Field Theory

13.1 Basic Theory of Field extension

Characteristic of a field F

Definition: Characteristic of a field is the smallest positive integer n such that $n.1_F = 0$, if such a n exist otherwise it is defined to bo 0.
Notation: $char(F)$
Example: $Char(R) = 0$
$Char(Z_p) = p$

Proposition: $Char(F)$ is either 0 or a prime p.
Proof: If $Char(F) = 0$ then done.
If $Char(F) = n$ where n is positive integer
To prove n is prime.
If n is composite say $n = ab$ then $n.1_F = 0$
$ab.1_F = 0$
$a.1_F b.1_F = 0$
Since F is a field so F has no zero divisors
so either $a.1_F = 0$ or $b.1_F = 0$
which is not possible since n is smallest positive integer such that $n.1_F = 0$
Therefore n should be a prime.

Prime Subfield

Definition: A prime subfield of a field F is the smallest subfield of F generated by the multiplicative identity 1_F of F.
Note: If $char(F) = 0$ then prime subfield of field F is Q.
If $char(F) = p$ then prime subfield of field F is F.
Example: Prime subfield of Q and R is Q.

Extension field

Definition: If K is a field containing te subfield F then K is said to be extension field of F.
Notation: K/F.

Degree of extension Definition: The degree of a field extension K/F is the dimension of K as a vector space over F.
Notation :[K:F]

Proposition: Let $\phi : F \to F'$ be homomorphism of fields. Then ϕ is either 0 or is injective, so the image of ϕ is either 0 or isomorphic to F.
Proof:Let $\phi : F \to F'$ be a homomorphism of fields such that $\phi(x) \equiv 0$ then done.
If not then there exist x such that $\phi(x) \neq 0$.
Since F' is a field so their exist inverse of $\phi(x)$.
i.e. $\phi(x).\phi(x)^{-1} = 1$
$\Rightarrow \phi(x.x^{-1}) = 1$
$\phi(1) = 1$
Suppose $\phi(x) = \phi(y)$
$\Rightarrow \phi(x) - \phi(y) = 0$
$\Rightarrow \phi(x - y) = 0$
Now we have to show $x - y = 0$
Suppose $x - y \neq 0$ as F is a field so $x - y$ have inverse in F
so $(x - y)(x - y)^{-1} = 1$
$\Rightarrow \phi((x - y)(x - y)^{-1}) = \phi(1)$

$\Rightarrow \phi(x-y)\phi((x-y)^{-1}) = 1$
Since $\phi(x-y) = 0$ so we get $0 = 1$
which is not possible
$x - y = 0$
so $x = y$
Hence ϕ is injective.

Theorem:Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Then there exist a field K containing an isomorphic copy of F in which $p(x)$ has a root.
Proof: Let F be a field and $p(x)$ be an irreducible polynomial in $F[x]$.
As $p(x)$ is an irreducible polynomial so ideal generated by $< p(x) >$ is maximal ideal in $F[x]$.
Then $F[x]/ < p(x) >$ is a field.
Consider $K = F[x]/ < p(x) >$.
Consider canonical projection π of $F[x]$ to K.
Now consider $\phi : \pi|_F : F \to K$ which is homomorphism and not identically zero. Since $\phi(1) = 1$. Since If there exist a homomorphism between two fields then that map is either identcally zero or is injective.
That is image of ϕ is isomorphic to F.
Therefore there exit an isomorphic copy of F in K.
Now to show that $p(x)$ has a root in K.
Consider $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$.
So $p(\bar{x}) = a_0 + a_1\bar{x} + a_2\bar{x}^2 + ... + a_n\bar{x}^n$.
$p(\bar{x}) = a_0 + a_1(x + p(x)) + a_2(x^2 + p(x)) + ... + a_n(x^n + p(x))$.
$p(\bar{x}) = p(x)(modp(x))$
$p(\bar{x}) = 0$ in K.
So $p(x)$ has a root in K.
Therefore there exist a field K which contains an isomorphic copy of $p(x)$ and a root of $p(x)$.

