completely in K. (In other words, generalize the corresponding theorem given for the characterization of finite-dimensional splitting fields.)

(4) Prove that if K is an algebraic closure of F, then it is a splitting field over F of all polynomials over F, or of all irreducible polynomials over F.

(5) Let F and F_0 be fields and $\sigma : F \to F_0$ an isomorphism. Show that σ extends to an isomorphism of any algebraic closure of F onto any algebraic closure of F_0.

Note that if we extented the definition of separability from a single polynomial to an arbitrary set of polynomials then we can view an algebraic closure of a field F as a splitting field over F of all polynomials in $F[x]$.

Definition. Let Γ be a set of monic polynomials with coefficients in F. Then an extension E/F is called a <u>splitting field</u> over F <u>of the set Γ</u> if

(1) every $f \in \Gamma$ is a product of linear factors in $E[x]$, and

(2) E is generated over F by the roots of the $f \in \Gamma$.

In some books, normality is defined in such a way that it is equivalent to being a splitting field of minimal polynomials of all (or some certain) elements of the extention. Here, we assume, additionally, that the extension is separable. Thus, in our context, normality of an extension is what is defined as being Galois in some sources.

Note also that we can generalize some key theorems involving normal and splitting extensions given so far for only finite-dimensional extensions to any algebraic extensions, which is covered in the following series of exercises.

<u>Exercise</u> 8. Let E/F be an algebraic extension. Then show that E/F is normal if and only if every irreducible polynomial over F having a root in E factors completely into distinct linear factors.

<u>Exercise</u> 9. Let Γ be a set of monic polynomials with coefficients in F. Show that there is an extension E of F which is a splitting field over F of the set Γ.

__Exercise__ 10. Let $\eta : F \longrightarrow F_0$ be an isomorphism of F onto F_0, Γ a set of monic polynomials over F, Γ_0 the corresponding set of polynomials over F_0, E and E_0 splitting fields over F and F_0 of Γ and Γ_0, respectively. Then prove that η can be extended to an isomorphism of E onto E_0.

__Exercise__ 11. Let $E/_F$ be an algebraic extension. Then prove that the following statements are equivalent:

(i) E is a splitting field over F;

(ii) Whenever an irreducible polynomial over F has a root in E, it factors completely into linear factors.

__Exercise__ 12. Let $E/_F$ be an algebraic extension. Show that E is a splitting field over F if and only if E is a splitting field over F of minimal polynomials (over F) of all elements of E.

__Exercise__ 13. Let $E/_F$ be an algebraic extension. Then show that the following statements are equivalent:

(i) $E/_F$ is normal;

(ii) E is separable over F and E is a splitting field over F.

__Exercise__ 14. Let E be a splitting field over F. Then prove that E is a separable extension of its subfield P of purely inseparable elements in E.

__Exercise__ 15. State and prove the appropriate generalization to infinite algebraic extensions of the third theorem of section "Separability".

Inseparable Extensions

Recall that an element u is called purely inseparable over a field F of characteristic $p \neq 0$ if $u^{p^r} \in F$ for some $r > 0$. Also, we say that an extension E/F is purely inseparable if every element of E is purely inseparable over F.

Notice that u is separable over F if its minimal polynomial f of degree n has n distinct roots (in some splitting field) and purely inseparable if f has precisely one root.

Theorem. If E is an algebraic extension of a field F of characteristic $p \neq 0$, then the following statements are equivalent:

(i) E is purely inseparable over F.

(ii) The minimal polynomial of any $u \in E$ is of the form $x^{p^r} - a \in F[x]$;

(iii) E is generated over F by a set of purely inseparable elements.

proof.

(i) $\Rightarrow$ (ii) : Let $u \in E$. Then u is purely inseparable over F. Then $u^{p^n} \in F$ for some $n > 0$. Suppose that n is as small as possible. Set $a = u^{p^n}$. Then the minimal

polynomial of u over F divides $x^{p^n}-a=(x-u)^{p^n}$.
It follows that $f=(x-u)^m$ for some $1\leq m\leq p^n$.
Let $m=kp^r$ with $(k,p)=1$. Then

$$f=(x-u)^m=(x-u)^{kp^r}=(x^{p^r}-u^{p^r})^k.$$

Since $(x-u)^m\in F[x]$, the coefficient of $x^{p^r(k-1)}$ (namely, $\pm ku^{p^r}$) must lie in F. Now $(p,k)=1$ implies that $u^{p^r}\in F$. Since $p^r\leq m\leq p^n$, by the choice of n, we get $p^r=p^n$ and $k=1$. This gives that

$$f=(x-u)^m=(x-u)^{p^r}=x^{p^r}-u^{p^r}=x^{p^r}-a.$$

(ii) $\Rightarrow$ (i) and (i) $\Rightarrow$ (iii) are trivial.

