) = \eta_2(x) = b$.*

Proposition .41 *An element $a \in K$ is a root of a polynomial $f(x)$ over F if and only if $(x - a) | f(x) \in \mathbb{K}[x]$.*

Hint(s): *Let $a \in K$. If a satisfies $f(x) \in F[x]$, then $x - a \in K[x]$. By the division algorithm, $f(x) = (x - a)q(x) + r(x)$, where $r(x) = 0$ or $deg(r(x)) < deg(x - a) = 1$. This implies $r(x)$ is a constant polynomial, so $f(x) = (x - a)q(x) + c$, and evaluating at $x = a$ yields $c = 0$. Hence, $(x - a) | f(x)$. The converse is straightforward.*

Theorem .52 *A polynomial of degree $n \geq 1$ over a field F cannot have more than n roots in any field extension of F.*

Proof: *Let $f(x)$ be a polynomial of degree n over F. For $n = 1$, $f(x) = \alpha + \beta x$, where $\alpha, \beta \in F$ and $\beta \neq 0$. Thus, $-\alpha\beta^{-1} \in F$ is the only root of $f(x)$. Suppose the result holds for all polynomials of degree $< n$. If K has no root (where K is a field extension of F), then the result is true. Let $a \in K$ satisfy $f(a) = 0$, and let the multiplicity of a be m, i.e., $(x - a)^m | f(x)$ and $(x - a)^{m+1} \nmid f(x)$. Therefore, $f(x) = (x - a)^m f_1(x)$, where $deg(f_1(x)) = n - m < n$. Thus, $f_1(x)$ cannot have more than $n - m$ roots in K, which implies that $f(x)$ cannot have more than n roots in K.*

Theorem .53 *If $p(x)$ is any irreducible polynomial over F, then there exists an extension E of F such that $[E : F] = deg(p(x))$ and $p(x)$ has a root in E.*

Theorem .54 *The above theorem was proposed by Kronecker.*

Definition .85 (Splitting Field) *Let $f(x)$ be any polynomial of degree $n \geq 1$ over a field F. A field extension E of F is a splitting field of $f(x)$ if:*

1. *$f(x)$ can be factored into n linear factors over E*
2. *There does not exist any proper subfield E' of E that contains F and allows $f(x)$ to be factored into n linear factors over E.*

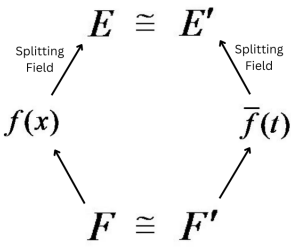
In other words, E is a splitting field of $f(x)$ if E contains n roots of $f(x)$ and $E = F(a_1, a_2, \cdots, a_n)$, where $a_1, a_2, \cdots, a_n$ are roots of $f(x)$.

Definition .86 (Conjugate) *Two elements a and b of a field K are said to be conjugate over a subfield F of K if they are algebraic over F and have the same minimal polynomial over F.*

Example 1.19.9 1. *$\sqrt{3}$ and $-\sqrt{3}$ are conjugate elements of R over $\mathbb{Q}$, as $x^2 - 3$ is the minimal polynomial over $\mathbb{Q}$ for both.*
2. *$(2)^{\frac{1}{3}}, (2)^{\frac{1}{3}}\omega, (2)^{\frac{1}{3}}\omega^2$, where $\omega^3 + \omega + 1 = 0$ and ω is a complex cube root of unity, are conjugate elements of $\mathbb{C}$ over $\mathbb{Q}$. They share the common minimal polynomial $x^3 - 2$.*

The roots of the minimal polynomial provide us with the conjugate elements.

Theorem .55 *Let $F \cong F'$, and let $f(x)$ be a polynomial over F with the corresponding polynomial $\bar{f}(t)$ in F'. If E is the splitting field of $f(x)$ and E' is the splitting field of $\bar{f}(t)$, then there exists an isomorphism $\phi : E \to E'$, where ϕ maps α to $\bar{\alpha}$ for all $\alpha \in F$ and $\bar{\alpha} \in F'$.*



In particular, if $F = F'$, i.e., the two splitting fields of same polynomial are isomorphic.