Theorem: Let $p(x)$ be an irreducible polynomial of degree n over the field F and K be the field
$F[x]/ < p(x) >$.Let $\theta \equiv \text{mod } (p(x)) \in K$. Then the elements $1, \theta, \theta^2, ...\theta^{n-1}$ are a basis for K as a vector space over F, so the degree of extension is n, i.e. $[K : F] = n$
Hence $K = \{a_0 + a_1\theta + a_2\theta^2 + ... + a_{n-1}\theta^{n-1} | a_i \in F\}$.
Proof: Let F and K be a field such that $K = F[x]/ < p(x) >$.
To show that: $1, \theta, \theta^2, ...\theta^{n-1}$ are a basis for K as a vector space over F.
i.e. to show that: $1, \theta, \theta^2, ...\theta^{n-1}$ spans K over F and is linearly independent.
Now as F is a field so $F[x]$ is an Euclidean domain.
Let $a(x) \in F[x]$ be a polynomial.
Apply division algorithm to $a(x)$ and $p(x)$ then there exist $q(x)$ and $r(x)$ such that $a(x) = p(x)q(x) + r(x)$, where $r(x) \equiv 0$ or $degr(x) < n$.
so we get $a(x) \equiv r(x)mod(p(x))$
This shows that every polynomial in K represents by a polynomial of degree less than n.
Hence the images $1, \theta, \theta^2, ...\theta^{n-1}$ of $1, x, x^2...x^{n-1}$ spans K over F
Now to show they are linearly independent.
Suppose $b_0 + b_1\theta + b_2\theta^2 + ... + b_{n-1}\theta^{n-1} = 0$
this is equivalent to $b_0 + b_1x + b_2x^2 + ... + b_{n-1}x^{n-1} \equiv 0 \text{ mod } p(x)$
i.e. $p(x)$ divides $b_0 + b_1x + b_2x^2 + ... + b_{n-1}x^{n-1}$ in $F[x]$ As $p(x)$ is of degree n so this is possible only when all $b_i's$ are zero. Therefore $1, \theta, \theta^2, ...\theta^{n-1}$ are a basis for K as a vector space over F.

Definition: Field generated by $\alpha, \beta, ...$ over F
Let K be an extension of the field F and let $\alpha, \beta, ... \in K$ be a collection of elements of K.Then the smallest subfield of K containing both F and the elements $\alpha, \beta, ... \in K$ denoted by $F(\alpha, \beta, ...)$ is called the field generated by $\alpha, \beta, ...$ over F.
Simple extension
Definition: If the field K is generated by a single element α over F, $K = F(\alpha)$, then K is said to be simple

extension of F and the element α is called a primitive element for the extension.

Theorem:Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root of $p(x)$. Let $F(\alpha)$ be a subfield of K generated over F by α. Then $F(\alpha) \approx F[x]/ < p(x) >$.
Proof: Let $\phi : F[x] \to F(\alpha)$ be a function defined by
$\phi(a(x)) = a(\alpha)$
Since $\phi(x)[a(x) + b(x)] = \phi[(a + b)(x)] = [a + b](\alpha) = a(\alpha) + b(\alpha)$
$= \phi(a(x)) + \phi(b(x))$
and $\phi([a(x)b(x)]) = \phi(c(x)) = c(\alpha) = a(\alpha)b(\alpha)$.
Therefore ϕ is homomorphism. Now to find kernel of ϕ
$ker(\phi) = \{p(x) \in F[x]|\phi(p(x)) = 0\}$
$ker(\phi) = \{p(x) \in F[x]|p(\alpha) = 0\}$
Since $p(\alpha) = 0$ so $p(x)$ is in the kernel of ϕ As $p(x)$ is an irreducible so $F[x]/ < p(x) >$ is a field and ϕ is an identity map on F so it is not zero map.
So ϕ is an isomorphism with its image. So ϕ is an isomorphism.
Therefore $F(\alpha) \approx F[x]/ < p(x) >$.

Theorem:Let $\phi : F \to F'$ be an isomorphism of fields.Let $p(x)$ be an irreducible polynomial in $F[x]$ and let $p'(x) \in F'[x]$ be the polynomial obtained by applying the map ϕ to the coefficients of $p(x)$.Let α be a root of $p(x)$ and β be a root of $p'(x)$. Then there is an isomorphism $\sigma : F(\alpha) \to F'(\beta)$ mapping α to β such that σ restricted to F is the isomorphism ϕ.
Proof: Since ϕ be an isomorphism between $F[x]$ and $F'[x]$ so image of maximal ideal $< p(x) >$ is maximal ideal $< p'(x) >$ so there is an isomorphism between $F[x]/ < p(x) >$ and $F'[x]/ < p'(x) >$. and since $F[x]/ < p(x) >\approx F(\alpha)$ and $F'[x]/ < p'(x) >\approx F'(\beta)$.
Therefore $F(\alpha) \approx F'(\beta)$.

13.2 Algebraic Extensions

Algebraic element: *Definition*: The element $\alpha \in K$ is said to be algebraic over F if α is root of some polynomial $f(x) \in F[x]$.
Transcendental element: *Definition*:If α is not algebraic over F that is α is not a root of any polynomial over F is called Transcendental element.
Algebraic extension: An extension K/F is said to be algebraic extension if every element of K is algebraic over F.

