Lemma 6.1. Let $L \supset K$ be a normal extension and F an intermediate field $K \subset F \subset L$.

a) Let $p(t) \in K[t]$ be an irreducible polynomial, $\alpha, \alpha' \in L$ such that $p(\alpha) = p(\alpha') = 0$. Then there exists an automorphism $\eta \in Gal(L/K)$ such that $\eta(\alpha) = \alpha'$,

b) Let $L \supset K$ be a normal extension,and $\eta_F : F \to L$ a K-homomorphism. Then there exists an automorphism $\eta \in Gal(L/K)$ such that $\eta(\beta) = \eta_F(\beta), \forall \beta \in F$,

c) the extension $L : F$ is normal.

Remark. a) is a special case of b). Really we can take $F = K(\alpha)$ and define $\eta_F : F \to L$ by $\eta_F(\alpha) = \alpha'$.

I'll prove only the part a) and leave parts b) and c) as a homework.

Proof of a). We can find $\alpha_2, ..., \alpha_n \in L$ such that $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$ where $\alpha_1 := \alpha$. By Lemma 3.3 there exists a K-homomorphism $\eta_1 : K(\alpha_1) \to L$ such that $\eta_1(\alpha_1) = \alpha'$.

Claim. There exists a K-homomorphisms $\eta_i : K(\alpha_1, \alpha_2, ..., \alpha_i) \to L, 1 \leq i \leq n$ such that η_i is an extension of $\eta_{i-1}, 2 \leq i \leq n$.

Proof of the Claim. We will prove the existence of a K-homomorphism $\eta_2 : K(\alpha_1, \alpha_2) \to L$ which extends η_1. The general case is easily done by induction.

Let $p(t) := Irr(\alpha_2, K, t) \in K[t]$ and

$q(t) := Irr(\alpha_2, K(\alpha_1), t) \in K(\alpha_1)[t]$. By the definition $p(\alpha_2) = 0$ and $q(t)$ is irreducible in $K(\alpha_1)[t]$. Therefore $q(t)|p(t)$. Since $p(t)$ has a root in L and the field L is normal we see that $p(t)$ decomposes in $L[t]$ in a product of linear factors. Since $q(t)|p(t)$ we see that $q(t)$ also decomposes in $L[t]$ in a product of linear factors. So we can find a $\alpha'_2 \in L$ such that $q(\alpha'_2) = 0$. It follows now from Lemma 3.3 that there exists an extension $\eta_2 : K(\alpha_1, \alpha_2) \to L$ of $\eta_1 : K(\alpha_1) \to L$ such that $\eta_2(\alpha_2) = \alpha'_2$.$\square$

To finish the proof of Lemma 6.1 we have to show that $\eta_n : L \to L$ is an automorphism. But we know that $\eta_n : L \to L$ is a K-linear map such that $Ker(\eta_n) = \{0\}$. Since $[L : K] < \infty$ this implies that $\eta_n : L \to L$ is an automorphism. $\square$

Lemma 6.2. Let $L \supset K$ be a finite normal extension, p= ch (K), $\alpha \in L$ an element such that for any K-homomorphism $f : K(\alpha) \to L$ we have $f(\alpha) = \alpha$. Then either $\alpha \in K$ or $p \geq 0$ and there exists $n > 0$ such that $\alpha^{p^n} \in K$.

Proof. As we know form Lemma 3.3 the set of K-homomorphism $f : K(\alpha) \to L$ can be identified with the set of roots of the polynomial $p(t) := Irr(\alpha, K, t)$ in L. So we see that all the roots of $p(t)$ in L are equal to α. Since the field L is normal we know that $p(t)$ decomposes in a product of linear factors in $L[t]$. So $p(t) = (t-\alpha)^m$ where $m =$deg($p(t)$).

Consider first the case when ch (K)=0. Then

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

where we omit the lower terms. Since $p(t) \in K[t]$ we have $m\alpha \in K$. By the assumption ch (K)=0 and we can divide by m. So $\alpha \in K$.

