Theorem 5.1. Let $G \subset Gal(L/K)$ be a finite subgroup, $L^G := \{\alpha \in L | g(l) = l, \forall g \in G\}$. Then $[L : L^G] = |G|$ where $|G|$ is the order of the group G.

Proof. Let $n = |G|, G = (g_1, g_2, ..., g_n), m = [L : L^G]$ and $(\alpha_1, ..., \alpha_m)$ be a basis of L as an L^G-vector space. We have to show that $m = n$.

We first show that $m \geq n$. Suppose $m < n$. We denote by

$$A : L^n \to L^m$$

an L-linear map given by

$$(x_1, ..., x_n) \to (\gamma_1, ..., \gamma_m), \gamma_j := \sum_{i=1}^{n} x_i g_i(\alpha_j)$$

Since $m < n$ we know that $Ker(A) \neq \{0\}$. So there exist $\{x_1, ..., x_n\} \subset L$ such that $(x_1, ..., x_n) \neq (0, ..., 0)$ and for all $j, 1 \leq j \leq m$ we have

$$\sum_{i=1}^{n} x_i g_i(\alpha_j) = 0$$

Since $(\alpha_1, ..., \alpha_m)$ an L^G-basis of L we see that for any $\alpha \in L$ we have $\sum_{i=1}^{n} x_i g_i(\alpha) = 0$. In other words field homomorphisms $g_1, ..., g_n : L \to L$ are linearly dependent. But this is not possible [see the Dedekinds's lemma]. So $m \geq n$.

Now we show that $m \leq n$. Suppose that $m > n$. Then we can find $n+1$ elements $(\beta_1, ..., \beta_{n+1}) \in L$ which are linearly independent over L^G. Consider an L-linear map $B : L^{n+1} \to L^n, B(\delta_1, ..., \delta_{n+1}) = (\gamma_1, ..., \gamma_n)$ where

$$\gamma_i := \sum_{j=1}^{n+1} \delta_j g_i(\beta_j), 1 \leq i \leq n$$

Since $m > n$ we see that $Ker(B) \neq \{0\}$. Therefore there exist $\delta_1, ..., \delta_{n+1} \in L$ such that $(\delta_1, ..., \delta_{n+1}) \neq (0, ..., 0)$ and

$$\sum_{j=1}^{n+1} \delta_j g_i(\beta_j) = 0 \forall i, 1 \leq i \leq n$$

Now we will argue as in the process of the proof of the Dedekinds's lemma. So we choose $\delta_1, ..., \delta_{n+1} \in L$ such that $(\delta_1, ..., \delta_{n+1}) \neq (0, ..., 0)$ and

$$(\star)\sum_{j=1}^{n+1}\delta_j g_i(\beta_j)=0, 1\leq i\leq n$$

in such a way that the minimal number of δ_i are different from 0. After renumbering we can assume that $(\delta_1,...,\delta_r)\neq(0,...,0)$

$$(\star)\sum_{j=1}^{r}\delta_j g_i(\beta_j)=0, 1\leq i\leq n$$

and that for any sequence $\delta'_j, 1\leq j\leq r-1$ such that $(\delta'_1,...,\delta'_{r-1})\neq(0,...,0)$ there exists $i, 1\leq i\leq n$ such that

$$\sum_{j=1}^{r-1}\delta'_j g_i(\beta_j)\neq 0$$

Let us apply $g\in G$ to $(\star)$. We will get a system of equalities

$$(\star_g)\sum_{j=1}^{r}g(\delta_j)gg_i(\beta_j)=0, 1\leq i\leq n$$

As follows from Lemma 4.2c) the set $\{gg_i\}, 1\leq i\leq n$ coincides with the set $\{g_i\}, 1\leq i\leq n$. Therefore the system $(\star)_g$ of equalities is equivalent to the system

$$(\star\star)_g\sum_{j=1}^{r}g(\delta_j)g_i(\beta_j)=0, 1\leq i\leq n$$

If we multiply $(\star)$ by $g(\delta_r)$, multiply $(\star\star)$ by δ_r and subtract we obtain the system

$$(\star\star\star)_g\sum_{j=1}^{r-1}(g(\delta_r)\delta_j-\delta_r g(\delta_j))g_i(\beta_j)=0, 1\leq i\leq n$$