(iii) $\Rightarrow$ (i): Let $u\in E$. By assumption $u=h(u_1,\dots,u_n)$ for some purely inseparable elements $u_1,\dots,u_n$ and a polynomial $h\in F[x_1,\dots,x_n]$. (Note that E/F is an algebraic extension which means that we may choose a polynomial h instead of a rational function.) Then $u_i^{p^{r_i}}\in F$ for some $r_i>0$. Set $r=\max\{r_i\}_{i=1}^n$. Then $u^{p^r}=h(u_1,\dots,u_n)^{p^r}\in F$ since the characteristic of F is equal to p. This completes the proof.

Corollary. If E is a finite-dimensional purely inseparable extension of F with $\operatorname{char} F=p\neq 0$, then $[E:F]=p^n$ for some $n\geq 0$.

Definition. Let E be an algebraic extension of F and S the largest subfield of E separable over F. The dimension $[S:F]$ is called the separable degree of E over F and is denoted $[E:F]_s$. The dimension $[E:S]$ is called the inseparable degree (or degree of inseparability) of E over F and is denoted $[E:F]_i$.

Remarks. $[E:F]_s = [E:F]$ and $[E:F]_i = 1$ if and only if E is separable over F. $[E:F]_i = [E:F]$ if and only if E is purely inseparable over F. In any case $[E:F] = [E:F]_s [E:F]_i$. If $[E:F]$ is finite and char $F = p \neq 0$, then $[E:F]_i$ is a power of p.

Lemma. Let $F \subset E \subset K \subset L$ be a tower of fields where L is a splitting field over F. If r is the cardinal number of distinct isomorphisms of K into L that leaves elements of E fixed (or, in other words, isomorphisms of K/E into L) and t is the cardinal number of distinct isomorphisms of E/F into L, then rt is the cardinal number of distinct isomorphisms of K/F into L.

proof. For $|I| = t$ and $|J| = r$, let $\{\sigma_i : i \in I\}$ be the set of all isomorphisms of E/F into L and $\{\tau_j : j \in J\}$ the set of all isomorphisms of K/E into L. Each σ_i extends to an automorphism of L/F which will be also denoted σ_i. Note that $\sigma_i \tau_j$ is an isomorphism of K/F into L. Suppose $\sigma_i \tau_j = \sigma_a \tau_b$. Then $\sigma_a^{-1} \sigma_i \tau_j = \tau_b$ which implies that $\sigma_a^{-1} \sigma_i |_E = id_E$. This gives that $\sigma_a = \sigma_i$ and so $i = a$. Since σ_i is injective, $\sigma_i \tau_j = \sigma_a \tau_b$ implies that $\tau_j = \tau_b$ and $j = b$. It follows that rt isomorphisms of K/F into L $\sigma_i \tau_j$ are all distinct. Let σ be an isomorphism of K/F into L. Then $\sigma|_E = \sigma_i$ for some i and $\sigma_i^{-1} \sigma$ is an isomorphism of K/F into L which is the identity on E. Therefore, $\sigma_i^{-1} \sigma = \tau_j$ for some j, whence $\sigma = \sigma_i \tau_j$. Thus the rt distinct maps $\sigma_i \tau_j$ are all of the isomorphisms of K/F into L.

