Definition 4.1. Given a field extension $L \supset K$ we denote by $Gal(L/K)$ the set of field isomorphisms $f : L \to L$ such that $f(c) = c, c \in K$.

Remark As you will see the set $Gal(L/K)$ has a natural group structure. We call it the *Galois group* of the extension $L \supset K$.

Lemma 4.1. Show that
a) for any $f, g \in Gal(L/K)$ the composition
$f \circ g : L \to L$
belongs to $Gal(L/K)$,
b) the composition law $(f, g) \to f \circ g$ defines a group structure on the set $Gal(L/K)$ with the unit equal to the identity map $Id : l \to l, l \in L$.
c) Let $G = (g_1, g_2, ..., g_n)$ be a finite group. Then for any $g \in G$ the sets $(gg_1, gg_2, ..., gg_n)$ and $(g_1, g_2, ..., g_n)$ coincide.

The proof of Lemma 4.1 assigned as a homework problem.

Let $L \supset K$ be a field extension, $Gal(L/K)$. To any intermediate field extension $F, K \subset F \subset L$ we can assign a subgroup $H(F) \subset Gal(L/K)$ define by

$$H(F) := \{h \in Gal(L/K) | h(f) = f \forall f \in F\}$$

Conversely to any subgroup $H \subset Gal(L/K)$ we can assign an intermediate field extension$F(H), K \subset F(H) \subset L$ where

$$F(H) := \{l \in L | h(l) = l \forall h \in H\}$$

In other words if $A(L, K)$ is the set of fields F in between K and L and $B(L, K)$ is the set of subgroups of G we constructed maps
$\tau : A(L, K) \to B(L, K), F \to H(F)$ and
$\eta : B(L, K) \to A(L, K), H \to F(H)$.

The Main theorem of the Galois theory.
For a finite field extension $L \supset K$
a) $|Gal(L/K)| \leq [L : K]$,
b) if $|Gal(L/K)| = [L : K]$ then the maps $\tau : A(L, K) \to B(L, K), F \to H(F)$ and
$\eta : B(L, K) \to A(L, K), H \to F(H)$ are isomorphisms,
c) $|Gal(L/K)| = [L : K]$ iff the extension $L \supset K$ is *normal* and *separable*,
d) any separable extension $L \supset K$ is contained in a normal extension $M \supset L \supset K$.

To finish the formulation of the main theorem we have to give definitions of normal and separable extensions.

Definition 4.2. A finite field extension $L \supset K$ is *normal* if any irreducible polynomial $p(t) \in K[t]$ which has a root in L has all it roots in L.

Theorem 4.2. An extension $L \supset K$ is normal and finite iff it is a splitting field for some polynomial over K.

Proof. a) Assume that $L \supset K$ is normal and finite. We have to construct a monic polynomial $q(t) \in K[t]$ such which decomposes in $L[t]$ in a product of linear factors

$$q(t) = (t - \alpha_1)^{m_1} \times ... \times (t - \alpha_n)^{m_n}, \alpha_i \in L, 1 \leq i \leq n$$

and $L = K(\alpha_1, ..., \alpha_n)$.

Since the extension $L \supset K$ is finite there exist $\beta_1, ..., \beta_m \in L$ such that $L = K(\beta_1, ..., \beta_m)$. Let $p_j(t) := Irr(\beta_j, K, t) \in K[t]$ be the corresponding minimal polynomials and $q(t) := \prod_{j=1}^{m} p_j(t)$. Since polynomials $p_j(t) \in K[t]$ are irreducible and have roots $\beta_j \in L$ it follows from the normality of $L \supset K$ that all the roots of $p_j(t) \in K[t]$ are in L. So L contains a splitting field of $q(t)$.

On the other hand since $L = K(\beta_1, ..., \beta_m)$ we see that this splitting field of $q(t)$ is equal to L.□

b) Assume now that L is a splitting field of a polynomial $q(t) \in K[t]$. Then $L \supset K$ is finite. We have to show that it is normal.

Let $p(t) \in K[t]$ be an irreducible polynomial and M be a splitting field of the product $q(t)p(t)$. For any root $\alpha \in M$ of $p(t)$ we can consider subfields $K(\alpha) \subset L(\alpha) \subset M$.

Lemma 4.2. The degree $[L(\alpha) : L]$ does not depend on a choice of a root $\alpha \in M$ of $p(t)$.

Proof. Let α_1, α_2 be roots of $p(t)$ in M. We have to show that $[L(\alpha_1) : L] = [L(\alpha_2) : L]$.