This is system of equations like $(\star)$ but with fewer terms. So our choice of r implies that for any $g\in G$ all the coefficients

$$g(\delta_r)\delta_j-\delta_r g(\delta_j), 1\leq j\leq r-1$$

are equal to zero. But this implies that for all $g\in G$ we have

$c_j=g(c_j), 1\leq j<r$ were $c_j:=\delta_j\delta_r^{-1}$. By the definition of the field L^G we know that $c_j\in L^G, 1\leq j<r$. Therefore the first of the equalities $(\star)$ implies the equality $\sum_{j=1}^{r}\delta_r c_j\beta_j=0$. Since $\delta_r\neq 0$ we have $\sum_{j=1}^{r}c_j\beta_j=0$.

But such an equality would imply that the elements $(\beta_1,...,\beta_r)\in L$ are linearly dependent over L^G. But this is not possible since the elements $(\beta_1, ..., \beta_{n+1}) \in L$ are linearly independent over L^G. So you see that the assumption $m > n$ also leads to a contradiction and we have $m = n$.□

Definition 5.1. Let $L \supset K$ be a finite field extension. A *normal closure* of $L : K$ is an extension N of L such that

a) $N : K$ is normal

and

b) if F is a field such that $L \subset F \subset N$ and $F : K$ is normal then $F = N$.

Definition 5.2. If M, N be two extensions of K and $f : M \to N$ a field homomorphism we say that f is a K-homomorphism if $f(c) = c, \forall c \in K$.

Lemma 5.1. a) for any finite field extension $L \supset K$ there exists normal closure N of $L : K$ such that $[N : K] < \infty$,

b) if $N \supset L$ is another normal closure of $L : K$ then the extensions $M : K$ and $N : K$ are isomorphic.

Proof of a). Let $\alpha_i, 1 \leq i \leq n$ be a basis of L over K. For any $i, 1 \leq i \leq n$ we define $p_i(t) := Irr(\alpha_i, K, t) \in K[t]$ and then define $q(t) := \prod_{i=1}^n p_i(t)$. Let N be a splitting field for $q(t)$ over L. Since $L = K(\alpha_1, ..., \alpha_n)$ we see that N is a splitting field for $q(t)$ over K. It follows now from Theorem 4.2 that $N : K$ is normal.

To prove that N is a normal closure of $L : K$ we have to show that for any $F, L \subset F \subset N$ such that $F : K$ is normal we have $F = N$. Since $F \supset L$ we know that for any $i, 1 \leq i \leq n$ the irreducible polynomial $p_i(t), 1 \leq i \leq n$ has a root α_i in F. Since $F : K$ is normal all the roots of $p_i(t)$ are in F. Therefore all the roots of $q(t)$ are in F. Since N is a splitting field for $q(t)$ over K we see that $F = N$.□

Proof of b). Suppose that N, M are two normal closures of $L : K$. Then as follows from the proof of a) both N and M are splitting fields of $q(t)$. It follows now from Theorem 3.1 that there exists a K-isomorphism $f : M \to N$.□

Lemma 5.2. a) Let $K \subset L \subset M \subset N$ be finite field extensions such that M is a normal closure of $L : K$ and $f : L \to N$ be a K-homomorphism. Then $Im(f) \subset M$,

b) Suppose $L \supset K$ is a finite field extension, and $M \supset L$ a normal extension containing L. Then for any K-homomorphism $g : L \to M$ there exists an isomorphism $\tilde{g} : M \to M$ such that $\tilde{g}(\alpha) = g(\alpha) \forall \alpha \in L$,

c) Suppose $L \supset K$ is a finite field extension, and $M \supset L$ a normal extension containing L such that for any K-homomorphism $f : L \to M$ we have $Im(f) \subset L$. Then the extension $L \supset K$ is normal,

d) If $K \subset L \subset M$ are finite field extensions such that $M : K$ is normal then $M : L$ is also normal.