Theorem. Let $F \subset E \subset K$ be a tower of fields where E/F is finite dimensional and K is a splitting field over F. The number of distinct isomorphisms of E/F into K is precisely $[E:F]_s$.

proof. Let S be the maximal subfield of E separable over F. Every isomorphism of S/F into K extends to an automorphism of K/F. We claim that the number of distinct isomorphisms of E/F into K is the same as the number of distinct isomorphisms of S/F into K. This trivially true if char $F=0$ since $E=S$ in that case. So let char $F=p\neq 0$ and suppose σ,τ are isomorphisms of E/F into K such that $\sigma|_S=\tau|_S$. If $u\in E$, then $u^{p^n}\in S$ for some $n\geq 0$. Therefore,

$$\sigma(u)^{p^n}=\sigma(u^{p^n})=\tau(u^{p^n})=\tau(u)^{p^n}$$

whence $\sigma(u)=\tau(u)$. Thus $\sigma|_S=\tau|_S$ implies $\sigma=\tau$, which proves our claim. Consequently, it suffices to assume that E is separable over F (that is, $E=S$), in which case we have $[E:F]=[E:F]_s$, $[E:M]=[E:M]_s$ and $[M:F]=[M:F]_s$ for any intermediate field M since, in this case, M is separable over F and E is separable over M.

Proceed now by induction on $n=[E:F]=[E:F]_s$ with the case $n=1$ trivial. If $n>1$ choose $u\in E\setminus F$; then $[F(u):F]=r>1$. If $r<n$ use the induction hypothesis together with the above lemma to prove the theorem. If $r=n$, then $E=F(u)$ and $[E:F]$ is the degree of the (separable) minimal polynomial $f\in F[x]$ of u. Every isomorphism σ of E/F into K is completely determined by $v=\sigma(u)$. Since v is a root of f, there are at most $[E:F]=\deg(f)$ such isomorphisms of E/F. Since K is a splitting field over F and f is separable,

f splits into n distinct linear factors in K which implies that f has n distinct roots in K. This gives that there are exactly $[E:F]$ distinct isomorphisms of E/F into K.

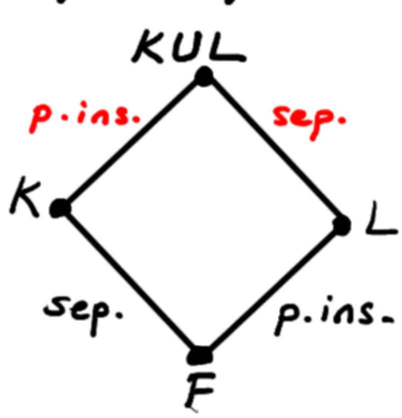
Corollary. If $F \subset E \subset K$ is a tower of fields where all extensions are finite dimensional, then $[K:F]_s = [K:E]_s [E:F]_s$ and $[K:F]_i = [K:E]_i [E:F]_i$.

proof. Left as an exercise.

Exercise 16. Prove the above corollary using the preceding lemma and theorem.

Corollary. Let K, L be two finite extensions of F, and assume that K/F is separable, L/F is purely inseparable. Assume K and L are subfields of a common field. Then

$$[KUL : L] = [K:F] = [KUL : F]_s$$
$$[KUL : K] = [L:F] = [KUL : F]_i .$$



proof. Left as an exercise.

Exercise 17. Prove the above corollary.

Corollary. Let $f \in F[x]$ be an irreducible monic polynomial over a field F, K a splitting field of f over F and u_1 a root of f in K. Then
(i) every root of f has multiplicity $[F(u_1):F]_i$, so that in $K[x]$

$$f = [(x-u_1)\dots(x-u_n)]^{[F(u_1):F]_i}$$

where $u_1,\dots,u_n$ are all the distinct roots of f and $n = [F(u_1):F]_s$;
(ii) $u_1^{[F(u_1):F]_i}$ is separable over F.

proof. Assume that $\operatorname{char} F = p \neq 0$ since the case $\operatorname{char} F = 0$ is trivial.
(i) For any $i > 1$ there is an isomorphism $\sigma : F(u_1) \to F(u_i)$ (that leaves F fixed) with $\sigma(u_1) = \sigma(u_i)$ and σ extends to an automorphism of K which will be also denoted σ since K is a splitting field of $f \in F[x]$. Now in $K[x]$ there are some $r_1,\dots,r_n$ with
$(x-u_1)^{r_1}\dots(x-u_n)^{r_n} = f = \sigma(f) = (x-\sigma(u_1))^{r_1}\dots(x-\sigma(u_n))^{r_n}$.
Since $u_1,\dots,u_n$ are distinct and σ is injective, unique factorization in $K[x]$ implies that $(x-u_i)^{r_i} = (x-\sigma(u_1))^{r_1}$ whence $r_1 = r_i$. This shows that every root of f has multiplicity $r = r_1$ so that $f = (x-u_1)^r\dots(x-u_n)^r$ and $[F(u_1):F] = \deg(f) = nr$.
Since there are exactly n isomorphisms of $F(u_1)/F$

into K, $[F(u_1):F]_s = n$. Therefore
$$[F(u_1):F]_i = [F(u_1):F] / [F(u_1):F]_s = nr/n = r.$$