Proposition: Let α be algebraic over F. Then there is unique monic irreducible polynomial $f(x) \in F[x]$ which has α as a root. A polynomial $g(x) \in F[x]$ has α as a root if and if $f(x)$ divides $g(x) \in F[x]$.
Proof: Let α be algebraic over F so suppose α satisfies a polynomial $h(x)$ of minimal degree in $F[x]$. As F is a field so without loss of generality assume that $h(x)$ is monic.
Now suppose $h(x)$ is reducible then $h(x) = a(x)b(x)$ such that degree of $a(x)$ and $b(x)$ is less than degree of $h(x)$.
Then $h(\alpha) = a(\alpha)b(\alpha)$, as $h(\alpha) = 0$
so $a(\alpha)b(\alpha) = 0$ but F is a field so either $a(\alpha) = 0$ or $b(\alpha) = 0$
which is not possible since $h(x)$ is minimal degree polynomial
So $h(x)$ is irreducible.
Therefore $h(x)$ is an irreducible monic polynomial having α as a root.
Now suppose $g(x) \in F[x]$ is any polynomial having α as a root.
Then by Euclidean algorithm there exists $q(x)$ and $r(x) \in F[x]$ such that
$h(x) = q(x)g(x) + r(x)$ with deg $r(x) <$ deg $g(x)$.
Then $f(\alpha) = q(\alpha)g(\alpha) + r(\alpha)$.
Since α is root of $h(x)$ and $g(x)$ so $r(\alpha) = 0$
Which contradict to the minimality of $h(x)$ unless $r(x) = 0$
Therefore $g(x)$ divides $h(x)$.

Now to prove $h(x)$ is unique.
Suppose $m(x)$ be another polynomial which satisfies the above conditions then $m(x)$ divides $h(x)$ and $h(x)$ divides $m(x)$.
So $m(x) = h(x)$. Hence there is unique monic irreducible polynomial which satisfied by α.

Corollary:If L/F extension of fields and α is algebraic over both F and L then minimal polynomial of α over L divides minimal polynomial of α over F in $L[x]$.
Proof: Let L/F is an extension of fields and as α is algebraic over F and L so there exist a minimal polynomial over F and L say $f(x)$ and $g(x)$ respectively.
Since As $f(x) \in F[x]$ and L is an extension of F so $f(x) \in L[x]$ so $g(x)$ divides $f(x)$ as $g(x)$ is a minimal polynomial for α in L.
Minimal Polynomial for α over F *Definition*:The polynomial of minimal degree which is unique monic and irreducible satisfied by α is called minimal polynomial for α over F.
Proposition: Let α be algebraic over field F and let $F(\alpha)$ be the field generated by α over F.
Then $F(\alpha) \approx F[x]/ < f(x) >$
so that in particular $[F(\alpha) : F] = \deg f(x) = \deg\alpha$.
i.e. the degree of α over F is the degree of extension it generates over F.
Proof: Since $F(\alpha) \approx F[x]/ < p(x) >$ where $p(x)$ is an irreducible polynomial over F satisfied by α so here $f(x)$ is a minimal polynomial for α so $F(\alpha) \approx F[x]/ < f(x) >$.
Proposition: The element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite.
Proof: Suppose α is algebraic over F.
Since if α is algebraic over F then the degree of extension $F(\alpha)/F$ is the degree of minimal polynomial for α over F.
Since degree of polynomial is finite so degree of extension $F(\alpha)/F$ is finite.
Conversely, suppose degree of extension of $F(\alpha)/F$ is finite say $[F(\alpha) : F] = n$
Consider $1, \alpha, \alpha^2, ..., \alpha^n$ i.e. $n + 1$ elements of $F(\alpha)$ which are linearly dependent over F so there exists $b_0, b_1, ..., b_n \in F$ not all zero such that $b_0 + b_1\alpha + b_2\alpha + ... + b_n\alpha = 0$
So α is root of nonzero polynomial over F
hence α is algebraic over F.
Corollary: If the extension K/F is finite then it is algebraic.
Proof: If $\alpha \in K$ then $F(\alpha)$ is a subfield of K.
So $[F(\alpha) : F] \leq [K : F]$.
Since degree of extension of K/F is finite so degree of extension of $F(\alpha)/F$ is finite
hence α is algebraic over F.

