Field and Galois Theory

Lectures by Uzi Vishne
Summary by Ari Feiglin (ari.feiglin@gmail.com)

Contents

1 Field Extensions and Minimal Polynomials

1.1 Dimensions of Field Extensions

Definition 1.1.1

Suppose F and K are fields such that $F \subseteq K$. Then the pair is called a **field extension** and is denoted K/F.

Notice that if K/F is a field extension, then K can be viewed as a F-linear space, and thus has a dimension. We denote this dimension $[K : F] := \dim_F K$, this is unsurprisingly called the *dimension* (or *degree* of the extension. An extension is called *finite* if its dimension is finite. Immediately we can prove a useful theorem about dimensions of extensions:

Theorem 1.1.2

Suppose K/F is a field extension and V a K-vector space. Then by viewing V as an F-linear space:

$$\dim_F V = \dim_K V \cdot [K : F]$$

Proof: let B_1 be a basis for V relative to K and B_2 be a basis for K relative to F. Then define $B = \{\alpha v \mid \alpha \in B_2, v \in B_1\} \subseteq V$, which we claim is a basis for V relative to F. Firstly, it is linearly independent: suppose $\alpha_1 v_1, \dots, \alpha_n v_n$ are in B and $\beta_1, \dots, \beta_n$ are in F such that

$$\beta_1\alpha_1 v_1 + \cdots + \beta_n\alpha_n v_n = 0$$

Since B_1 is a basis for V, then $\beta_i\alpha_i = 0$ for all i, and since B_2 is a basis it has no zeroes, so $\beta_i = 0$ for all i, meaning B is linearly independent.
B spans V since if $v \in B$ then $v = \sum_{i=1}^n \alpha_i v_i$ for $v_i \in B_1$ and $\alpha_i \in K$, and so each α_i can be written as the linear combination of elements in B_2. So all in all v can be written as the linear combination of elements in B. And so B is a basis of V, and $(\alpha, v) \mapsto \alpha v$ is a bijection from $B_1 \times B_2$ to B: it obviously is surjective and if $\alpha_1 v_1 = \alpha_2 v_2$ then $\alpha_1 = \alpha_2$ and $v_1 = v_2$ since B_1 is linearly independent. Thus V is a basis of cardinality $|B_1 \times B_2| = \dim_K V \cdot [K : F]$ as required. ∎

In particular if $E/K/F$ are field extensions then

$$[E : F] = [E : K] \cdot [K : F]$$

this is called the *multiplicity of dimension*.

1.2 Constructing Fields

Recall the following methods of constructing fields:

(1) If R is a commutative ring and $M \lhd R$ is a maximal ideal that ${}^{R}\!/_{M}$ is a field. In particular if F is a field, $R = F[x]$, and p is an irreducible polynomial then (p) is maximal and so ${}^{F[x]}\!/_{(p)}$ is a field.

(2) If F is a field, so is the field of rational functions:

$$F \subseteq F(x) := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in F[x], g \neq 0 \right\}$$

(3) If C is a chain of fields (meaning that for every $F, F' \in C$ either $F \subseteq F'$ or $F' \subseteq F$), then $\bigcup_{F\in C} F$ is also a field (the theory of fields is *inductive*). So for example $F(\lambda_1, \lambda_2, \dots)$ is a field, the union of the chain $F_n = F(\lambda_1, \dots, \lambda_n)$, the field of rational functions over F_{n-1}.

(4) If C is a chain of fields, then $\bigcap_{F\in C} F$ is also a field.

Definition 1.2.1

Let K/F be a field extension and $a \in K$, then denote $F(a)$ the smallest subfield of K containing both F and a.

It is not hard to see that

$$F(a) = \left\{ \frac{f(a)}{g(a)} \;\middle|\; f, g \in F[x], g(a) \neq 0 \right\}$$

Though we can actually get a simpler structure for $F(a)$.

Definition 1.2.2

Let K/F be a field extension with $a \in K$, then define the **evaluation homomorphism** at a to be the homomorphism $\psi_a \colon F[x] \longrightarrow K$ defined by $\psi_a(s) = s$ for $s \in F$ and $\psi_a(x) = a$. This uniquely defines

$$\psi_a\left(\sum \alpha_i x^i\right) = \sum \alpha_i a^i$$

Definition 1.2.3

Let K/F be a field extension, then $a \in K$ is **transcendental** if the kernel of the evaluation homomorphism is trivial: $\ker \psi_a = 1$. Otherwise a is **algebraic**.

If a is transcendental then $\ker \psi_a = 1$ and so by the isomorphism theorem

$$\mathrm{Im}\psi_a = \{f(a) \mid f \in F[x]\} = F[a] \cong {}^{F[x]}\big/_{\ker \psi_a} \cong F[x]$$

In fact we can extend ψ_a to a homomorphism $F(x) \longrightarrow F(a)$, and we similarly get an isomorphism $F(x) \cong F(a)$. Thus in the case that a is transcendental, we get

$$\begin{array}{ccccccc} F & \subseteq & F[a] & \subseteq & F(a) & \subseteq & K \\ & & \cong & & \cong & & \\ & & F[x] & & F(x) & & \end{array}$$

Otherwise, suppose a is algebraic. Since $F[x]$ is a Euclidean domain, it is a PID, and therefore every ideal is a prime ideal. In particular $\ker \psi_a$ must be generated by some polynomial h_a. This means that $\ker \psi_a = (h_a) = h \cdot F[x]$, and so $h_a(a) = 0$ and if $f(a) = 0$ as well then h_a divides f. h_a is therefore called the *minimal polynomial* of a.

Now if $n = \deg h$ then $F[a] = \mathrm{span}\{1, a, \dots, a^{n-1}\}$ since if $f \in F[x]$ then $f = h_a q + r$ for $\deg r < n$ by Euclidean division, and so $f(a) = r(a)$. And $r(x)$ is in $\mathrm{span}\{1, \dots, a^{n-1}\}$ due to its dimension being at most $n-1$. Thus $\{1, \dots, a^{n-1}\}$ spans $F[a]$, and it is a basis since any linear combination cannot be zero as $h_a(x)$ is minimal and has degree n. Therefore $F[a]$ is a F-linear space of dimension n.