Consider extensions $K \subset L \subset L(\alpha_i), i = 1, 2$. The product formula implies that $[L(\alpha_i) : L][L : K] = [L(\alpha_i) : K]$. So for the proof of the equality $[L(\alpha_1) : L] = [L(\alpha_2) : L]$ it is sufficient to show that $[L(\alpha_1) : K] = [L(\alpha_2) : K]$.

It is clear [see Lemma 3.4] that $L(\alpha_i)$ is a splitting field for $q(t)$ over $K(\alpha_i)$. Since [see Lemma 2.4] each of the fields $K(\alpha_i)$ is isomorphic to the quotient ring $K[t]/(p(t))$ there exists and isomorphism

$\eta : K(\alpha_1) \to K(\alpha_2)$ such that $\eta(c) = c, c \in K$.

It follows now from Theorem 3.1 that the the isomorphism $\eta : K(\alpha_1) \to K(\alpha_2)$ can be extended to an isomorphism $\tilde{\eta} : L(\alpha_1) \to$

$L(\alpha_2)$. But the existence of an isomorphism $\tilde{\eta} : L(\alpha_1) \to L(\alpha_2)$ implies the equality $[L(\alpha_1) : K] = [L(\alpha_2) : K]$. Lemma 4.3 is proven.□

Now we can finish the proof of Theorem 4.2. Let $p(t) \in K[t]$ be an irreducible polynomial which has a root $\alpha \in L$. We want to show that all the roots of $p(t)$ in M are actually in L. Let $\beta \in M$ be a root of $p(t)$. It follows from Lemma 4.2 that $[L(\alpha) : L] = [L(\beta) : L]$. Since $\alpha \in L$ we have $[L(\alpha) : L] = 1$. Therefore $[L(\beta) : L] = 1$. So $\beta \in L$.□

Definition 4.3. a) An irreducible polynomial $p(t) \in K[t]$ is *separable* if it does not have multiple roots in a splitting field,

b) A finite field extension $L \supset K$ is *separable* if for any $\alpha \in L$ the minimal polynomial $p(t) = Irr(\alpha, K, t) \in K[t]$ of α is separable,

c) We denote by $D : K[t] \to K[t]$ the K-linear map such that $D(t^n) := nt^{n-1}$,

d) we say that a field K of characteristic $p > 0$ is *perfect* if for any $\alpha \in K$ the equation $t^p - \alpha = 0$ has a solution in K.

We start with the following useful results.

Lemma 4.3. a) For any $q(t), r(t) \in K[t]$ we have

$$D(qr)(t) = Dq(t)r(t) + q(t)Dr(t)$$

b) is If K is a field of characteristic zero and $q(t) \in K[t]$ is such that $Dq(t) = 0$ the $q(t) = c \in K$,

c) let K be a perfect field of characteristic p. Then any polynomial $q(t) \in K[t]$ such that $Dq(t) = 0$ has a form $q(t) = r^p(t)$ for some $r(t) \in K[t]$.

The proof of Lemma 4.3 assigned as a homework problem.

Lemma 4.4. A polynomial $q(t) \in K[t]$ has a multiple root in it's splitting field iff polynomials $q(t)$ and $Dq(t)$ have a common factor of degree > 0.

Proof of Lemma 4.4. a) Suppose that $q(t) \in K[t]$ has a multiple root. We want to show that $q(t), Dq(t) \in K[t]$ are not relatively prime. Suppose that they are relatively prime. Then there exists $a(t), b(t) \in K[t]$ such that $a(t)q(t) + Dq(t)b(t) = 1$.

On the other hand if $q(t) \in K[t]$ has a multiple root $\alpha \in L$ we have

$$q(t) = (t - \alpha)^2 r(t), r(t) \in L[t]$$

But then

$$Dq(t) = 2(t - \alpha)r(t) + (t - \alpha)^2 Dr(t)$$

So

$(t-\alpha)|q(t)$ and $(t-\alpha)|Dq(t)$. So α is a root of the polynomial $a(t)q(t)+Dq(t)b(t)$. But this is impossible since $a(t)q(t)+Dq(t)b(t) = 1$.

The contradiction shows that $q(t), Dq(t) \in K[t]$ are not relatively prime.

b) Assume now that polynomials $q(t)$ and $Dq(t)$ have a common factor $r(t)$ of degree > 0. Let $\alpha \in L$ be a root of $r(t)$. I claim that it is a multiple root of $q(t)$.