Quadratic extension over field of characteristic $\neq 2$:
Let F be a field of characteristic $\neq 2$ and let K be an extension of F such that $[K : F] = 2$
Let $\alpha \in K$ such that $\alpha \notin F$ so there exist a polynomial of degree 2 say $f(x) = x^2 + bx + c$.
So $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$.
As $b \in F$ so $\frac{b}{2} \in F$ and $b^2 - 4ac$ is not a perfect square So $F(\alpha) = F(\sqrt{b^2 - 4c}) = K$.
Theorem: Let $F \subseteq K \subseteq L$ be fields.Then $[L : F] = [L : K][K : F]$.
that is extension degrees are multiplicative, where if one side of equation is infinite
the other side is also infinite.
Proof: Suppose degree of extension are finite say $[L : K] = m$ and $[K : F] = n$.
So the number of elements in the basis for L over K is m and K over F is n say
$\alpha_1, \alpha_2, ..., \alpha_m$ be a basis for L over K and
$\beta_1, \beta_2, ..., \beta_n$ be a basis for K over F.
So every element of L can be written as linear combination of elements of basis.
say $x \in L$ so $x = a_1\alpha_1 + a_2\alpha_2 + ... + a_m\alpha_m$ where $a_i \in K$
also every a_i is linear combination of $\beta_i' s$ that is
$a_i = b_{i1}\beta_1 + b_{i2}\beta_2 + ... + b_{in}\beta_n$ where $i = 1, 2, ..., m$
and b_{ij} are the elements of F

If we substitute the values of a_i in x so we get $\sum_{i=1,2,...,mj=1,2,...,n} b_{ij}\alpha i\beta_j$
so these $\alpha_i\beta_j$ are total mn elements
Since we have to show that $[L:F]=m.n$ So consider linear combination
$\sum_{i=1,2,...,mj=1,2,...,n} b_{ij}\alpha i\beta_j = 0$ where all b_{ij} are in F
since this linear combination is nothing but $a_1\alpha_1 + a_2\alpha_2 + ... + a_m\alpha_m = 0$
Since $\alpha_i's$ are the basis for L over K so all coefficients $a_i = 0$
so $b_{i1}\beta_1 + b_{i2}\beta_2 + ... + b_{in}\beta_n = 0$ where $i = 1,2,...,m$
Since β_j $j = 1,2,...,n$ form a basis for K over F.
so every coefficient is equal to 0 that is $b_{ij} = 0$ for all i and j
So $\alpha_i\beta_j$ are linearly independent over F and
Since $x \in L$ can be written as linear combination of elements over F
Hence $\alpha_i\beta_j$ forms a basis for L over F.
that is $[L:F] = m.n = [L:K][K:F]$
Now if $[K:F]$ is infinite then there are infinitely many elements of K, so elements of L which are linearly independent over F, so that $[L:F]$ is infinite.
Similarly if $[L:K]$ is infinite there are infinitely many elements of L linearly independent over Kso certainly linearly independent over F, so $[L:F]$ is infinite
Hence if both $[L:K]$ and $[K:F]$ are finite then $[L:F]$ is finite and if $[L:F]$ is infinite then atleast one of them is infinite.

Corollary: Suppose L/F is a finite extension and let K be any subfield of L containing F, $F \subset K \subset L$. Then $[K:F]$ divides $[L:F]$.
Proof: Since $F \subset K \subset L$ so $[L:F] = [L:K][K:F]$
Hence $[K:F]$ divides $[L:F]$.

Finitely generated extension:
Definition: An extension K/F is finitely generated if there are elements $\alpha_1, \alpha_2, ..., \alpha_k$ in K such that $K = F(\alpha_1, \alpha_2, ..., \alpha_k)$.

Lemma:$F(\alpha, \beta) = (F(\alpha))(\beta)$
Proof: Since $F(\alpha)$ is contained in $F(\alpha, \beta)$ and also $\beta \in F(\alpha, beta)$
so $(F(\alpha))(\beta) \subset F(\alpha, \beta)$.
Now since $(F(\alpha))(\beta)$ contains F, α, β but $F(\alpha, \beta)$ is the smallest field which contains this elements
so $F(\alpha, \beta) \subset (F(\alpha))(\beta)$.
We can generalize this theorem as
$F(\alpha_1, \alpha_2, ..., \alpha_k) = (F(\alpha_1, \alpha_2, ..., \alpha_{k-1})(\alpha_k)$