Notice that

$$ {}^{F[x]}\big/_{(h_a)} = {}^{F[x]}\big/_{\ker \psi_a} \cong \mathrm{Im}\psi_a = \{f(a) \mid f \in F[x]\} = F[a] = \mathrm{span}\{1, \dots, a^{n-1}\} \subseteq K$$

Since K is an integral domain, so is $F[a]$. Therefore (h_a) is a prime ideal, since a quotient ring is an integral domain iff the ideal is prime. Since $F[x]$ is a PID, prime and maximal ideals are the same, so (h_a) is maximal and therefore $F[a]$ is a field.

So we have proven

Proposition 1.2.4

Let K/F be a field extension and $a \in K$ algebraic in F. Let h_a be a's minimal polynomial over F, then

(1) h_a is irreducible,

(2) $F[a]$ is a field,

(3) $[F[a] : F] = n = \deg h_a$ and has a basis $\{1, a, \ldots, a^{n-1}\}$.

In particular we have shown that when a is algebraic, $F(a) = F[a]$.

Proposition 1.2.5

Suppose $F \subseteq K$ where F is a field and K is an integral domain. Further suppose $[K : F]$ is finite. Then every element of K is algebraic and K is a field.

Proof: let $a \in K$, then

$$[K : F] = [K : F[a]] \cdot [F[a] : F]$$

meaning $[F[a] : F]$ must be finite and so a must be algebraic (as otherwise $F[a] \cong F[x]$ which has infinite degree). Since $F[a]$ is a field, it must have a multiplicative inverse for a, meaning K is a field. ■

Notice that $[F[a,b] : F[a]] \leq [F[b] : F]$, since the minimal polynomial of b relative to F, h_b, is also a zeroing a polynomial of b over $F[a]$. And so $[F[a,b] : F[a]] \leq \deg h_b = [F[b] : F]$. Thus we have that by multiplicity

$$[F[a,b] : F] = [F[a,b] : F[a]] \cdot [F[a] : F] \leq [F[b] : F] \cdot [F[a] : F]$$

And inductively we can show

Proposition 1.2.6

Suppose K/F is a field extension and $a_1, \ldots, a_n$ then

$$[F[a_1, \ldots, a_n] : F] \leq \prod_{i=1}^{n} [F[a_i] : F]$$

Definition 1.2.7

Call a field extension K/F **algebraic** if every $a \in K$ is algebraic over F.

Lemma 1.2.8

Suppose $F_3/F_2/F_1$ are field extensions such that F_2/F_1 is algebraic and $a \in F_3$ is algebraic over F_2. Then it is also algebraic over F_1.

Proof: there exists an $f \in F_2[x]$ such that $f(a) = 0$. Suppose $f = \sum b_i x^i$, then a is algebraic over $F_1[b_0, \ldots, b_n]$. Then

$$[F_1[b_0, \ldots, b_n, a] : F_1] = [F_1[b_0, \ldots, b_n, a] : F_1[b_0, \ldots, b_n]] \cdot [F_1[b_0, \ldots, b_n] : F_1]$$

and since a is algebraic over $F_1[b_0, \ldots, b_n]$ and $b_i \in F_2$ are algebraic over F_1, the right-hand side is finite. Thus a is algebraic over F_1 by the left-hand side, as required. ■

Theorem 1.2.9

Let K/F be a field extension, then

$$\mathrm{Alg}_F(K) := \{a \in K \mid a \text{ is algebraic over } F\}$$

is a field. Furthermore, every element in $K \setminus \mathrm{Alg}_F(K)$ is transcendental over $\mathrm{Alg}_F(K)$.

Proof: notice that $F[a \cdot b], F[a+b] \subseteq F[a,b]$ and $[F[a,b] : F] \leq [F[a] : F] \cdot [F[b] : F] < \infty$ for $a, b \in \mathrm{Alg}_F(K)$. So $\mathrm{Alg}_F(K)$ is closed under addition and multiplication. It is also obviously closed under additive inverses since $F[-a] = F[a]$. And since $F[a]$ is a field, $a^{-1} \in F[a]$ so $F[a^{-1}] \subseteq F[a]$ and thus $[F[a^{-1}] : F] \leq [F[a] : F] < \infty$, so a^{-1} is algebraic over F. So $\mathrm{Alg}_F(K)$ is indeed a field.

Now suppose $a \in K \setminus \mathrm{Alg}_F(K)$ is algebraic over $\mathrm{Alg}_F(K)$. Then by the above lemma, it is algebraic over F since $\mathrm{Alg}_F(K)/F$ is trivially algebraic. But then $a \in \mathrm{Alg}_F(K)$ by definition, in contradiction. ■

1.3 Splitting Fields

Proposition 1.3.1

Let F be a field and $f \in F[x]$ be an irreducible polynomial. Then there exists a field extension K/F such that f has a root in K and $[K : F] = \deg f$.

Proof: since f is irreducible, (f) is maximal (since $F[x]$ is a PID so prime ideals are maximal). Thus $K = {}^{F[x]}\big/_{(f)}$ is a field. The dimension of K is $\deg f$ since it has a basis $\left\{1, x, \ldots, x^{\deg f - 1}\right\}$.

By the second isomorphism theorem,

$$ {}^{F}\big/_{F \cap (f)} \cong {}^{F + (f)}\big/_{(f)} \subseteq {}^{F[x]}\big/_{(f)} = K $$

But $F \cap (f) = 0$, and so ${}^{F}\big/_{F \cap (f)} = {}^{F}\big/_{0} \cong F$. Thus we can embed F into K, so we can view K/F as a field extension.

Now, define $\alpha = x + (f)$, and suppose $f(x) = \sum_{i=0}^{n} a_i x^i$ for $a_i \in F$. Then

$$ f(\alpha) = \sum_{i=0}^{n} a_i \big(x + (f)\big)^i = \sum_{i=0}^{n} a_i (x^i + (f)) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} a_i (f) = f + (f) = 0 $$

Thus α is a root of f in K. ■

Corollary 1.3.2

Let F be a field and $f \in F[x]$ a polynomial. Then there exists a field extension K/F such that f has a root in K and $[K : F] \leq \deg f$.

