Theorem 7.1. 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. Let M be a normal closure of $L : K$. Consider first the case when $L \supset K$ is an elementary extension. In this case there exists $\alpha \in L$ such that $L = K(\alpha)$. We know that $\deg(p(t)) = [L : K]$ and it follows from Lemma 3.3 that the separable degree $[L : K]_s$ is equal to the number of roots of the polynomial $p(t) := Irr(\alpha, K, t)$ in M. Since the number of roots of the polynomial $p(t)$ in M is not bigger then it's degree we see that $[L : K]_s \leq \deg(p(t)) = [L : K]$. Moreover $[L : K] = [L : K]_s$ iff the polynomial $p(t)$ is separable. So the Theorem 7.1 is true for elementary extensions.

Now we prove the Theorem 7.1 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 6.5 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. In other words we want to show that for any $\alpha \in L$ the extension $K(\alpha) : K$ is separable. But we know that $[L : K(\alpha)] \leq [L : K(\alpha)]_s$ and $[K(\alpha) : K]_s \leq [K(\alpha) : K]$. Therefore the equality $[L : K] = [L : K]_s$ implies the equality

$[K(\alpha) : K] = [K(\alpha) : K]_s$ and it follows from the beginning of the proof of Theorem 5.2 that the polynomial $p(t) := Irr(\alpha, K, t)$ is 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 7.1. 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 immediately from the definition that the extension $F : K$ is also separable. So it is sufficient to show that the extensions $L : F$ is separable.

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 $r(t)|R(t)$. So all the roots of $r(t)$ are simple.□

Now we can finish the proof of Theorem 7.1. 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 the field extensions $L : K(\alpha)$ and $K(\alpha) : K$ are separable the equality follows from the inductive assumption.□

Lemma 7.2. 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 7.2 is assigned as a homework problem.

Definition 7.1. 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 $F, K \subset F \subset L$ 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) $\tau \circ \eta = Id_{A(L,K)}$
d) $\eta \circ \tau = Id_{B(L,K)}$.

Proof. The part a) follows from Theorem 7.1.

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). 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 6.1. c) 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 $\tau \circ \eta(F) = F$.

Proof of d) 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 c) that $[L : F] = |H|$. So $|U| = |H|$ and the inclusion $U \subset H$ implies that $U = H$.□

Lemma 7.3. For a finite field extension $L \supset K$ the following three conditions are equivalent

a) $L : K$ is normal,

b) for every extension M of K containing L and every K-homomorphism $f : L \to M$ we have $Im(f) \subset L$ and f induces an automorphism of L

c) there exists a normal extension N of K containing L such that for every K-homomorphism $f : L \to N$ we have $Im(f) \subset L$,

.

Proof. We show that *a*) ⇒ *b*) ⇒ *c*) ⇒ *a*).

a) ⇒ *b*).We first show that for any $\alpha \in L$ we have $f(\alpha) \in L$. Let $p(t) = Irr(\alpha, K, t) \in K[t]$ be the irreducible polynomial monic which has a root $\alpha \in L$. Since L is normal the polynomial splits in $L[t]$ to a product of linear factors. So all it roots belong to L. Since $f : L \to M$ is K-homomorphism we know that $f(\alpha) \in M$ is a root of $p(t)$. So $f(\alpha) \in L$.

To show that f induces an automorphism of L we observe that dim $_K L < \infty$. Since f is an imbedding it induces an automorphism of L.

b) ⇒ *c*). Follows from Lemma 5.1.

c) ⇒ *a*). Let $p(t) = Irr(\alpha, K, t) \in K[t]$ be the irreducible polynomial monic which has a root $\alpha \in L$. We want to show that all his roots in a normal closure N of $L : K$ are actually in L. Let $\beta \in N$ be a root of $p(t)$. As follows from Lemma 6.1 a) there exists an automorphism f of N such that $f(\alpha) = \beta$. Since by c) we have $f(L) \subset L$ we see that $\beta \in L$.□

lemma 7.4. a) Let $L \supset K$ be a finite extension, $F, E \subset L$ subfields containing K and $EF \subset L$ be the minimal subfield of L containing both E and F. If both extensions $E : K$ and $F : K$ are separable then the extension $EF : K$ is separable,

b) $L_s := \{\alpha \in L |$ the extension $K(\alpha) : K$ is separable$\}$. Then $L_s \subset L$ is a subfield,

c) $[L_s : K] = [L : K]_s$

I'll leave the proof of lemma 7.4 as a homework.