Theorem: The extension K/F is finite if and only if K is generated by finite number of algebraic elements over F.
Proof: Suppose K/F is finite that is say $[K:F] = n$ so there are n elements in the basis
Suppose $\alpha_1, \alpha_2, ..., \alpha_n$ be a basis for K as a vector space over F.
Since $F(\alpha_i)$ is a subfield of K for $i = 1,2,...n$
$[F(\alpha_i):F]$ divides $[K:F]$ for $i = 1,2,...,n$
so each α_i is algebraic over F
Since $\alpha_1, \alpha_2, ..., \alpha_n$ be a basis for K so K is generated by α_i
That is K is generated by finite number of algebraic elements over F.
Conversely suppose K is generated by finite number of algebraic elements over F.
To show K/F is finite.
Let $\alpha_1 \in K$ be an algebraic element over F then the simple extension $F(\alpha_1)/F$ is finite
now as $\alpha_2 \in K$ is also algebraic so $(F(\alpha_1))(\alpha_2)/F$ is finite
since $(F(\alpha_1))(\alpha_2) = F(\alpha_1, \alpha_2)$ so $F(\alpha_1, \alpha_2)/F$ is finite.

since K is generated by finite number of algebraic elements so Hence $K = F(\alpha_1, \alpha_2, ..., \alpha_n)/F$ is finite.

Corollary: Suppose α and β are algebraic over F. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ for $\beta \neq 0$ are all algebraic.
Proof: Since $F(\alpha, \beta)$ contain this all elements as it is field
and since this field is generated by finite number of algebraic elements so is algebraic. hence $\alpha \pm \beta, \alpha\beta, \alpha/\beta$.

Corollary: Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.
Proof: Let K be collection of all algebraic elements of L over F
Let $\alpha, \beta \in K$ that is α, β are algebraic hence $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ for $\beta \neq 0$ are all algebraic. So $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K$.
hence K is a subfield of L.

Theorem: If K is algebraic over F and L is algebraic over K, then L is algebraic over F.
Proof: Let α be any element of L. Then α is algebraic over K so α satisfies some polynomial equation say $a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0$. Where $a_i \in K$
Now consider the field $F(\alpha, a_0, a_1, ..., a_n)$ generated over F by α and the coefficient of this polynomial.
Since K/F is algebraic so the elements $a_0, a_1, ..., a_n$ are all algebraic over hence the extension $F(a_0, a_1, ..., a_n)/F$ is finite.
and since α generates an extesnion of degree atmost n
since $F(\alpha, a_0, a_1, ..., a_n) = [F(\alpha, a_0, a_1, ..., a_n) : F(a_0, a_1, ..., a_n)][F(a_0, a_1, ..., a_n) : F]$
So $F(\alpha, a_0, a_1, ..., a_n)$ is finite hence it is algebraic.
so α is algebraic over F.
Hence L is algebraic over F.

Composite field: Let K_1 and K_2 be two subfields of K then the composite field of K_1 and K_2 is the smallest subfield of K conatining both K_1 and K_2 .
In general composite of any collection of subfield of K is the smallest subfield containing both K_1 and K_2.
Proposition: Let K_1 and $K2$ be two finite extension of a field F contained in K. Then $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$ with equality if and only if an F basis for one of the fields remains linearly independent over the other fields. If $\alpha_1, \alpha_2, ..., \alpha_n$ and $\beta_1, \beta_2, ..., \beta_m$ are bases for K_1 and K_2 over F respectively, then the elements $\alpha_i\beta_j$ for $i = 1, 2, ..., n$ and $j = 1, 2, ..., m$ span K_1K_2 over F.
Proof: Since $\alpha_1, \alpha_2, ..., \alpha_n$ and $\beta_1, \beta_2, ..., \beta_m$ are bases for K_1 and K_2 over F
so we can write $K_1K_2 = F(\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_m) = K_1(\beta_1, \beta_2, ..., \beta_m)$
so $\beta_1, \beta_2, ..., \beta_m$ span K_1K_2 over K_1
therefore $[K_1K_2 : K_1] \leq m$ as $m = [K_2 : F]$
so $[K_1K_2 : K_1] \leq [K_2 : F]$ here equality holds if and only if $\beta_1, \beta_2, ..., \beta_m$ are linearly independent over K_1.
Since $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$
Hence $[K_1K_2 : F] \leq [K_2 : F][K_1 : F]$.