Assume now that ch (K)=p> 0. 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 we omit the lower terms.

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

Lemma 6.3. Let $F \supset K$ be a extension such that any element $\alpha \in F$ is algebraic over K and every monic polynomial $p(t) \in K[t]$ splits in $F[t]$ into a product of linear factors. Then the field F is algebraicly closed.

Proof. We want to show that any monic polynomial $r(t) = \sum_{i=0}^{n} c_i t^i \in F[t], n > 0$ has a root in F. Let $L = K(c_0, ..., c_{n-1})$. Since every element in F is algebraic over K we see that $[L : K] < \infty$.

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 $\beta_j \in F, 1 \leq j \leq a$ be the set of roots of $q(t)$ in F and $N = K(\beta_1, ..., \beta_a) \subset F$. Since $q(t)$ splits in $F[t]$ into a product of factors of the type $t - \beta_j$ we see that N is a splitting field of $q(t)$ over K. So [by Theorem 4.2] $N : K$ is normal.

Let X be the set of all K-homomorphisms $f : L \to N$. The group $Gal(N/K)$ of the automorphisms of N over K acts on the set X by $f \to g(f), g \in Gal(N/K)$ where $g(f)(l) := g(f(l)), l \in L$.

For any $f \in X$ we define $p_f(t) := \sum_{i=0}^{n} f(c_i) t^i \in N[t]$ and define

$$R(t) := \prod_{f \in X} p_f(t) \in N[t]$$

Let us write $R(t) = \sum_{i=0}^{d} r_i t^i, r_i \in N$. I claim that for any $g(r_i) = r_i$ for any $g \in Gal(L : K), 1 \leq i \leq d$. Really when we act by g on $R(t)$ we only interchange the order of the factors in the product $R(t) := \prod_{f \in X} p_f(t)$. As follows from Lemma 6.2 either $R(t) \in K[t]$ or ch $(K) := p > 0$ and there exists $n > 0$ such that $c_i^{p^n} \in K, \forall i, 1 \leq i \leq d$. But in this case $R(t)^{p^n} = \sum_{i=0}^{d} r_i^{p^n} t^i \in K[t]$.

We see that there exists $m > 0$ such that $R(t)^m \in K[t]$. Therefore the polynomial $R(t)^m \in K[t]$ splits in $F[t]$ into a product of factors. So any divisor of the polynomial $R(t)$ also splits in $F[t]$ into a product of linear factors. Since $p(t) = p(t)_{Id}$ is a divisor of $R(t)$ we see that $p(t)$ has a root in F.$\square$

Definition 6.1. Let K be a field. An *algebraic closure* of K is an extension $\bar{K} \supset K$ which is algebraicly closed and such that any element $\alpha \in \bar{K}$ is algebraic over K.

Remark. If $L \supset K$ is a finite extension that any algebraic closure $\bar{L}$ of L is also an algebraic closure K.

Theorem 6.1. Let K be a field. Then

a) there exists an algebraic closure $\bar{K}$ of K,

b) if $\bar{K}' \supset K$ is another algebraic closure of K then there exists a K-isomorphism $\eta : \bar{K} \to \bar{K}'$.

Proof. I'll consider only the case when the field K is countable. In this case the set of polynomials $q(t) \in K[t]$ is also countable. So we can write a sequence $q_n(t) \in K[t], n > 0$ of monic polynomials such that any monic polynomial appears in this sequence. Now we construct an sequence of fields $L_n, n \geq 0$ and imbeddings $L_n \hookrightarrow L_{n+1}$ as follows. Let $L_0 = K$ and L_n be a splitting field of the polynomial $q_n(t)$ over L_{n-1}. We define $\bar{K} := \cup_{n=0} L_n$. It is clear that the field $\bar{K}$ satisfies the conditions of Lemma 6.3. So $\bar{K}$ algebraicly closed. Since all the fields L_n are finite over K any element of $\bar{K}$ is algebraic over K. So $\bar{K}$ is an algebraic closure of K.