Example 1.19.10 *Consider two polynomials $x^2 + 3$ and $x^2 + x + 1$ over $\mathbb{Q}$. Both polynomials have roots that are in extensions of $\mathbb{Q}$. The roots of $x^2 + 3$ are $\pm\sqrt{-3}$, so $\mathbb{Q}(\sqrt{-3})$ is a splitting field of $x^2 + 3$. Similarly, the roots of $x^2 + x + 1$ are ω and ω^2, where ω is a cube root of unity. Therefore, $\mathbb{Q}(\omega)$ is a splitting field of $1 + x + x^2$. Moreover, $\sqrt{-3} = 2\omega + 1 \in \mathbb{Q}(\omega)$ and $\omega = \frac{1}{2} + \frac{\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$, leading to the conclusion that $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. Thus, both the polynomials $x^2 + 3$ and $x^2 + x + 1$ have the same splitting fields.*

Remark 10 *For any polynomial $f(x)$ of degree $n \geq 1$ over F, there exists an extension E of F where $f(x)$ has n roots in E, and $[E : F] \leq n!$.*

Example 1.19.11 *Consider the polynomial $x^3 - 2$ over $\mathbb{Q}$. The roots are $\alpha = (2)^{\frac{1}{3}}$, $\omega\alpha$, and $\omega^2\alpha$. If E is the splitting field of $x^3 - 2$, then $[E : \mathbb{Q}] \leq 3! = 6$. Moreover, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. This implies that $3|[E : \mathbb{Q}]$ and $2|[E : \mathbb{Q}]$, leading to $6|[E : \mathbb{Q}]$, hence $[E : \mathbb{Q}] = 6$.*

Example 1.19.12 *Consider the polynomial $x^4 - 1$ over $\mathbb{Q}$. The roots are $1, -1, i$, and $-i$. The splitting field of $x^4 - 1$ is $\mathbb{Q}(i)$, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.*

Exercise 62 *Find the degree of the splitting field of $x^5 - 3x^3 + x^2 - 3$ over $\mathbb{Q}$.*

Solution: *The polynomial $x^5 - 3x^3 + x^2 - 3 = (x^2 - 3)(x^3 + 1)$ has roots $\pm\sqrt{3}$, -1, and $\frac{1 \pm \sqrt{3}i}{2}$. The splitting field $K = \mathbb{Q}(\pm\sqrt{3}, -1, \frac{1 \pm i\sqrt{3}}{2})$. We claim that $K = \mathbb{Q}(\sqrt{3}, i)$, as $\frac{1 \pm i\sqrt{3}}{2} \in \mathbb{Q}(\sqrt{3}, i)$ and $\frac{1 + i\sqrt{3}}{2} - \frac{1 - i\sqrt{3}}{2} = \sqrt{3}i \Rightarrow i \in K$. Now, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \leq 4$, and the minimal polynomial of $\sqrt{3}$ has degree 2, so $2|[K : \mathbb{Q}]$. If $[K : \mathbb{Q}] = 2$, then $[K : \mathbb{Q}(\sqrt{3})] = 4$, which would mean $K = \mathbb{Q}(\sqrt{3})$, contradicting the inclusion of i in K. Hence $[K : \mathbb{Q}] = 4$.*

1.20. Separable/Inseparable Extensions

Definition .87 *For a polynomial $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ in $F[x]$, its derivative, denoted as $f'(x)$, is defined as $f'(x) = \alpha_1 + 2\alpha_2 x + \cdots + n\alpha_n x^{n-1}$.*

Proposition .42 *For $f(x) \in F[x]$ and $\alpha \in K$ (an extension of F), α is a multiple root of $f(x)$ if and only if α is a common root of $f(x)$ and $f'(x)$.*

Proposition .43 *If an irreducible polynomial $f(x)$ over F has a multiple root, then its derivative $f'(x) = 0$.*

Hint(s): *If α is a common root of $f(x)$ and $f'(x)$, then $f(x) | f'(x)$. This can only happen if $f'(x) = 0$.*

Corollary .56 *No irreducible polynomial over a field of characteristic zero has a multiple root in any field extension.*

Example 1.20.1 *If $charF \neq 0$, let $F = \mathbb{Z}_2(t)$. Consider $f(x) = x^2 - t$, where t is an indeterminate. Let K be a splitting field of $f(x)$, and let a_1 and a_2 be roots of $f(x)$ in K. Then, $x^2 - t = (x - a_1)(x - a_2)$. Comparing, we find that $a_1 = -a_2$ ($-a_2 = a_1$ in F), so $a_1 = a_2 = a$. Thus, $x^2 - t = (x - a)^2$, and a is a multiple root of $f(x)$. Also, $f'(x) = 2x = 0$ in $F[x]$.*

Definition .88 *An irreducible polynomial $f(x) \in F[x]$ of degree n is said to be separable if it has n distinct roots in its splitting field. Otherwise, $f(x)$ is inseparable.*

A polynomial $f(x)$ is said to be separable if all of its irreducible factors are separable. Otherwise, it is inseparable.