Corollary: Suppose that $[K_1 : F] = n$ and $[K_2 : F] = m$ where n and m are relatively prime. Then $[K_1K_2 : F] = [K_2 : F][K_1 : F]$.
Proof: Since $[K_1K_2 : F] \leq [K_2 : F][K_1 : F]$ so $[K_1K_2 : F] \leq nm$ now since $[K_1K_2 : F]$ divisible by n and m as K_1 and K_2 are subfield of K_1K_2 so it is divisible their least common multiple also. here $(n, m) = 1$ so lcm of n and m is nm
so $[K_1K_2 : F]$ is divisible by nm that is $nm \leq [K_1K_2 : F]$
Hence $[K_1K_2 : F] = [K_2 : F][K_1 : F]$

Splitting field and algebraic closures:
Splitting field:The extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.
Theorem: For any field F, if $f(x) \in F[x]$ then there exist an extension K of F which is a splitting field for $f(x)$.

Proof: Let $f(x)$ be a polynomial in $F[x]$ of degree n
First we will show that there exist an extension E of F for which $f(x)$ splits completely into linear factors by induction on n
For $n = 1$ that polynomial of degree one, so it has root in F only.
So here extension $E = F$. Therefore statement is true for $n = 1$
Now suppose $n > 1$.
Assume that statement is true for all polynomials of degree less than n.
we have a polynomial which is either reducible or irreducible. If it is reducible and every factor is linear then again $E = F$
Otherwise there exist atleast one irreducible factor which is of degree atleast two say $p(x)$
Since if polynomial is irreducible then we can find an extension in which this polynomial is reducible say extension is E_1.say α is root of this polynomial which is in E_1.
Over E_1 the polynomial $f(x)$ has linear factor $x - \alpha$.
then degree of remaining factor say $f_1(x)$ is $n-1$. by induction there exist and extension E of E_1 containing all the roots of $f_1(x)$. Since $\alpha \in E$, E is an extension of F containing all the roots of $f(x)$. Now let K be the intersection of all the subfields of E containing F which also contain all roots of $f(x)$. Then K is a splitting field for $f(x)$.
Normal extension : If K is an algebraic extension of F which is splitting field over F for a collection of polynomials $f(x) \in F[x]$ then K is called normal extension of F.

Proposition: A splitting field of a polynomial of degree n over F is of degree atmost $n!$ over F.
Proof: Let $f(x) \in F[x]$ be any polynomial of degree n
now attach one root of $f(x)$ to the base field say the extension is F_1.
So the degree of extension of F_1 over F is atmost n. since degree is equal to n if $f(x)$ is irreducible over F.
Over F_1 the polynomial $f(x)$ has atleast one linear factor so that any other root of $f(x)$ satisfies an equation of degree atmost $n-1$ over F_1.
If we adjoin again one of root to F_1 so the degree of extension is atmost $n-1$.
In this way degree of extension of a splitting field is atmost $n!$.
Primitive nth root of unity: The generator of the cyclic group of all nth roots of unity is called primitive nth root of unity.

Theorem: Let $\phi : F \to F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be any polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by ϕ to the coefficient of $f(x)$.Let E be the splitting field for $f(x)$ over F and E' be the splitting field for $f'(x)$ over F'. Then the isomorphism ϕ extends to an isomorphism $\sigma : E \to E'$.
Proof: We will prove it by mathematical induction.
Since if $\phi : F \to F'$ be an isomorphism then there exist an isomorphism between two rings that is $F[x]$ to $F'[x]$ by $f(x)$ to $f'(x)$. So irreducible factor of $f(x)$ corresponds to the irreducible factor of $f'(x)$.
now for $n = 1$ that is $f(x)$ is a linear polynomial in $F[x]$ so $f'(x)$ is a linear polynomial in $F'[x]$that is $f(x)$ splits completely into linear factors in $F[x]$ and $f'(x)$ splits completely into linear factors in $F'[x]$ so splitting field for $f(x)$ over F is $E = F$ and splitting field for $f'(x)$ over F' is $E' = F'$. So in this case $\sigma = \phi$ so result is true for $n = 1$.
Now suppose result is true for all polynomial of degree $< n$.
To prove for n
If $f(x)$ has n linear factors then take $E = F$ and $E' = F'$ so again $\sigma = \phi$ hence result is true. Now suppose $p(x)$ is an irreducible factor of $f(x)$ of degree atleast 2 and $p'(x)$ ne an corresponding irreducible factor of $f'(x)$. now let α be a root of $p(x)$ and β be a root of $p'(x)$ the we can extend ϕ to an isomorphism $\sigma' : F(\alpha) \to F(\beta)$.
Let $F_1 = F(\alpha)$ and $F_1' = F(\beta)$ so we have an isomorphism $\phi : F_1 \to F_1'$. and $f(x) = (x - \alpha)f_1(x)$ over F_1 and $f_1(x)$ has degree $n-1$ similarly $f'(x) = (x - \beta)f_1'(x)$ over F_1'. Let E be the splitting field for the polynomial $f_1(x)$ over F_1 and E' be the splitting field for the polynomial $f_1'(x)$ over F_1'. so by induction there exist an isomorphism between E and E' say $\sigma : E \to E'$ extending $\sigma' : F_1 \to F_1'$. hence extending $\phi : F \to F'$.