Definition 7.2 Let $L \supset K$ be a finite extension of characteristic $p > 0$. We say that an element $\alpha \in L$ is *purely inseparable* over K if there exists $n \geq 0$ such that $\alpha^{p^n} \in K$.

Lemma 7.5. Let $L \supset K$ be a finite extension and $p :=$ch (K)> 0. The following four conditions are equivalent:

P1. $L_s = K$,

P2. every element $\alpha \in L$ is purely inseparable,

P3. for every element $\alpha \in L$ we have $Irr(\alpha, K, t) = t^{p^n} - a$ for some $n \geq 0, a \in K$,

P4. there exists a set of generators $\alpha_1, ..., \alpha_m \in L$ of L over K [that is $L = K(\alpha_1, ..., \alpha_m)$] such that all elements $\alpha_i, 1 \leq i \leq m$ are purely inseparable over K.

P1 implies P2. Let M be a normal closure of L over K. Assume P1. Fix $\alpha \in L$. We want to show that every element $\alpha \in L$ is purely inseparable. As follows from Lemma 5.3 we have $[K(\alpha) : K]_s = 1$. Let $p(t) := Irr(\alpha, K, t)$. As follows from Lemma 3.3 to the number of distinct roots of $p(t)$ in M is equal to $[K(\alpha) : K]_s$. So $p(t) = (t - \alpha)^m$.

I claim that there exists $n \geq 0$ such that $m = p^n$.

Really write $m = p^n r$ where r is prime to p. Then we have

$$p(t) = ((t - \alpha)^{p^n})^r = (t^{p^n} - \alpha^{p^n})^r = t^{p^n r} - r\alpha^{p^n} t^{p^n (r-1)r} + ...$$

where ... stay for lower terms.

Since $p(t) \in K[t]$ we see that $r\alpha^{p^n} \in K$. Since r is prime to p we can divide by r. Therefore $\alpha^{p^n} \in K$ and $p(t) = (t - \alpha)^{p^n}$. Since $p(t) \in K[t]$ we see that $\alpha^{p^n} \in K$.$\square$

I'll leave for you to show that P2 implies P3 and that P3 implies P4.

P4 implies P1. We have to show that any K-homomorphism $f : L \to M$ is equal to the identity. Since $L = K(\alpha_1, ..., \alpha_m)$ it is sufficient to show that

$f(\alpha_i) = \alpha_i, 1 \leq i \leq m$. Since the elements α_i are purely inseparable for any $i, 1 \leq i \leq n$ there exists $n \geq 0$ such that α_i is a root of the polynomial $p(t) = t^{p^n} - a$. But then $p(t) = (t - \alpha_i)^{p^n}$ and therefore α_i is it's only root. Since $f(\alpha_i)$ is also a root of $p(t)$ we see that $f(\alpha_i) = \alpha_i$.□

Definition 7.2. Let $L \supset K$ be a finite extension.

a) We say that the extension $L \supset K$ is *purely inseparable* if it satisfies the conditions of Lemma 7.6,

b) we define $[L : K]_i := [L : L_s] = [L : K]/[L : K]_s$.

Now we finish the proof of Theorem 2.1. Remind the Definition 2.3.

We say that a finite extension $L \supset K$ satisfies the condition $\star$ if there exists only a finite number of subfields $F \subset L$ containing K.

Theorem 7.2. a) A finite extension $L \supset K$ is elementary iff it satisfies the condition $\star$,

b) any finite separable extension $L \supset K$ is elementary.

Proof of a) We have to show that

i) if $L \supset K$ is a finite extension of K which satisfies the condition $\star$ then the extension $L \supset K$ is elementary

and

ii) if $L \supset K$ is an elementary extension then it satisfies the condition $\star$.

The part i) was proven in the second lecture. Now we will proof the part ii).

So assume that $L = K(\alpha)$. We want to show that the set A of intermediate fields $F, K \subset F \subset L$ is finite.

