V. Fields and Galois Theory


4. If $F$ is a spitting field over $K$ of $S$, then $F$ is also a spitting field over $K$ of the set $T$ of all irreducible factors of polynomials in $S$.

Let $S = f_{i \in I}$ where $f_i \in K[x]$. Denote the roots of $f_i$ by $\{u_{ij}\}_{j=1}^n$. Then $F = K(\{u_{ij}\})$ and $f_i = u_{i0} \prod_{j=1}^n (x - u_{ij})$ where $u_{ij} \in F$. Now let $g$ be an irreducible factor of some $f_i$ so $f_i = gh$ where $g$ is irreducible in $K[x]$. Now

$$f_i = u_{i0} (x - u_{i1}) (x - u_{i2}) \cdots (x - u_{in}) \implies g = (x - u_{ip}) \cdots (x - u_{ir})$$

for some $1 \leq p, q \leq i_n$. So $g$ splits in $F$.

For $u \in \{u_{ij}\}$, $u \notin K$, but $u$ is a root of some $f_i$. If we factor $f_i$ into its irreducible factors, then $u$ is a root of some $g_{ij}$. To see this, suppose $U$ were not a root of any $g_{ij}$. Denote the roots of the $g_{ij}$ by $\{v_k\}_{k=1}^m$. Then the $\{v_k\}$ are exactly the roots of $f_i$. So $u \notin \{v_k\} \implies u$ is not a root of $f_i$. So choice of $u$. Thus $F$ is generated over $K$ by the roots of the $g_{ij}$ (the polynomials of $T$). \hfill \blacksquare

5. If $f \in K[x]$ has degree $n$ and $F$ is a spitting field of $f$ over $K$, then $[F : K]$ divides $n!$.

$f$ has degree $n = 1$ \implies $f$ is linear \implies $f$ splits in $K[x]$. Then $[F : K] = 1$, which divides $n!$ trivially; so let $\deg f > 1$. Then $[F : K] = m \leq n!$ by 3.2.

$\deg f = n \implies f = u_0 (x - u_1) (x - u_2) \cdots (x - u_n)$ where $u_i \in F$. Say $\{u_k\}$ are the roots of $f$ that are not already in $K$, so $F = K(\{u_k\})$. Note: $u_k$ is algebraic over $K$ of degree $d_k$.

Let $f = g_1 \cdots g_h \cdot h_1 \cdots h_s$ be a factorization (as reduced as possible) of $f$ in $K[x]$, where the $h_i$ are those factors which spit in $K[x]$. Then the $\{u_k\}_{k=1}^m$ are precisely the roots of the $g_i$. Then

$$[F : K] = m = \prod_{k=1}^p d_k, \text{ and } \deg g_k = d_k.$$  

$\deg f = n = m + q$, where $m$ is the degree of $g_1 \cdots g_r$ and $q$ is the degree of $h_1 \cdots h_s$.

$n! = am + b$ for some $a, b \in \mathbb{N}, b < m$. Then

$$m \leq n \implies n! = 1 \cdot 2 \cdot 3 \cdots m \cdots (n - 1) n$$

So $m$ divides $n!$. \hfill \blacksquare
6. Let $K$ be a field such that for every extension field $F$, the maximal algebraic extension of $K$ contained in $F$ is $K$ itself. Then $K$ is algebraically closed.

The hypotheses mean, loosely translated, that $K$ has no proper algebraic extension, i.e., $K$ is the only algebraic extension of $K$. But this just means $K$ is closed, by 3.3(iv). Yippee.

9. $F$ is an algebraic closure of $K$ if and only if $F$ is algebraic over $K$ and for every algebraic extension $E$ of $K$ there exists a $K$-monomorphism $E \to F$.

$\Rightarrow$ $F$ is algebraic over $K$ and algebraically closed by definition 3.4. Let $E$ be any algebraic extension of $K$. If $E$ is algebraically closed, then $E$ meets the criteria for being an algebraic closure of $K$ and hence $E \cong_K F$ by 3.6. So without loss of generality suppose $E$ is not algebraically closed. Since algebraic closure s always exist, we can whip out the algebraic closure $M$ of $E$. Then $M : E$ algebraic and $E : K$ algebraic will imply $M : K$ algebraic by 1.13, so $M$ is also an algebraically closed of $K$. Evidently, $M$ is hot stuff! Now $M \cong_K F$ by 3.6, so

$$E \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \qu
10. Let $F : K$ be an algebraic extension, and suppose $K'$ is some field isomorphic to $K$ by $\sigma : K' \xrightarrow{\sim} K$. $F$ is an algebraic closure of $K \iff F$ is algebraic over $K$ and for every algebraic extension $E$ of $K'$, $\sigma$ extends to a monomorphism $E \to F$.