Corollary: Any two splitting field for a polynomial $f(x) \in F[x]$ are isomorphic.
Proof: Consider $\phi : F \to F$ then splitting field E and E' are isomorphic. That is take identity map.

Algebraic Closure: The field $\bar{F}$ is called algebraic closure of F is $\bar{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\bar{F}$

Algebraically closed: The field K is said to be algebraically closed if every polynomial with coefficient in K has a root in K.

Proposition: $K = \bar{K}$ if and only if K is algebraically closed.
Proof: Let K be algebraically closed field then by definition every polynomial $f(x) \in K[x]$ has a root in K. So if α is a root of $f(x)$ then $\alpha \in K$ so $x - \alpha \in K[x]$.and remaining factor is in $K[x]$ so again root of $f(x)$ is in K hence linear factor is in $K[x]$ so continuing in this way we get the polynomial $f(x)$ splits completely in $K[x]$. and since every element in K has a polynomial in $K[x]$ which is satisfied by that element hence K itself is an algebraic closure of K. That is $K = \bar{K}$.
Conversely if $K = \bar{K}$ then K itself is an algebraic closure of K means every polynomial in $K[x]$ splits completely in $K[x]$ that is Every polynomial has a root in K so K is algebraically closed.

Proposition: Let $\bar{F}$ be an algebraic closure of F. then $\bar{F}$ is algebraically closed.
Proof: Let $\bar{F}$ be an algebraic closure of F. To show $\bar{F}$ is an algebraically closed that is to show every polynomial in $\bar{F}[x]$ has root in $\bar{F}$.
Now let $f(x)$ be a polynomial in $\bar{F}[x]$ and α be a root of $f(x)$ then α generates an algebraic extension $\bar{F}(\alpha)$ of $\bar{F}$ since simple extension is algebraic. and $\bar{F}$ is algebraic over F so $\bar{F}(\alpha)$ is an algebraic over F hence α is algebraic over F so $\alpha \in \bar{F}$. It is true for every root hence $\bar{F}$ is algebraically closed.

Proposition: Let K be an algebraically closed field and let F be a subfield of K. Then the collection of elements $\bar{F}$ of K that are algebraic over F is an algebraic closure of F. an algebraic closure of F is unique up to isomorphism.
Proof: Let K be an algebraically closed field and F be a subfield of K and $\bar{F}$ be a collection of algebraic elements of K over F.
Since every element in $\bar{F}$ is algebraic so $\bar{F}$ is an algebraic extension. Let $f(x)$ be any polynomial in $F[x]$ as K is an algebraically closed field so $f(x)$ splits completely in $K[x]$. Let $x - \alpha$ a linear factor of $f(x)$ which is in $K[x]$. as α is a root of $f(x)$ so α is algebraic over F so $\alpha \in \bar{F}$ so every linear factor of $f(x)$ has coefficient in $\bar{F}[x]$. that is $f(x)$ splits completely in $\bar{F}[x]$ so $\bar{F}$ is algebraic closure of F.

Separable and inseparable extensions:
Separable Polynomial: A polynomial $f(x) \in F[x]$ is called a separable polynomial if it has no multiple root. A Polynomial which is not separable is called inseparable polynomial.

Example: The polynomial $x^2 - 2$ has two distinct roots as $\pm\sqrt{2}$ so this polynomial is separable.and the polynomial $(x^2 - 2)^n$ for $\geq$ is inseparable since it has multiple roots as $\pm\sqrt{2}$

Derivative of polynomial: Let $f(x) \in F[x]$ be a polynomial such that $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ then derivative is defined as $D_xf(x) = a_1 + 2a_2x + ... + na_nx^{n-1}$.