Proof: take an irreducible factorization of f and apply the above result to one of its factors. ■

Definition 1.3.3

Suppose F is a field and $f \in F[x]$. Then f **splits** in F if there exist $\alpha_1, \ldots, \alpha_n \in F$ such that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$.

Proposition 1.3.4

Let $f \in F[x]$ then there exists a field extension K/F such that f splits in K and $[K : F] \leq (\deg f)!$.

Proof: by induction on $n = \deg f$. For $n = 1$, f is linear and thus has a root so we can take $K = F$. Now suppose $\deg f = n + 1$, then by corollary 1.3.2 there exists a field extension K_0/F such that f has a root in K_0 and $[K_0 : F] \leq n + 1$. Now suppose $\alpha \in K_0$ is a root of f, then there exists a $g(x) \in K_0[x]$ such that $(x - \alpha) g(x) = f(x)$ and so $\deg g \leq n$. Therefore inductively there is a field extension K/K_0 which splits $g(x)$ and thus $f(x)$ and

$$ [K : F] = [K : K_0] \cdot [K_0 : F] \leq n! \cdot (n+1) = (n+1)! $$

as required. ■

Definition 1.3.5

Suppose K/F is a field extension and $\varphi\colon F \hookrightarrow E$ is an embedding into some other field E. Then an **extension** of φ to K is an embedding $\overline{\varphi}\colon K \hookrightarrow E$ such that $\overline{\varphi}\big|_F = \varphi$ ($\overline{\varphi}$ is equal to φ on F). Let us then define

$$\eta^{\varphi}_{K/F} := \#\{\overline{\varphi} \mid \overline{\varphi} \text{ is an extension of } \varphi\}$$

In other words, an extension is an embedding $\overline{\varphi}$ such that the following diagram commutes:

$$\begin{tikzcd} & E & \\ F \arrow[ur, "\varphi"] \arrow[rr, "\iota"] & & K \arrow[ul, "\overline{\varphi}"'] \end{tikzcd}$$

Where $\iota\colon F \longrightarrow K$ is the inclusion embedding.

Suppose f, g are two field homomorphisms $F(a_1, \ldots, a_n) \longrightarrow K$ such that $f(x) = g(x)$ for all $x \in F$ and $f(a_i) = g(a_i)$ for $1 \leq i \leq n$. Then $f(x) = g(x)$ on all of $F(a_1, \ldots, a_n)$. This is since $\{r \in F(a_1, \ldots, a_n) \mid f(r) = g(r)\}$ is a field containing F and $a_1, \ldots, a_n$ and thus $F(a_1, \ldots, a_n)$.

In particular if $\varphi\colon F \hookrightarrow E$ is an embedding, then an extension $\overline{\varphi}\colon F(a_1, \ldots, a_n) \longrightarrow E$ is defined entirely by its image on $a_1, \ldots, a_n$.

Proposition 1.3.6

Suppose $K = F[\alpha]$, then $\eta^{\varphi}_{K/F}$ is equal to the number of distinct roots the minimal polynomial of α has in E. Formally, if $h(x) = \sum_{i=0}^n a_i x^i$ then define $\hat{h}(x) = \sum_{i=0}^n \varphi(a_i)x^i$, and $\eta^{\varphi}_{K/F}$ is equal to the number of roots $\hat{h}(x)$ has in E.

In particular $\eta^{\varphi}_{K/F}$ is independent of the choice of φ.

Proof: let $h(x) \in F[x]$ be the minimal polynomial of α, and $\overline{\varphi}$ be an extension of φ to K, then

$$\hat{h}(\overline{\varphi}(\alpha)) = \sum_{i=0}^n \varphi(a_i)\overline{\varphi}(\alpha)^i = \sum_{i=0}^n \overline{\varphi}(a_i)\overline{\varphi}(\alpha^i) = \overline{\varphi}\left(\sum_{i=0}^n a_i\alpha^i\right) = \overline{\varphi}(h(\alpha)) = \overline{\varphi}(0) = 0$$

Thus $\overline{\varphi}(\alpha)$ must be a root of $\hat{h}(x)$, and as explained above extensions of embeddings to $K = F[\alpha]$ are dependent only on their image of α. So there are at most as many extensions as there are distinct roots of $\hat{h}$.

Now suppose $\beta \in E$ is a root of $\hat{h}$, then we claim that there exists an extension with $\overline{\varphi}(\alpha) = \beta$. Indeed, $\alpha \notin F$ and β is not in the image of φ (as then $0 = \hat{h}(\varphi(a)) = \varphi(\hat{h}(a))$ so a is a root of $\hat{h}(x)$ but $\hat{h}$ is irreducible), so this is well-defined. ■

Definition 1.3.7

A polynomial f which splits over E is called **separable** over E if its linear factors are all distinct (ie. it has $n = \deg f$ distinct roots in E).

When we have an embedding $\varphi\colon F \hookrightarrow E$ and a polynomial $f \in F[x]$ and we say that f has some property in E (eg. splits over E, separable over E), then we mean that its image under φ has that property. Meaning if $f(x) = \sum_{i=0}^n a_i x^i$ then $\sum_{i=0}^n \varphi(a_i)x^i$ has said property.

Theorem 1.3.8

Let K/F be a finite extension, and let $\varphi\colon F \hookrightarrow E$ be an embedding. Then

(1) $\eta^{E}_{K/F} \leq [K : F]$;

(2) if $K = F[\alpha_1, \ldots, \alpha_n]$ where α_i are roots of some $f \in F[x]$ which splits over E, then $1 \leq \eta^{\varphi}_{K/F}$.

Meaning there exists at least one extension of φ to K;

(3) if f is also separable over E, then $\eta^{\varphi}_{K/F} = [K : F]$.