Proposition .44 *An irreducible polynomial $f(x)$ is separable if and only if $f'(x) \neq 0$.*

Note 29 *If f is irreducible and has a multiple root, then $f'(x) = 0$.*

Note 30 *Every non-zero polynomial over a field with characteristic zero is separable.*

Exercise 63 *Verify the previous note.*

Note 31 *$x - 1$ and $x^2 + x + 1$ are irreducible over $\mathbb{Q}$ with $char(\mathbb{Q}) = 0 \Rightarrow x - 1$ and $x^2 + x + 1$ are separable.*

Define $f(x) = (x - 1)^2(x^2 + x + 1)$, which has the root 1 with multiplicity 2, but the factors (irreducible) are separable. Therefore, $f(x)$ is separable by definition. This illustrates that the concept of distinct roots is seen only in the extension and with irreducible factors but and not over the field where the polynomial is defined and with a full polynomial.

Proposition .45 *An irreducible polynomial $f(x)$ over a field F of characteristic p (> 0) is inseparable if and only if $f(x) \in F[x^p]$.*

Proof: *Let $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ (inseparable if and only if $f'(x) = 0$). $f'(x) = \alpha_1 + 2\alpha_2 x + \cdots + n\alpha_n x^{n-1} = 0 \Leftrightarrow \alpha_1 = 2\alpha_2 = \cdots = n\alpha_n = 0$. Hence, $p | k \ : \ k = 1, 2, \cdots$, or $\alpha_k = 0$ i.e., $k = pk_1$ i.e., term $\alpha_k x^k = \alpha_{k_1 p} x^{k_1 p} \Leftarrow f(x) \in F[x^p]$.*

Definition .89 *An element $a \in K$ (extension of F) which is algebraic over F is called separable (inseparable) over F if the minimal polynomial of a over F is separable (inseparable).*

An algebraic extension K of F is called a separable extension if every element of K is separable over $\mathbb{F}$. Otherwise, it is an inseparable extension.

Proposition .46 *Every polynomial over a field of characteristic zero is separable. Therefore, every algebraic extension of a field of characteristic zero is a separable extension.*

Example 1.20.2 *Consider an infinite field with finite characteristic, such as $F = \mathbb{Z}_2(t)$. If K is the splitting field of $x^2 - t$, then K is an algebraic extension (finite extension) but not a separable extension.*

Consider an integral domain D with characteristic p. Also, let $a, b \in D$, then $(a + b)^p = a^p + {}^pC_1 a^{p-1} b + \cdots + {}^pC_p b^p$. Here, $p | {}^pC_r$, $r = 1, 2, \cdots, p - 1 \Rightarrow (a + b)^p = a^p + b^p$. A map $\sigma : D \to D$ by $a \to a^p$ is a homomorphism as $\sigma(a + b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$ (verify). Also, $\ker\sigma = \{a \in D \ : \ a^p = 0\} = \{a \in D \ : \ a = 0\} = \{0\} \Rightarrow \sigma$ is one-to-one. Now, choose D as a finite integral domain. Then, D and $\sigma(D)$ have the same number of elements, i.e., σ is onto as well since $\sigma(D) = D$. Thus, $\sigma : a \to a^p$ is an automorphism.