Proposition: A polynomial $f(x)$ has multiple root α if and only of α is a root of $D_xf(x)$. That is $f(x)$ and $D_xf(x)$ are both divisible by the minimal polynomial for α. In particular $f(x)$ is separable if and only if it is relatively prime to its derivative: $(f(x), D_xf(x)) = 1$
Proof: Suppose α is a multiple root of $f(x)$ then we have to show α is also root of $D_xf(x)$. So we can write $f(x)$ as $f(x) = (x - \alpha)^n g(x)$ so $D_xf(x) = n(x - \alpha)^{n-1}g(x) + (x - \alpha)^n D_xg(x)$
so α is a root of $f(x)$
Conversely suppose that α is a root of both $f(x)$ and $D_xf(x)$ then we have to show that α is a multiple root of $f(x)$. Since $f(x)$ can be written as $f(x) = (x - \alpha)h(x)$

So the derivative is $D_xf(x) = h(x) + (x-\alpha)D_xh(x)$ since α is a root of its derivative so $D_xf(\alpha) = 0$ so from the above equation we get $0 = h(\alpha)$ so α is a root of $h(x)$ so $h(x) = (x-\alpha)h_1(x)$ so $f(x) = (x-\alpha)^2h_1(x)$ hence α is a multiple root of $f(x)$.

Corollary: Every irreducible polynomial over a field of characteristic 0 is separable. A polynomial over such a field is separable if and only if it is product of distinct irreducible polynomials.
Proof: Suppose F is a field of characteristic 0. and $p(x) \in F[x]$ an irreducible polynomial of degree n. Then the derivative $D_xp(x)$ is of degree $n-1$. Since $p(x)$ is irreducible so up to constant factors 1 and $p(x)$ are the only factors of $p(x)$. So $D_xp(x)$ must be relatively prime to $p(x)$ so $p(x)$ is irreducible over F. and since distinct irreducible have no common zero so it is separable.

Proposition: Let F be a field of characteristic p. Then for any $a, b \in F, (a+b)^p = a^p + b^p$ and $(ab)^p = a^pb^p$
Proof: Since $(a+b)^p = a^p + C_1^pa^{p-1}b + C_2^pa^{p-2}b^2 + ... + C_i^pa^{p-i}b^i + ... + b^n$
Since $C_i^p = \frac{p!}{i!(p-i)!}$ so every coefficient is divisible by p hence equal to 0.
so $(a+b)^p = a^p + b^p$ and $(ab)^p = a^pb^p$.
Frobenius endomorphism of F: The map $\phi : F \to F$ defined by $\phi(a) = a^p$ which is injective homomorphism is called Frobenius endomorphism.
Corollary: Suppose that F is a finite field of characteristic p then every element of F is a pth power in F.
Proof: Since $\phi : F \to F$ defined by $\phi(a) = a^p$
To show: ϕ is isomorphism. Since this map is homomorphism. and if we have a function from field to field then function is either zero or injective that is if function is not injective then it should be zero map. Now to show it is injective suppose $\phi(a) = \phi(b)$ such that $a \neq b$ let $k = a - b$ as $a \neq b$ so $k \neq 0$ so $\phi(k) = \phi(a-b) = \phi(a) - \phi(b) = 0$ since we can write any element $x\imath F$ as $x = k.k^{-1}.x$ so $\phi(x) = \phi(k.k^{-1}.x) = \phi(k)\phi(k^{-1}.x) = 0$ so this map is zero map. hence it map is not injective then it is zero map but here map is not a zero map so it is injective.
Since function is from finite field to itself so it is surjective.hence this map is an isomorphism so any element a can be of the form a^p.

Proposition Every irreducible polynomial over a finite field is separable. A polynomial over such a field is separable if and only if it is product of distinct irreducible polynomials.
Proof: Let F be a finite field with characteristic p. Suppose $p(x)$ is an irreducible polynomial in $F[x]$ we have to show that it is separable
suppose $p(x)$ is inseparable polynomial then $p(x) = q(x^p)$ for some polynomial $q(x) \in F[x]$. Let $q(x) = a_mx^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ where $a_i \in F$ since every element in F is pth power of element in F so let $a_i = b_i^p$
So $p(x) = q(x^p) = a_m(x^p)^m + a_{m-1}(x^p)^{m-1} + ...a_1(x^p) + a_0$
$= b_m^p(x^p)^m + b_{m-1}^p(x^p)^{m-1} + ... + b_1^p(x^p) + b_0^p$
$= (b_mx^m)^p + (b_{m-1}x^{m-1})^p + ... + (b_1x)^p + b_0^p$
$= (b_mx^m + b_{m-1}x^{m-1} + ... + b_1x + b_0)^p$
so $p(x)$ is the pth power of a polynomial in $F[x]$ which is contradiction to the irreducibility of $p(x)$. And since distinct irreducible do not have common zero's so polynomial is separable.

Perfect Field : A field K of characteristic p is said to be perfect field if every element of K is a pth power in K that is $K = K^p$. Any field of characteristic 0 is also called perfect field.

Separable field: A field K is said to be separable over F if every element of K is the root of a separable polynomial over F. A field which is not separable is inseparable.