Proof: since K/F is finite, we have that $K = F[\alpha_1, \dots, \alpha_n]$ (we can take $\{\alpha_1, \dots, \alpha_n\}$ to be a basis for K as a F-linear space).

(1) We proceed inductively on n. For $n = 1$, by the previous proposition $\eta^{\varphi}_{K/F}$ is equal to the number of roots h_{α_1} (the minimal polynomial of α_1) has in E.
For the inductive step, define $F_1 = F[\alpha_1]$, and so

$$\begin{aligned}\eta^{\varphi}_{K/F} &= \#\{\varphi'' \colon K \longrightarrow E \text{ is an extension of } \varphi\} \\ &= \#\bigcup\{\varphi'' \colon K \longrightarrow E \text{ is an extension of } \varphi' \mid \varphi' \colon F_1 \longrightarrow E \text{ is an extension of } \varphi\} \\ &= \sum_{\varphi'} \eta^{\varphi'}_{K/F_1}\end{aligned}$$

By our inductive hypothesis, $\eta^{\varphi'}_{K/F_1} \leq [K : F_1]$ and $\eta^{\varphi}_{F_1/F} \leq [F_1 : F]$ so

$$\leq \sum_{\varphi'} [K : F_1] = [F_1 : F] \cdot [K : F] = [K : F]$$

as required.

(2) Again, we proceed inductively on n. For $n = 1$, $K = F[\alpha]$ and $\eta^{\varphi}_{K/F}$ is equal to the number of roots h_α has in E. But since $f(\alpha) = 0$ and h_α is minimal, h_α must divide f and therefore split in E, meaning it has at least one root in E. So $1 \leq \eta^{\varphi}_{K/F}$ as required.
Inductively, set $F_1 = F[\alpha_1]$ and so there exists an extension of φ to $\varphi' \colon F_1 \hookrightarrow E$ by our base case. And there then exists an extension of φ' to $\varphi'' \colon K \hookrightarrow E$, so there exists at least one extension as required.

(3) If we review the proof of (2), for the base case we must have that f is separable and splits in E, which means that h_α does as well. Then h_α has precisely $\deg h_\alpha$ distinct roots in E, so $\eta^{\varphi}_{K/F} = \deg h_\alpha = [K : F]$ as required. The rest of the proof proceeds similarly. ■

Definition 1.3.9

Let $f \in F[x]$ be any polynomial over F. Then a field $F \subseteq K$ is called a **splitting field** if f splits over K and it contains no other field over which f splits (meaning it is the smallest field which splits f).

Notice that if K is a splitting field of $f \in F[x]$, then K is of the form $K = F[\alpha_1, \dots, \alpha_n]$ where α_i are roots of f in K. Then

$$[K : F] \leq \prod_{i=1}^{n} [F[\alpha_i] : F] < \infty$$

so K/F is a finite extension. And such a finite field exists: we know there exists a field extension F_1 such that f has a root α_1 in F_1, so there must be an extension F_2/F_1 such that $f/(x - \alpha)$ has a root α_2 in F_2, and we continue inductively. This gives us a field F_n with roots $\alpha_1, \dots, \alpha_n$ and so defining $K = F[\alpha_1, \dots, \alpha_n]$ gives us a splitting field.

Theorem 1.3.10

Any two splitting fields of a polynomial $f \in F[x]$ are isomorphic.

Proof: let K be a splitting field of f, and suppose f splits in E, where $F \subseteq E$. By the above theorem, there must exist an extension of the inclusion embedding $F \hookrightarrow E$ to an embedding $K \hookrightarrow E$. This embedding gives rise to an embedding of F-linear spaces, meaning $[K : F] \leq [E : F]$. In particular, if E is another splitting field of f then $[E : F] \leq [K : F]$ as well, so that K and E are isomorphic F-linear spaces, and thus are isomorphic as fields. ■

Definition 1.3.11

Let $f(x) = \sum_{k=0}^{n} a_k x^k \in F[x]$ be a polynomial. We define its **formal derivative** to be the polynomial

$$f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$$

It is not hard to prove that $(f+g)' = f' + g'$ and $(f \cdot g)' = f'g + fg'$.

Lemma 1.3.12

Let $f, g \in F[x]$ and define $r(x) = \gcd(f, g)$. Then $r(x)$ is the gcd of f and g over *every* field extension K/F.

Proof: let $r_K(x)$ be the gcd of f, g over K. Since $r(x)$ still divides f, g we have that $r(x) | r_K(x)$. And by Euclid's algorithm there exist $a(x), b(x) \in F[x]$ such that

$$r(x) = a(x)f(x) + b(x)g(x)$$

But $r_K(x)$ divides f, g so it divides $r(x)$. Thus $r_K(x) = r(x)$ as required. ■

Theorem 1.3.13

Let $f \in F[x]$ be a polynomial, then f is separable if and only if $\gcd(f, f') = 1$.

Proof: let K be a splitting field of f. Suppose f is not separable, then it has the form $f(x) = (x-\alpha)^m g(x)$ for $g(x) \in K[x]$ and $m > 1$. But then $f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x)$ and so $x - \alpha$ is a common factor of both f and f' so $\gcd(f, f') \neq 1$ in $K[x]$, but the gcd of f, f' in F is equal to its gcd in K by the above lemma.
Alternatively if f is separable, then $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$ and so

$$f'(x) = \sum_{j=1}^{n} \prod_{\substack{1 \leq i \leq n \\ i \neq j}} (x - \alpha_i)$$

But the irreducible factors of f, which are $x - \alpha_i$, do not divide $f'(x)$ since no two roots are equal. Thus $\gcd(f, f') = 1$. ■

Recall that for any ring R, there is a unique homomorphism $\varphi \colon \mathbb{Z} \longrightarrow R$. In particular if F is a field then $\mathbb{Z}/\ker\varphi \cong \mathrm{Im}\varphi \subseteq F$. Since F is a field, $\mathrm{Im}\varphi$ is an integral domain and so $\ker\varphi$ is a prime ideal of $\mathbb{Z}$, meaning $\ker\varphi = (p)$ for some prime p or 0. This is called the *characteristic* of F.
Since $\varphi(n) = 1 + \cdots + 1$, the characteristic of F is simply the prime p such that $\varphi(p) = 0$, ie. $1 + \cdots + 1 = 0$ (p times), or 0 if no such primes exist.