Let $M \supset L$ be a splitting field of $p(t) := Irr(\alpha, K, t) \in K[t]$. Then

$$p(t) = \prod_{i=1}^{s} (t - \alpha_i)^{m_i}, \alpha_i \in M, m_i > 0$$

Let B be the set of monic polynomials in $r(t) \in M[t]$ which divide $p(t)$. Since any such monic polynomials in $r(t) \in M[t]$ has a form

$$r(t) = \prod_{i=1}^{s} (t - \alpha_i)^{n_i}, \alpha_i \in M, 0 \leq n_i \leq m_i > 0$$

we see that the set B is finite.

So for a proof of ii) it is sufficient to construct an imbedding of the set A into the set B.

Given an intermediate field $F, K \subset F \subset L$ consider the polynomial $r_F(t) := Irr(\alpha, F, t) \in F[t]$. As we know $\deg r_F(t) = [F(\alpha) : F]$. Since $F(\alpha) \supset K(\alpha) = L$ we see that $F(\alpha) = L$ and $\deg(r_F(t)) = [L : F]$.

Since $p(\alpha) = 0$, the polynomial $r_F(t) \in F[t]$ is irreducible in $F[t]$ and $r_F(\alpha) = 0$ we see that $r_F(t)|p(t)$. So $r_F(t) \in B$ and we constructed a map $A \to B$. To finish the proof of ii) it is sufficient to show that we can reconstruct the field F if we know the polynomial $r_F(t)$.

Let $F_0 \subset L$ be the field generated over K by the coefficients of the polynomial $r_F(t)$. I claim that $F = F_0$.

By the construction we have $r_F(t) \in F_0[t]$. The inclusion $r_F(t) \in F[t]$ implies that $F_0 \subset F$. Since the polynomial $r_F(t) \in F[t]$ is irreducible it is also irreducible in $F_0[t]$. So we see that $\text{deg} r_F(t) = [L : F_0]$. Now the inclusion $F_0 \subset F$ implies that $F_0 = F$.

By the definition the field F_0 is is determined by the knowledge of the polynomial $r_F(t)$.$\square$

To prove b) we have to show that any finite separable extension $L \supset K$ satisfies the condition $\star$.

In the case when K is a finite field there is nothing to prove. So we assume that the field K is infinite.

Since the extension $L \supset K$ is finite we can find $\alpha_1, ..., \alpha_n \in L$ such that that $L = K(\alpha_1, ..., \alpha_n)$. We have to show that there exists $\beta \in L$ such that $L = K(\beta)$. I'll prove the result for $n = 2$. The general case follows easily by induction. [We have run through analogous reduction to the case $n = 2$ a number of times] .

So assume that $L = K(\alpha_1, \alpha_2)$. Let M be a normal closure of $L, d := [L : K]$. Since the extension $L \supset K$ is separable it follows from Theorem 5.2 that there exists d distinct field homomorphisms $f_i : L \to M, 1 \leq i \leq d$. Consider the polynomial

$$q(t) := \prod_{1 \leq i \neq j \leq d} (f_i(\alpha_1) + tf_i(\alpha_2) - f_j(\alpha_1) - tf_j(\alpha_2))$$

By the construction $f_i \neq f_j$ for $i \neq j$. So $q(t) \neq 0$ and the polynomial $q(t)$ has only finite number of roots. Since $|K| = \infty$ there exists $c \in K$ such that $q(c) \neq 0$. In other words $f_i(\alpha_1) + tf_i(\alpha_2) \neq f_j(\alpha_1) + tf_j(\alpha_2)$ if $1 \leq i \neq j \leq d$. Let $\beta := \alpha_1 + c\alpha_2$ for $1 \leq i \neq j \leq d, L' := K(\beta)$. We want to show that $L' = L$.

Let Let $g_i : L' \to M, \leq i \leq d$ be the restrictions of f_i to $L' \subset L$. Since $f_i(\alpha) \neq f_j(\alpha)$ for $1 \leq i \neq j \leq d$ we see that the field homomorphisms $g_i : L' \to M$ are distinct. Therefore $[L' : K]_s \geq d = [L : K]$. It follows now from Theorem 5.2 that $[L' : K] \geq [L : K]$. Since $L' \subset L$ this is possible only if $L' = L$.$\square$