Before discussing the uniqueness of an algebraic closure we consider the following useful result.

Lemma 6.4. Let $p(t) \in K[t]$ be an irreducible polynomial, $\alpha, \alpha' \in \bar{K}$ be roots of $p(t)$. Then there exists an automorphism $\eta \in Gal(\bar{K}/K)$ such that $\eta(\alpha) = \alpha'$.

Proof of Lemma 6.4. Let $n \geq 0$ be an index such that $\alpha, \alpha' \in L_n$. Since the field L_n is normal over K it follows from Lemma 6.1 a) that there exists an automorphism $\eta_n : L_n \to L_n$ such that $\eta_n(\alpha) = \alpha'$.

It follows now from Lemma 6.1 b) that there exists an automorphism $\eta_{n+1} : L_{n+1} \to L_{n+1}$ whose restriction on L_n is equal to η_n. Putting together all the automorphisms $\eta_m : L_m \to L_m, m \geq n$ we obtain an automorphism $\eta \in Gal(\bar{K}/K)$ such that $\eta(\alpha) = \alpha'$.$\square$

Now we can prove the second part of the Theorem 6.1. Let $\bar{K}' \supset K$ be another algebraic closure of K. Since the field $\bar{K}'$ is an algebraic closure of K, it follows from Lemma 3.3 that any K-homomorphism $\nu_i : L_i \to \bar{K}'$ can be extended to a homomorphism $\nu_{i+1} : L_{i+1} \to \bar{K}'$. Putting the homomorphism $\nu_i : L_i \to \bar{K}'$ together we obtain a K-homomorphism $\nu : \bar{K} \to \bar{K}'$.

To show that the K-homomorphism $\nu : \bar{K} \to \bar{K}'$ is an isomorphism it is sufficient to prove that for any $\alpha' \in \bar{K}'$ there exists $\alpha \in \bar{K}$ such that $\nu(\alpha) = \alpha'$.

By the definition of an algebraic closure any $\alpha' \in \bar{K}'$ is algebraic over K and we can consider an irreducible polynomial $p(t) := Irr(\alpha', K, t) \in K[t]$. Since the field $\bar{K}$ is algebraicly closed there exists $\alpha \in \bar{K}$ such that $p(\alpha) = 0$. Choose $n \geq 0$ such that $\alpha \in L_n$ and define $L'_n := \nu(L_n) \subset \bar{K}'$. Since the field L_n is normal over K the irreducible polynomial $p(t)$ can be written as a product

$$p(t) = \prod_{i=0}^{r} (t - \alpha_i)^{m_i}, \alpha_i \in L_n, \alpha_1 = \alpha$$

Therefore

$$\nu(p(t)) = \prod_{i=0}^{r} (t - \nu(\alpha_i))^{m_i}$$

Since $p(t) \in K[t]$ we have $\nu(p(t)) = p(t)$ and therefore

$$p(t) = \prod_{i=0}^{r} (t - \nu(\alpha_i))^{m_i}$$

Since α' is a root of $p(t)$ in L'_n we see that $\alpha' = \nu(\alpha_i)$ for some $i, 1 \leq i \leq r$.$\square$

Definition 6.2. Let $L \supset K$ be a finite extension and $\bar{K}$ an algebraic closure of K [which is also an algebraic closure of L, see the Remark after the definition 6.1].

a) We denote by $H(L/K)$ the set of K-homomorphisms of L to $\bar{K}$.

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.

Remark. It follows from Theorem 6.1 this set does not depend on a choice of an algebraic closure $\bar{K}$ of K.

Lemma 6.5. Let $K \subset F \subset L$ be finite field extensions. Then $[L:K]_s = [L:F]_s[F:K]_s$

Proof . For any K-homomorphism $g \in H(F/K)$ we denote by $H(L/K)_g \subset H(L/K)$ the subset of K- 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 6.4 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 6.5. 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 $[L:K]_s = [L:F]_s[F:K]_s$.$\square$