Definition 1.3.14

The **characteristic** of a field F is the unique positive generator of the kernel of $\varphi \colon \mathbb{Z} \longrightarrow F$. Equivalently it is the minimum number p such that $1 + \cdots + 1 = 0$ (p times), or 0 if no such p exists.

If F has characteristic 0, then φ is an embedding so we can view $\mathbb{Z}$ as a subfield of F. But then the field generated by $\mathbb{Z}$ must also be a subfield of (embeddable into) F, meaning $\mathbb{Q} \subseteq F$. Similarly for fields of characteristic $p > 0$, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subseteq F$.
Notice that for fields of characteristic p, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is zero for $k \neq 0, p$. Thus:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k} = a^p + b^p$$

So $x \mapsto x^p$ is a homomorphism, called the *Frobenius homomorphism*. It can be viewed as a homomorphism to $F^p = \{x^p \mid x \in F\}$ (which is a field precisely because the Frobenius homomorphism is a homomorphism). The homomorphism has a trivial kernel, so $F \cong F^p$. In particular every element of F is of the form x^p.

Theorem 1.3.15

Let $f \in F[x]$ be an irreducible polynomial, then the following are equivalent:

(**1**) f is not separable (has a multiple root),

(**2**) F has a characteristic $p > 0$, and $f(x) = g(x^p)$ for some $g \in F[x]$,

(**3**) every root of f is a multiple root.

Proof: (1) $\implies$ (2): by theorem 1.3.13 we have that $\gcd(f, f') \neq 1$. But f is irreducible and thus has no nontrivial divisors, so $f' = 0$. But since f is nonconstant, we must have that F is of characteristic p (since in characteristic 0 a nonconstant polynomial cannot have a zero derivative).

Now, if $f(x) = \sum_{k=0}^{n} a_k x^k$ then $ka_k = 0$ for all k since $f'(x) = 0$. So for k not divisible by p, this means that $k \neq 0$ and so $a_k = 0$. Thus

$$f(x) = \sum_{p|k} a_k x^k = \sum_j a_{pj} x^{pj}$$

so define $g(x) = \sum_j a_{pj} x^j$ and we have the desired result.

(2) $\implies$ (3): take a splitting field of $g(x)$, then write $g(x) = a \prod_i (x - a_i)^{m_i}$. Then we have that $f(x) = a \prod_i (x^p - a_i)^{m_i}$. We can extend this to a field with p-roots of a_i (which are roots of $x^p - a_i$), α_i, and so over this field $f(x) = a \prod_i (x - \alpha_i)^{pm_i}$. So all the roots of f have a multiplicity greater than 1.

(3) $\implies$ (1) is trivial. ■

2 Galois Groups

2.1 Galois Groups

Definition 2.1.1

Let K/F, K'/F be field extensions, then a homomorphism $\varphi\colon K \longrightarrow K'$ is called a **F-homomorphism** if $\varphi(a) = a$ for all $a \in F$. φ is an **F-automorphism** if $K = K'$ and φ is an automorphism.

Notice that if φ is a field homomorphism, then it is injective since its kernel is an ideal, and the only ideals of a field are F and 0. Since a homomorphism must map 1 to 1, its kernel cannot be F, meaning it must be injective. Thus to validate that $\varphi\colon K \longrightarrow K$ is an automorphism, we need to check only that it is surjective.

Furthermore, if $\varphi\colon K \longrightarrow K$ is an F-homomorphism, then it is an injective linear operator on K. If $[K : F]$ is finite, we know from linear algebra that φ is then surjective. So over finite field extensions, all F-endomorphisms (homomorphisms over a field) are automorphisms.

Definition 2.1.2

Let K/F be a field extension, then we define its **Galois group** to be

$$\mathrm{Gal}(K/F) := \{\sigma\colon K \longrightarrow K \mid \sigma \text{ is an } F\text{-automorphism}\}$$

Let $f \in F[x]$ with a root $\alpha \in K$ and $\sigma \in \mathrm{Gal}(K/F)$. Then we know that

$$f(\sigma(a)) = \sigma(f(a)) = \sigma(0) = 0$$

thus F-automorphisms must permute the roots of polynomials.

Proposition 2.1.3

Let K/F be a field extension and $f \in F[x]$ be irreducible with roots $a, b \in K$. Then there exists an F-isomorphism $\varphi\colon F[a] \longrightarrow F[b]$.

Proof: the inclusion map $\iota\colon F \longrightarrow F[b]$ can be extended to $\iota\colon F[x] \longrightarrow F[b]$ by $\iota(x) = b$. This is obviously surjective, and its kernel is all polynomials g such that $g(b) = 0$. Since f is the minimal polynomial of b, we have that $\ker\iota = (f)$, and so by the first isomorphism theorem there is an isomorphism

$$\varphi\colon {}^{F[x]}\big/_{(f)} \longrightarrow F[b]$$

similarly we can construct an isomorphism

$$\psi\colon {}^{F[x]}\big/_{(f)} \longrightarrow F[a]$$

then our desired isomorphism is $\varphi\psi^{-1}$. ∎

Recall from theorem 1.3.8 that if K/F is a field extension and $\iota\colon F \longrightarrow K$ the inclusion map, then

$$\eta^{\iota}_{K/F} \leq [K : F]$$

but extensions of ι to embeddings $K \hookrightarrow K$ are precisely the F-homomorphisms. Meaning $|\mathrm{Gal}(K/F)| \leq \eta^{\iota}_{K/F}$, and this is an equality when $[K : F]$ is finite since F-homomorphisms are automorphisms over finite dimensional vector spaces. So $|\mathrm{Gal}(K/F)| \leq [K : F]$.