The proof of Lemma 5.2 assigned as a homework problem.

Definition 5.3. Let $L \supset K$ be a finite extension, $M \supset L$ a normal extension containing L.

a) We denote by $H(L/K)$ the set of K-homomorphisms of L to M.

Remark. It follows from Lemma 5.2 this set does not depend on a choice of a normal extension M.

b) we denote by $[L : K]_s$ the number of elements in the set $H(L/K)$ and say that $[L : K]_s$ is the *separable degree* of L over K.

Lemma 5.3. Let $K \subset F \subset L$ be finite field extensions. Then $[L : K]_s = [L : F]_s[F : K]_s$

Proof . For any field homomorphism $g \in H(F/K)$ we denote by $H(L/K)_g \subset H(L/K)$ the subset of field homomorphism $f \in H(L/K)$ such that $f(\alpha) = g(\alpha)$ for all $\alpha \in F$. It is clear that $H(L/K)_{Id} = H(L/F)$ and that

$$H(L/K) = \cup_{g \in H(F/K)} H(L/K)_g$$

Therefore

$$[L : K]_s = \sum_{g \in H(F/K)} |(H(L/K)_g|$$

Claim. For any $g \in H(F/K)$ we have $|(H(L/K)_g| = |H(L/K)_{Id}|$.

Proof of the Claim. Choose $g \in H(F/K)$. As follows from Lemma 5.2 there exists an isomorphism $\tilde{g} : M \to M$ such that $\tilde{g}(\alpha) = g(\alpha) \forall \alpha \in L$. It is clear that

$$\tilde{g}(H(L/K)_{Id}) = (H(L/K)_g \square$$

Now we can finish the proof of Lemma 5.3. Since $H(L/K)_{Id} = H(L/F)$ we have $|(H(L/K)_{Id}| = [L : F]_s$ and it follows from the Claim that $|(H(L/K)_g| = [L : F]_s \forall g \in H(F/K)$. So $[L : K]_s = [L : F]_s[F : K]_s$.$\square$

Theorem 5.2. Let $L \supset K$ be a finite extension. Then

a)$[L : K] \geq [L : K]_s$

b) the extension $L \supset K$ is separable iff $[L : K] = [L : K]_s$.

Proof . Consider first the case when $L \supset K$ is an elementary extension. That is there exists $\alpha \in L$ such that $L = K(\alpha)$. As follows from Lemma 3.3 the separable degree $[L : K]_s$ is equal to the number of roots of the polynomial $p(t) := Irr(\alpha, K, t)$ in M. We know that $\deg(p(t)) = [L : K]$,that $[L : K]_s \leq \deg(p(t)) = [L : K]$ and that $[L : K] = [L : K]_s$ iff the polynomial $p(t)$ is separable. So the Theorem 5.2 is true for elementary extensions.

Now we prove the Theorem 5.2 by induction in $[L : K]$. If $[L : K] = 1$ then $L = K$ and there is nothing to prove. So assume $[L : K] > 1$, choose $\alpha \in L - K$ and write $p(t) := Irr(\alpha, K, t)$.

Since $[L : K(\alpha)] < [L : K]$ we know from the inductive assumption that $[L : K(\alpha)]_s < [L : K(\alpha)]$. It follows now from Lemma 5.4 that

$$[L : K]_s = [L : K(\alpha)]_s[K(\alpha) : K]_s \leq [L : K(\alpha)][K(\alpha) : K]$$

This prove the part a).

Assume now that $[L : K] = [L : K]_s$. We want to show that the extension $L \supset K$ is separable. Since we now that

$[L : K(\alpha)] \leq [L : K(\alpha)]_s$ and $[K(\alpha) : K]_s \leq [K(\alpha) : K]$ the equality $[L : K] = [L : K]_s$ implies the equality $[K(\alpha) : K] = [K(\alpha) : K]_s$. So it follows from the beginning of the proof of Theorem 5.2 that the polynomial $p(t) := Irr(\alpha, K, t)$ is is separable. We see that for any $\alpha \in L$ the polynomial $p(t) := Irr(\alpha, K, t)$ is is separable. Therefore the extension $L \supset K$ is separable.