$\Rightarrow$ $E$ is an algebraic extension of $K' \implies E \equiv K (\{u_i\})$ where the $\{u_i\}_{i \in I}$ are algebraic over $K'$. Let $S$ consist of every irreducible polynomial of $K'[x]$ and let $K'$ denote the algebraic closure of $K'$. Then $K'$ is a splitting field for $S$ and $T = \sigma S$ has $F$ for a splitting field. Now $\sigma$ extends to an isomorphism

$\bar{\sigma} : K' \xrightarrow{\sim} F$

by 3.8. Since $E$ algebraic over $K' \implies E \subseteq K'$ by 3.3(iv), we have $\{u_i\} \subset E \subset K'$, which shows that $\bar{\sigma} (u_i)$ is defined for every $i$. Denote $\bar{\sigma} (u_i) = v_i$. Now we have

$\bar{\sigma}|_E : K' (\{u_i\}) \xrightarrow{\sim} K (\{v_i\})$ and $i : K (\{v_i\}) \xrightarrow{c} F$

where $\bar{\sigma}|_E$ is an isomorphism, and $i$ is a monomorphism by inclusion. Hence,

$i \circ \bar{\sigma}|_E : E \xrightarrow{c} F$

is a monomorphism extending $\sigma$. This is all illustrated in the following diagram.

\[
\begin{array}{ccc}
K' & \xrightarrow{\sigma} & K \\
\downarrow \bar{\sigma} \downarrow & & \downarrow i \\
E & \xrightarrow{\bar{\sigma}|_E} & K (\{v_i\}) \\
\downarrow \downarrow & & \downarrow i \\
K' & \xrightarrow{\sigma} & K
\end{array}
\]

$\Leftarrow$ Let $K' = K$ and let $E$ be any algebraic extension of $F$ so that the hypothesis gives an extension of $\sigma$ to a monomorphism

$\bar{\sigma} : E \to F$.

Then $F$ has no algebraic extension other than itself and is hence closed by 3.3(iv)$^1$. Since $F$ algebraic over $K$ is given, $F$ is the algebraic closure of $K$ by 3.4(i). This is illustrated in the following diagram.

\[
\begin{array}{ccc}
E & \xrightarrow{\sigma} & F \\
\downarrow \downarrow & & \downarrow \\
K' = K & \xrightarrow{\sigma} & K
\end{array}
\]

$^1$See also #6
11. a) For a collection of elements \( X = \{u_1, \ldots, u_n\} \subset F \) which are separable over \( K \),
\( K(u_1, \ldots, u_n) \) is a separable extension of \( K \).

For each \( i \), let \( f_i \) be the corresponding irreducible polynomial of \( u_i \). Define 
\( T = \{f_i\}_{i=1}^n \) and let \( S \) be the set of all roots of the \( \{f_i\} \). Then \( K(X) \) is separable over \( K \) by 3.11(iii). Since \( K(u_1, \ldots, u_n) \subset K \), \( K(u_1, \ldots, u_n) \) is clearly also separable over \( K \).

\( \blacksquare \)

b) If \( F \) is generated by a (possibly infinite) set of separable elements over \( K \), then \( F \) is a separable extension of \( K \).

Pick \( v \in F \) so \( v = \frac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)} \) for some \( \{u_1, \ldots, u_n\} \subset X \). Then \( K(u_1, \ldots, u_n) \) is separable over \( K \) by part (a), so \( v \) is separable over \( K \).

\( \blacksquare \)

12. Let \( E \) be an intermediate field of the extension \( F : K \).

a) If \( u \in F \) is separable over \( K \), then \( u \) is separable over \( E \).

Let \( f \in K[x] \) be the irreducible polynomial of \( u \). Then \( M \) is a splitting field of \( f \) such that \( f = (x - a_1)(x - a_2)\cdots(x - a_n) \) with \( a_i \in M \), \( \forall i \). Let \( g \in E[x] \) be the irreducible polynomial of \( u \) over \( E \). Then
\[
g \mid f \implies g = (x - a_{k_1})\cdots(x - a_{k_m})
\]
where \( \{a_{k_1}, \ldots, a_{k_m}\} \) is a subset of the \( \{a_i\}_{i=1}^n \) above. Hence, the \( \{a_{k_j}\}_{j=1}^m \) are distinct, which shows \( u \) is separable over \( E \).

\( \blacksquare \)

b) If \( F \) is separable over \( K \), then \( F \) is separable over \( E \) and \( E \) is separable over \( K \).

\( F \) is separable over \( K \) \implies every \( u \in F \) is separable over \( K \)
\[\implies \text{every } u \in F \text{ is separable over } E \quad \text{by (a)}\]
\[\implies F \text{ is separable over } E. \]

Then simply note that
\( u \in E \implies u \in F \implies u \text{ is separable over } K \)
implies that \( E \) is separable over \( K \).