(ii) Since r is a power of $p = \operatorname{char} F$, we have $f = (x-u_1)^r \dots (x-u_n)^r = (x^r - u_1^r) \dots (x^r - u_n^r)$. Thus f is a polynomial in x^r with coefficient in F, say $f = \sum_{i=0}^{n} a_i x^{ri}$. Consequently, u_1^r is a root of
$$g = \sum_{i=0}^{n} a_i x^i = (x - u_1^r) \dots (x - u_n^r) \in F[x]$$
Since $u_1, \dots, u_n$ are distinct and the minimal polynomial of u_1^r divides g, $u_1^r = u_1^{[F(u_1):F]_i}$ is separable over F.

In summary, if $u \in \overline{F}$ and f is the minimal polynomial of u over F, then there are two cases:

(i) $\operatorname{char} F = 0$; in which case all roots of f have multiplicity 1 (i.e., f is separable), or

(ii) $\operatorname{char} F = p \neq 0$; in which case there exists an integer $m \geq 0$ such that every root of f has multiplicity p^m, for any root u of f $[F(u):F] = p^m [F(u):F]_s$, there are exactly $[F(u):F]_s$ roots of f, and u^{p^m} is separable over F.

Theorem. Let E^p denote the field of all elements x^p $(x \in E)$, where E is a field of characteristic $p \neq 0$ and is a finite extension of F. Then the following statements are equivalent:

(i) E is separable over F;

(ii) $E^{p^n} \cup F = E$ for all $n \geq 1$.

proof.

(i) $\Rightarrow$ (ii): Notice that E is separable over $E^{p^n} \cup F$ $(n \geq 1)$. Since E is also purely inseparable over $E^{p^n} \cup F$, we get $E = E^{p^n} \cup F$.

(ii) $\Rightarrow$ (i): Let S be the maximal separable subfield of E over F. Let $E = F(u_1, \ldots, u_n)$. Since E is purely inseparable over S, there exists m such that $u_i^{p^m} \in S$ for each $i = 1, \ldots, n$. Hence $E^{p^m} \subseteq S$. But $E^{p^m} \cup F = E$ whence $E = S$ is separable over F.

Theorem. Let K/F be an algebraic extension with K a splitting field over F. Let G be the Galois group of K/F and E the fixed subfield of K under G. Then E is purely inseparable over F, and K is separable over E. If S is the maximal separable subextension of K over F, then $K = S \cup E$ and $E \cap S = F$.

proof. Let $u \in E$. Let τ be an embedding of K over F

into $\overline{K}$ and extend τ to an embedding of K, which we denote also by τ. Then τ is an automorphism of K over F because K is a splitting field over F. By definition, $\tau(u)=u$ and τ is identity on $F(u)$. Hence $[F(u):F]_s = 1$ and u is purely inseparable over F. Thus E is purely inseparable over F. The intersection of S and E is both separable and purely inseparable over F, and hence is equal to F.

Since $E = G' = \{u \in K : \sigma(u) = u \text{ for all } \sigma \in G\}$, E is a closed subfield of K over F, that is, K/E is a normal extension. It follows that K is separable over E.

We now have the following picture:

$$\begin{tikzcd}
& K \arrow[d, dash] & \\
& S \cup E \arrow[dl, dash] \arrow[dr, dash] & \\
S \arrow[dr, dash, "\text{sep.}"'] & & E \arrow[dl, dash, "\text{p. ins.}"] \\
& S \cap E = F &
\end{tikzcd}$$

We know that K is purely inseparable over S, hence purely inseparable over $S \cup E$. Furthermore, K is separable over E, hence separable over $S \cup E$. Hence $K = S \cup E$.

Remark. Recall that a normal algebraic extension has been shown to be a splitting separable extension. By above theorem, one can show that any algebraic splitting extension is decomposed into a normal and a purely inseparable extension (see the exercise below!).

Exercise 18. Let K/F be an algebraic extension with K a splitting field over F and let S be the maximal separable subextension of K over F. Show that S is normal over F.