Furthermore, if K is the splitting field of some $f \in F[x]$ which is also separable in K then by the same theorem, $|\mathrm{Gal}(K/F)| = [K : F]$. Let us summarize this:

Proposition 2.1.4

If K/F is a finite extension, then $|\mathrm{Gal}(K/F)| \leq [K : F]$. And if furthermore K is the splitting field of some separable polynomial $f \in F[x]$, then this becomes an equality.

In the future we will generalize this result: in fact $|\mathrm{Gal}(K/F)| = [K : F]$ if and only if K is the splitting field of some separable polynomial.

Example 2.1.5

Compute $\mathrm{Gal}\big(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}\big)$.

Notice that $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is the splitting field of $(x^2 - 2)(x^2 - 3)$, which is also separable. So by the above proposition

$$|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = [E : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$$

We know that $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ and so $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. And $x^2 - 3$ is a zeroing polynomial of $\sqrt{3}$ in E, and since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$, we have that $[E : \mathbb{Q}[\sqrt{2}]] = 2$. Thys $|\mathrm{Gal}(E/\mathbb{Q})| = 4$.

And as we know, every F-automorphism is defined entirely by where it maps $\sqrt{2}$ and $\sqrt{3}$. We know that $\sqrt{2}$ must map to $\pm\sqrt{2}$ because these are the roots of $x^2 - 2$. And $\sqrt{3}$ must map to $\pm\sqrt{3}$. This gives us exactly 4 automorphisms, and so we have found all the elements of $\mathrm{Gal}(E/\mathbb{Q})$.

If we denote $\sqrt{2}$ by 1, $-\sqrt{2}$ by 2, $\sqrt{3}$ by 3, and $-\sqrt{3}$ by 4 we can embed $\mathrm{Gal}(E/\mathbb{Q})$ in S_4 as follows:

(1) the automorphism $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$ corresponds to the transposition $(1, 2)$;

(2) the automorphism $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$ corresponds to the identity.

(3) the automorphism $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$ corresponds to the permutation $(1, 2)(3, 4)$;

(4) the automorphism $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$ corresponds to the transposition $(3, 4)$;

This is the Klein four-group V, and so

$$\mathrm{Gal}\Big(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}\Big) \cong V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \blacksquare$$

Notice that if F is the *prime field* of K (meaning $F = \mathbb{F}_p$ if K is of characteristic $p > 0$, and $F = \mathbb{Q}$ if $p = 0$), then every automorphism of K must keep F constant, since $\sigma(n) = \sigma(1) + \cdots + \sigma(1) = n$ and $\sigma(a/b) = \sigma(a)/\sigma(b) = a/b$. Thus every automorphism of K is an F-automorphism automatically, meaning in the case that F is K's prime field:

$$\mathrm{Aut}(K) = \mathrm{Gal}(K/F)$$

Definition 2.1.6

Let K be a field and $G \leq \mathrm{Aut}(K)$ a subgroup of K's automorphisms, then define the **fixed-point field**

$$K^G := \{a \in K \mid \forall \sigma \in G \colon \sigma(a) = a\}$$

The fixed point field is indeed a field, as is easily verified.

Notice the following properties:

(1) If $F_2 \subseteq F_1$ then $\mathrm{Gal}(K/L_2) \supseteq \mathrm{Gal}(K/L_1)$ since any L_1-automorphism must necessarily also keep L_2 constant.

(2) If $H_2 \subseteq H_1$ then $K^{H_2} \supseteq K^{H_1}$ since if a is held constant by every $\sigma \in H_1$, then it must also be held constant by every $\sigma \in H_2$.

(3) For every F, $F \subseteq K^{\mathrm{Gal}(K/F)}$ since by definition, every element of F must be held constant by an F-automorphism.

(4) For every H, $H \subseteq \operatorname{Gal}\big(K/K^H\big)$ since every automorphism in H must be a K^H-automorphism, since it by definition holds elements of K^H constant.

Notice then that if L is an intermediate field of K/F (meaning $K/L/F$), $\operatorname{Gal}(K/L)$ is a subgroup of $\operatorname{Gal}(K/F)$, since $F \subseteq L$. And conversely, if H is a subgroup of $\operatorname{Gal}(K/F)$ then H is an intermediate field of K/F, since F is necessarily contained in K^H.

So we have the following correspondence between objects:

$$\begin{tikzcd}
\{\text{Subgroups of } \operatorname{Gal}(K/F)\} \arrow[r, bend right, mapsto, "K^\bullet"'] & \{\text{Intermediate fields of } K/F\} \arrow[l, bend right, mapsto, "\operatorname{Gal}(K/\bullet)"']
\end{tikzcd}$$

Definition 2.1.7

Let X and Y be two posets (partially ordered sets), then a pair of functions $\alpha\colon X \longrightarrow Y$ and $\beta\colon Y \longrightarrow X$ is a **Galois correspondence** if

(1) α and β reverse order, meaning if $x_1 \leq x_2$ then $\alpha(x_1) \leq \alpha(x_2)$ and similar for β;

(2) for every $x \in X$ and $y \in Y$, $x \leq \beta(\alpha(x))$ and $y \leq \alpha(\beta(y))$.

For example (in fact, this is *the* example), $\alpha\colon F \mapsto \operatorname{Gal}(K/F)$ and $\beta\colon H \mapsto K^H$ is a Galois correspondence by the properties above.

Proposition 2.1.8

α, β form a Galois correspondence if and only if for all $x \in X$ and $y \in Y$, $y \leq \alpha(x) \iff x \leq \beta(y)$.

Proof: suppose α, β form a Galois correspondence. Then if $x \leq \beta(y)$ then $y \leq \alpha(\beta(y)) \leq \alpha(x)$ (both inequalities are due to the correspondence being Galois: the first is by (2) and the second is by (1)). The proof for α is similar.