\( \blacksquare \)
13. Suppose \([F : K] < \infty\). Then the following conditions are equivalent:

i) \(F\) is Galois over \(K\).

ii) \(F\) is separable over \(K\) and a splitting field of some polynomial \(f \in K[x]\).

iii) \(F\) is a splitting field over \(K\) of a polynomial \(f \in K[x]\) whose irreducible factors are separable.

\[
\begin{align*}
\text{\(i \Rightarrow ii\)} & \quad [F : K] < \infty \implies F \text{ is algebraic over } K, \text{ so if we are given that } F \text{ is Galois over } K, \text{ then } F \text{ is separable and a splitting field over } K \text{ of } S \subseteq K[x]. \text{ Hence } [F : K] < \infty \implies F = K(u_1, u_2, \ldots, u_n). \text{ Let } \{f_i\}_{i=1}^n \text{ be the irreducible polynomials of the } \{u_i\}. \text{ Then } F \text{ is a splitting field of } f = \prod_{i=1}^n f_i. \\
\text{\(i \Rightarrow iii\)} & \quad \text{Continuing from above, note that } F \text{ is separable } \implies \{u_i\} \text{ are separable } \implies \{f_i\} \text{ are separable. But then } f \text{ is a polynomial in } K[x] \text{ whose irreducible factors are separable.} \\
\text{\(ii \Rightarrow i\)} & \quad \text{Let } S = \{f\} \text{ so that the result is immediate from 3.11.} \\
\text{\(iii \Rightarrow ii\)} & \quad \text{We just need to show } F \text{ is separable, so let } \{f_i\} \text{ be the irreducible factors of } f. \text{ The } f_i \text{ are separable, so}
\end{align*}
\]

\[f_i(x) = (x - a_{i_1})(x - a_{i_2}) \cdots (x - a_{i_r})\]

where \(a_{i_1} \neq a_{i_2}\) and \(a_{i_3} \in F \setminus K, \forall k.\) \(f\) spits in \(F,\) so all the roots of

\[f(x) = \prod_{i=1}^n \prod_{\alpha=1}^\gamma (x - a_{i_\alpha})\]

lie in \(F.\) Since \(f_i\) are the irreducible factors, they are separable by hypothesis, i.e., the \(a_{i_\alpha}\) are distinct. Hence, \(F = K(\{a_{i_\alpha}\})\) is separable over \(K\) and a splitting field of \(F.\)

\[\square\]

17. If an intermediate field \(E\) is normal over \(K,\) then \(E\) is stable (relative to \(F\) and \(K\)).

\(E\) is stable iff \(\forall \sigma \in \text{Aut}_K F, \ u \in E \implies \sigma(u) \in E.\)

Pick \(u \in E\) and let \(f \in K[x]\) be the minimal polynomial of \(u.\) Then for any \(\sigma \in \text{Aut}_K F, \ \sigma(u)\) is also a root of \(f\) by V.2.2. Now \(E\) is normal over \(K,\) and \(f\) has a root in \(E,\) so \(f\) must spit in \(E.\) This shows \(\sigma(u) \in E.\)

\[\blacksquare\]
18. Let $F$ be normal over $K$ and $E$ an intermediate field. Then $E$ is normal over $K$ if and only if $E$ is stable. Furthermore, $\frac{\text{Aut}_KF}{\text{Aut}_KE} \cong \text{Aut}_KE$.

$\Rightarrow$ This follows immediately by the previous exercise.

$\Leftarrow$ $E$ is normal iff every irreducible polynomial with a root in $E$ spits in $E$.

Let $f \in K[x]$ be an irreducible polynomial with a root $u \in E$. We know by V.2.2 that $\sigma(u)$ is also a root of $f$, and we have by hypothesis that $\sigma(u) \in E$. Thus, it only remains to show that every root $v$ of $f$ is $\sigma(u)$, for some $\sigma \in \text{Aut}_KF$.

$u, v$ are both roots of the same irreducible polynomial $f$. Therefore, by V.1.9, the identity homomorphism $\sigma : K \xrightarrow{id} K$ extends to an isomorphism $\sigma : K(u) \xrightarrow{\sim} K(v)$ such that $\sigma(u) = v$ and $\sigma|_K = id$. In other words, we can find a $\sigma \in \text{Aut}_KF$ taking $u$ to $v$. ■

22. If $F$ is algebraic over $K$ and every element of $F$ belongs to an intermediate field that is normal over $K$, then $F$ is normal over $K$.

Let $f \in K[x]$ be an irreducible polynomial with a root $u \in F$. Then $u \in E$ where $E \triangleleft K$. Since $E$ is normal, $f$ spits in $E$ as $f(x) = (x - u_1)(x - u_2) \cdots (x - u_n)$. Then $\{u_i\}_{i=1}^n \subset E \subset F$, so $f$ spits in $F$. In other words, $F \triangleleft K$. ■

23. If $[F : K] = 2$, then $F$ is normal over $K$.

$[F : K] = 2 \implies F : K$ is algebraic and $F = K(u)$ for some $u$ of degree 2.

Let $f \in K[x]$ be the irreducible polynomial of $u$, so

$f(x) = x^2 + a_1 x + a_0$ for $a_i \in K$, and

$f(x) = (x - u)(x - v)$

$= x^2 - (u + v)x + uv$

for some $v \in F$. Hence, $uv \in K \implies v = \frac{a_0}{u} \in K$. Thus, $f$ spits in $F$ and $F \triangleleft K$. ■