Assume now that the extension $L \supset K$ is separable. We want to show that $[L : K] = [L : K]_s$. We start with the following result.

Lemma 5.4. Let $K \subset F \subset L$ be finite extensions. If the extension $L : K$ is separable then the extensions $L : F$ and $F : K$ are also separable.

Proof . Suppose the extension $L : K$ is separable. It follows from the definition that the extension $F : K$ is also separable.

So we have. Let M be a normal closure of $L : K$. To show that the extension $L : F$ is separable we have to show that for any $\alpha \in L$ the polynomial

$r(t) := Irr(\alpha, F, t) \in F[t]$ has simple roots in M. Let

$R(t) := Irr(\alpha, K, t) \in K[t]$. Since $L : K$ is separable we know that the polynomial $R(t)$ has simple roots in M. On the other hand $r(t)|R(t)$, because R is a polynomial in $K[t] \subset F[t]$ with $R(\alpha) = 0$ but r is the *minimal* polynomial of α over F so it generates the ideal of polynomials in $F[t]$ vanishing at α. So all the roots of $r(t)$ are simple.$\square$

Now we can finish the proof of Theorem 5.2. Let $L \supset K$ be a separable extension. We want to show that $[L : K] = [L : K]_s$. Since $[L : K]_s = [L : K(\alpha)]_s[K(\alpha) : K]_s$ and filed extensions $L : K(\alpha)$

and $[K(\alpha) : K$ are separable the equality follows from the inductive assumption.□

Lemma 5.5. a). Let $K \subset F \subset L$ be finite extensions. If the extensions $L : F$ and $F : K$ are separable then the extension $L : K$ is also separable.

b) If $K \subset L$ is a finite separable extension then the normal closure M of $L : K$ is separable over K.

The proof of Lemma 5.5.is assigned as a homework problem.

Definition 5.4. Let $L \supset K$ be a finite normal field extension, $G := Gal(L/K)$ be the Galois group of $L : K$. To any intermediate field extension $F, K \subset F \subset L$ we can assign a subgroup $H(F) \subset Gal(L/K)$ define by

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

By the definition $H(F) = Gal(L : F)$.
Conversely to any subgroup $H \subset Gal(L/K)$ we can assign an intermediate field extension $L^H, K \subset L^H \subset L$ where

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

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
$\eta : B(L, K) \to A(L, K), \tau : H \to L^H$.

The Main theorem of the Galois theory.
Let $L \supset K$ a finite normal separable field extension . Then
a) $|Gal(L/K)| = [L : K]$,
b) $L^G = K$
c) the maps $\tau : A(L, K) \to B(L, K), F \to H(F)$ and
$\eta : B(L, K) \to A(L, K), H \to L^H$ are one-to-one and onto.

Proof. The part a) follows from Theorem 5.2.

Proof of b). Let $F := L^H$. As follows from a), the product formula and Theorem 5.1 we have $[F : K] = [L : K]/[L : F] = 1$. So $F = K$.

Proof of c). We have to show that
i) $\tau \circ \eta = Id_{A(L,K)}$ and
ii) $\eta \circ \tau = Id_{B(L,K)}$.

Proof of i). Let $F \in A(L, K)$ be subfield of L containing $K, H(F) := \eta(F) \subset G$. Since the extension $L \supset K$ is normal it follows from Lemma 5.2 that the extension $L \supset F$ is also normal. So it follows from a) that

$|H(F)| = [L : F]$. Since $H(F) = Gal(L : F)$ it follows from b) that $L^H = F$. So $\tau \circ \eta(F) = F$.

ii) Let $U \subset B(L, K)$ be a subgroup of G and $F := L^U$. Define $H := H(F)$. We want to show that $U = H$. By the definition, for any $u \in U, \alpha \in F$ we have $u(\alpha) = \alpha$. In other words $U \subset H$. As follows from Theorem 5.1 we have $[L : F] = |U|$. On the other hand, it follows from i) that $[L : F] = |H|$. So $|U| = |H|$ and the inclusion $U \subset H$ implies that $U = H$.$\square$