Conversely, since $\beta(y) \leq \beta(y)$ we get that $y \leq \alpha(\beta(y))$ (setting $x = \beta(y)$). And similar for α. Now if $x \leq x'$ then $x \leq x' \leq \beta(\alpha(x'))$, so setting $y = \alpha(x')$ we have $x \leq \beta(y)$ and so $y \leq \alpha(x)$, meaning $\alpha(x') \leq \alpha(x)$ as required. ■

Proposition 2.1.9

Let α, β be a Galois correspondence, then

(1) $\alpha \circ \beta \circ \alpha = \alpha$ and $\beta \circ \alpha \circ \beta = \beta$,

(2) $\beta(\alpha(x)) = x$ if and only if $x \in \operatorname{Im}(\beta)$ and $\alpha(\beta(y)) = y$ if and only if $y \in \operatorname{Im}\alpha$,

(3) α and β are inverse functions between $\operatorname{Im}\beta$ and $\operatorname{Im}\alpha$.

Proof:

(1) Since $x \leq \beta\alpha x$, we have $\alpha x \geq \alpha\beta\alpha x$ Conversely, let $y = \alpha x$ then this means $y \leq \alpha\beta y$, and so $\alpha x \leq \alpha\beta\alpha x$ as required. Similar for $\beta\alpha\beta$.

(2) If $\alpha\beta(y) = y$ then trivially $y \in \operatorname{Im}\alpha$, and if $y \in \operatorname{Im}\alpha$ then $y = \alpha x$ and so $\alpha\beta(y) = \alpha\beta\alpha(x) = \alpha(x) = y$ by (1).

(3) This is direct from (2). ■

Definition 2.1.10

An extension K/F is

(1) **Separable** if it is algebraic and the minimal polynomial of every $a \in K$ is separable.

(2) **Normal** if it is algebraic and the minimal polynomial of every $a \in K$ splits over K.

(3) **Galois** if it is both separable and normal. Meaning every minimal polynomial splits into distinct linear factors over K.

Lemma 2.1.11

Let K/F be an extension, $a, b \in K$ with minimal polynomials f_a and f_b respectively. Then $f_a = f_b$ or f_a, f_b are coprime (which is independent on what field we look at, since the gcd is the same).

Proof: suppose $f_a \neq f_b$. Then they can't share a root since because if they did then they would both be the minimal polynomial of said root. Now, let E be a splitting field of f_a, then since f_a splits into linear factors over E and these are all coprime with f_b since they don't share a root, the gcd in E of f_a and f_b is 1. But the gcd in a field extension is equal to the gcd in the field itself, so f_a and f_b are coprime. ■

Theorem 2.1.12

Let K/F be a finite extension, then the following are equivalent:

(1) K/F is Galois,

(2) K is the splitting field of some separable polynomial over F,

(3) $|\mathrm{Gal}(K/F)| = [K : F]$,

(4) $F = K^{\mathrm{Gal}(K/F)}$,

(5) $F = K^G$ for some $G \leq \mathrm{Gal}(K/F)$.

Proof: (1) $\implies$ (2): suppose $K = F[a_1, \dots, a_n]$ and let f_i be the minimal polynomial of a_i. Since K/F is Galois, each f_i splits into distinct linear factors over K. Define $f = \prod_i f_i$ where we remove repetitions, and by the above lemma these are all coprime and in particular do not share roots. Therefore f is separable. K is generated by the roots of f and is therefore its splitting field, as required.

(2) $\implies$ (3): we proved this in proposition 2.1.4.

(5) $\implies$ (1): let $a \in K$ and f be its minimal polynomial. Let $a_1, \dots, a_n$ be the distinct roots of f in K, then define $h = \prod_i (x - a_i) \in K[x]$. Obviously we have that h divides f. Now, we know that $\sigma \in G$ permutes roots of f, and so $h \in \big(K[x]\big)^G = K^G[x] = F[x]$.

(3) $\implies$ (4): let $G = \mathrm{Gal}(K/F)$ and define $F' = K^G$, so F' satisfies (5) which implies (1), meaning K/F' is Galois. And we showed that (1) implies (3), meaning $|\mathrm{Gal}(K/F')| = [K : F']$. Now, we know that $\mathrm{Gal}(K/F') = \alpha\beta\alpha(F) = \mathrm{Gal}(K/F)$ so we have that

$$[K : F] = |\mathrm{Gal}(K/F)| = |\mathrm{Gal}(K/F')| = [K : F']$$

and $F \subseteq F'$, meaning $F = F'$ as required.

(4) $\implies$ (5) is trivial. ■

If $K/L/F$ is an extension such that K/F is Galois, then K/L is also Galois. This is since for $a \in K$, let h_a^F and h_a^L be the minimal polynomials of a in F and L respectively. We know that h_a^F splits into distinct linear factors over K, and since h_a^L must divide it, it does too. So K/L is also Galois. In particular $K^{\mathrm{Gal}(K/L)} = L$.

So if we once again look at our Galois correspondence,

$$\{\text{Subgroups of } \mathrm{Gal}(K/F)\} \underset{\beta = K^{\bullet}}{\overset{\alpha = \mathrm{Gal}(K/\bullet)}{\rightleftarrows}} \{\text{Intermediate fields of } K/F\}$$

In particular, we have that $\beta\alpha = \mathrm{id}$. We have shown then that for every $K/L/F$ Galois, there exists a subgroup $G \leq \mathrm{Gal}(K/F)$ such that $K^G = L$. But then we can ask, for which subgroups $H \leq G$ is there an intermediate field L such that $\mathrm{Gal}(K/L) = H$?

Lemma 2.1.13 (Artin's Lemma)

Let $H \leq \mathrm{Aut}(K)$ be a finite subgroup, then $[K : K^H] \leq |H|$.

Proof: suppose $H = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$, and take any $x_1, \ldots, x_m \in K$ for any m larger than n. We need to show that $x_1, \ldots, x_m$ is linearly dependent over K^H. Meaning we need to find $a_1, \ldots, a_m \in K^H$ such that $\sum_i a_i x_i = 0$. If we apply $\sigma_i \in H$ to this sum, since $a_j \in K^H$, we get

$$\sigma_i\left(\sum_j a_j x_j\right) = \sum_j a_j \sigma_i(x_j) = 0$$

Let X be the $n \times m$ matrix defined by $X = (\sigma_i(x_j))_{ij}$ and define $\vec{a} = (a_1, \ldots, a_m)^\top$. So we need to solve

$$X\vec{a} = 0$$

But $X \in M_{n\times m}(K)$, and since $m > n$, it has a nontrivial nullspace. So there exists a $\vec{a} \in K^m$ which solves this equation. But recall we need $\vec{a}$ to be a vector over K^H.