Assume this is not true. Since $r(t)|q(t)$ we know that α is a root of $q(t)$. If it is not a multiple root of $q(t)$ then

$$q(t) = (t-\alpha)s(t), r(t) \in L[t]$$

where α is not a root of $s(t)$. But

$$Dq(t) = (t-\alpha)Dr(t) + s(t)$$

So

$$Dq(\alpha) = s(\alpha) \neq 0$$

This contradiction proves the Lemma.□

Theorem 4.3. If $p(t) \in K[t]$ is an irreducible polynomial such that $Dp(t) \neq 0$ then the polynomial $p(t)$ is separable.

Proof. Suppose that an irreducible polynomial $p(t) \in K[t]$ is such that $Dp(t) \neq 0$ and $L \supset K$ is a splitting field of $p(t)$. We show that an assumption that $p(t)$ has a multiple root in $\alpha \in L$ leads to a contradiction.

Let $r(t) \in K[t]$ be the greatest common divisor of $p(t)$ and $Dp(t)$. As follows from Lemma 4.5 $(t-\alpha)|r(t)$ in $L[t]$. Therefore deg $r(t)$ is > 0. On the other hand deg $r(t) \leq$deg $Dp(t) <$deg $p(t)$. Since $r(t) \in K[t]$ is the greatest common divisor of $p(t)$ and $Dp(t)$ it divides $p(t)$. But is impossible since $p(t)$ is irreducible.□

Corollary . Let K be a field of characteristic zero. Then

a) Any irreducible polynomial over a field of characteristic zero is separable,

b) a finite field extension $L \supset K$ is separable.

Really if $\mathrm{ch}(K) = 0, q(t) \in K[t]$ is such that $Dq(t) = 0$ then, by Lemma 4.3 b),$q(t) = 0$.

We start the proof of the Main theorem with the following result of Dedekind.

Definition 4.4. Let K, L be fields and $f_1, ..., f_n : K \to L$ be field homomorphisms from K to L. We say that the homomorphisms are

linearly independent if for any $\alpha_1, ..., \alpha_n \in L$ such that $(\alpha_1, ..., \alpha_n) \neq (0, ..., 0)$ there exists $\beta \in K$ such that
$\sum_{i=1}^{n} \alpha_i f_i(\beta) \neq 0$.

Lemma 4.5. Any set $f_1, ..., f_n : K \to L$ of distinct field homomorphisms is linearly independent.

Proof. We assume that $f_1, ..., f_n : K \to L$ are linearly dependent and show that this assumption leads to a contradiction.

If $f_1, ..., f_n : K \to L$ are linearly dependent then there exists
$\alpha_1, ..., \alpha_n \in L$ such that $(\alpha_1, ..., \alpha_n) \neq (0, ..., 0)$ and for all $\beta \in K$ we have
$\sum_{i=1}^{n} \alpha_i f_i(\beta) = 0$.
Let $m \leq n$ be the smallest number such that we can find $\alpha_1, ..., \alpha_m \in L$ such that $(\alpha_1, ..., \alpha_m) \neq (0, ..., 0)$ and for all $\beta \in K$ we have

$$(\star) \sum_{i=1}^{m} \alpha_i f_i(\beta) = 0$$

If $m = 1$ then we have $\alpha_1 f_1(\beta) = 0$ for all $\beta \in K$. In particular $\alpha_1 f_1(1) = 0$. But $f_1(1) = 1$. So we have $\alpha_1 = 0$. But this equality would contradict our assumption.

So we can assume that $m > 1$. Since $f_1 \neq f_m$ we can find $\gamma \in K$ such that $f_1(\gamma) \neq f_m(\gamma)$. The identity

$$\sum_{i=1}^{m} \alpha_i f_i(\beta) = 0, \beta \in K$$

implies the identity

$$\sum_{i=1}^{m} \alpha_i f_i(\beta\gamma) = 0, \beta \in K$$

Since $f_i : K \to L, 1 \leq i \leq n$ are field homomorphisms we see that

$$(\star\star) \sum_{i=1}^{m} \alpha_i f_i(\beta) f_i(\gamma) = 0, \beta \in K$$

If we multiply $(\star)$ by $f_m(\gamma)$ and subtract the result from $(\star\star)$ we obtain an identity

$$\sum_{i=1}^{m-1} \alpha_i' f_i(\beta) = 0, \beta \in K, \alpha_i' := \alpha_i(f_i(\gamma) - f_n(\gamma))$$

By the construction $\alpha_i' \neq 0$. But the existence of such an identity contradicts to our choice of m. This contradiction proves Lemma 4.5.
$\square$