Theorem .57 *Any algebraic extension of a finite field is separable.*

Proof: *Let $f(x)$ be any irreducible polynomial over F. Suppose $f(x)$ is inseparable over F. Then, $f(x) \in F[x^p]$,*

i.e., $f(x) = \beta_0 + \beta_1 x^p + \cdots + \beta_m x^{mp}$ *for some* $\beta_i \in F$. *Now,* $\alpha \to \alpha^p$ *for* $\alpha \in F$ *is an automorphism. Therefore, for all* $\beta_i \in F$, *we can find* $\alpha_i \in F$ *such that* $\beta_i = \alpha_i^p$, $i = 0, 1, \cdots, m$. *Consequently,* $f(x) = \alpha_0^p + \alpha_1^p x^p + \cdots + \alpha_m^p x^{mp} = (\alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m)^p$, *which implies that* $f(\alpha)$ *is not irreducible. This is a contradiction, so* $f(x)$ *must be separable. Hence, any algebraic extension K of F has its elements' minimal polynomial separable, making K a separable extension of F.*

Theorem .58 *Let F be an infinite field and E be a field extension of F. If a and b are algebraic over F and separable, then there exists* $c \in E$ *such that* $F(c) = F(a, b)$.

Note 32 *Any finite separable extension of an infinite field is a simple extension (prove it using induction).*

Definition .90 *A field having a finite number of elements is called a Galois field.*

Example 1.20.3 *1.* $\mathbb{Z}_p$ *for some prime p*

2. *Consider the splitting field K of* $x^2 + x + 1$ *over* $\mathbb{Z}_2$, *i.e., K consists of* 0, 1, *and* $1 + \alpha$ *where* $1 + \alpha + \alpha^2 = 0$. *This makes K a Galois field with 4 elements.*
3. *Let K be the splitting field of* $x^2 + 1$ *over* $\mathbb{Z}_3$. *Then, K has 9 elements:* $0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha$, *where* $\alpha^2 + 1 = 0$ *(since* $\frac{\mathbb{Z}_3[x]}{<x^2+1>} \cong \mathbb{Z}_3(\alpha)$ *and* α *is a root of* $x^2 + 1$ *with* $x^2 + 1$ *being the minimal polynomial of* α*).*

Example 1.20.4 *Prove that the order of every finite field is a single prime power, i.e.,* $|F| = p^n$ *for some prime p and* $n \in \mathbb{N}$.

Hint(s): *The prime subfield P of F is isomorphic to* $\mathbb{Z}_p$. *Let* $[F : P] = n$. *Treat F as a vector space over P with basis* $\{a_1, a_2, \cdots, a_n\}$ *so that* $\forall\ x \in F \Rightarrow x = \sum_{i=1}^{n} \lambda_i a_i$ *for some* $\lambda_i \in P$. *The presentation is unique. Therefore, a total of* p^n *such elements are possible.*

Proposition .47 *If a field F has* $q = p^n$ *elements, then F is a splitting field of* $x^q - x$ *over its prime subfield.*

Hint(s): $F \backslash \{0\}$ *is a group under multiplication of order* $q - 1 \Rightarrow a^{q-1} = 1$ *for all* $a \in F \backslash \{0\}$. *This implies* $a^q = a$. *Also,* $0^q = 0 \Rightarrow \forall\ b \in F \Rightarrow b^q = b$. *Hence, q roots of* $x^q - x$ *are in F. Since* $x^q - x \in P[x]$ *(over a prime field), it cannot have more than q roots in any extension of P. All roots of* $x^q - x$ *are in* $F \Rightarrow F$ *is the splitting field of* $x^q - x$ *over P.*

Proposition .48 *For every prime number p and* $n \in \mathbb{N}$, *there exists a field of order* p^n.

Proof: *Consider* $f(x) = x^{p^n} - x$ *over* $\mathbb{Z}_p[x]$. *If K is the splitting field of* $f(x)$, *we claim that K has* p^n *elements.* $f'(x) = p^n x^{p^n - 1} - 1 = -1$ *(since* $char(\mathbb{Z}_p) = p$*). This implies that* $f(x)$ *and* $f'(x)$ *have no common root. Therefore, there are* p^n *distinct roots of* $f(x)$ *in K. Let L be the set of all roots of* $f(x)$. *Since* 0 *and* 1 *are in L, and* $a - b$ *and* ab^{-1} *are also in L (check it) for all* $a, b \in L$, *L is a subfield of K that contains all roots of* $f(x) \Rightarrow K = L$ *where K is the splitting field. Hence,* $|K| = p^n$.

Exercise 64 *A field is finite if and only if its multiplicative group is cyclic.*

Definition .91 *A field F is called a perfect field if all finite extensions of F are separable.*

Exercise 65 *Prove that any algebraic extension of a perfect field is a separable extension.*