So let us choose a solution $\vec{a}$ whose number of zeroes is minimal (meaning $\#\{1 \leq i \leq m \mid a_i = 0\}$ is minimal). We can reorder indexes and assume that $a_1 \neq 0$, and so $a_1^{-1}\vec{a}$ is also solution with the same number of zeros, so we can assume $a_1 = 1$. We now claim that $a_i \in K^H$ for all i, and once we have proved this we have finished our proof.

Suppose that $a_i \notin K^H$, without loss of generality $i = 2$. So there exists a $\sigma_k \in K^H$ such that $\sigma_k(a_i) \neq a_i$. We know that $\sum_j a_j \sigma_i(x_j) = 0$ for all i, and so composing with σ_k we get

$$\sum_j \sigma_k(a_j)\sigma_{k+i}(x_j) = 0$$

for all i. But since composing with σ_k is an invertible operation, this means that $\sum_j \sigma_k(a_j)\sigma_i(x_j) = 0$ for all i. Thus $(1, \sigma_k(a_2), \ldots, \sigma_k(a_m))$ is also a solution to $X\vec{a} = 0$. And thus

$$(1, a_2, \ldots, a_m) - (1, \sigma_k(a_2), \ldots, \sigma_k(a_m)) = (0, a_2 - \sigma_k(a_2), \ldots, a_m - \sigma_k(a_m))$$

is also a solution to the system. It is non-trivial since $a_2 \neq \sigma_k(a_2)$, but it has fewer zeros than our first solution since if $a_i = 0$ then $a_i - \sigma_k(a_i) = 0$ still, and we made the first index 0. This is a contradiction to the fact that we chose our first solution to have a minimal number of zeros, completing the proof. ∎

So for a Galois extension K/F, if $H \leq \mathrm{Gal}(K/F)$ then by theorem 2.1.12, K^H is Galois and so $[K : K^H] = \left|\mathrm{Gal}\left(K/K^H\right)\right|$. And since $H \leq \mathrm{Gal}\left(K/K^H\right)$, we have that

$$|H| \leq \left|\mathrm{Gal}\left(K/K^H\right)\right| = [K : K^H] \leq |H|$$

where the final inequality is due to Artin's Lemma. Thus $\mathrm{Gal}\left(K/K^H\right) = H$. So we have proven

Theorem 2.1.14 (The Fundamental Theorem of Galois Theory)

Let K/F be a finite dimensional Galois extension. Then the Galois correspondence

$$\begin{tikzcd}
\{\text{Subgroups of } \mathrm{Gal}(K/F)\} \arrow[r, bend right, "\beta = K^\bullet"'] & \{\text{Intermediate fields of } K/F\} \arrow[l, bend right, "\alpha = \mathrm{Gal}(K/\bullet)"']
\end{tikzcd}$$

is a bijective correspondence (meaning α and β are inverses of one another).

Corollary 2.1.15

If K/F is a finite Galois extension, then there are only a finite number of intermediate fields.

Proof: the number of intermediate fields is $\mathrm{Gal}(K/F)$ which is $[K : F]$, finite. ■

Corollary 2.1.16

Let K/F be a finite Galois extension, $G = \mathrm{Gal}(K/F)$.

(1) if $H_1 \leq H_2$ then $[H_2 : H_1] = \left[K^{H_1} : K^{H_2}\right]$,

(2) for $\sigma \in G$, $H \leq G$, $L = K^H$, then $\sigma(L)$ corresponds to $\sigma H \sigma^{-1}$ in the Galois correspondence,

(3) $H \leq G$ is normal in G if and only if K^H/F is Galois. In such a case, $\mathrm{Gal}\big(E^H/F\big) \cong {}^{G}\!\big/_{H}$.

Proof:

(1) We know that

$$|H_2| = \left[K : K^{H_2}\right] = \left[K : K^{H_1}\right] \cdot \left[K^{H_1} : K^{H_2}\right] = |H_1| \cdot \left[K^{H_1} : K^{H_2}\right]$$

and so $[H_2 : H_1] = \frac{|H_2|}{|H_1|} = \left[K^{H_1} : K^{H_2}\right]$.

(2) We need to show that $\mathrm{Gal}(K/\sigma(L)) = \sigma H \sigma^{-1}$ and $K^{\sigma H \sigma^{-1}} = L$. But since we know that the correspondence is bijective, proving only the first equality is sufficient.

$$\begin{aligned}
\mathrm{Gal}(K/\sigma(L)) &= \{\varphi \in G \mid \forall \alpha \in L \colon \varphi(\sigma(\alpha)) = \sigma(\alpha)\} \\
&= \left\{\varphi \in G \;\middle|\; \forall \alpha \in L \colon \sigma^{-1}\varphi\sigma\alpha = \alpha\right\} \\
&= \left\{\varphi \in G \;\middle|\; \sigma\varphi\sigma^{-1} \in \mathrm{Gal}(K/L)\right\} \\
&= \sigma \,\mathrm{Gal}(K/L)\sigma^{-1} = \sigma H \sigma^{-1}
\end{aligned}$$

(3) Suppose first that $H \trianglelefteq G$ is normal in G. So $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$ and thus by (2),

$$\sigma(K^H) = K^{\sigma H \sigma^{-1}} = K^H$$

Thus the map $\sigma \mapsto \sigma\big|_{K^H}$ from G to $\mathrm{Gal}\big(K^H/F\big)$ is well-defined since $\sigma(K^H) = K^H$. The map is also surjective since every K^H-automorphism can be extended to an K-automorphism by theorem 1.3.8 (since K/K^H is Galois and thus can be generated by the roots of a polynomial which splits over K).

Notice that the kernel of this map is all K-automorphisms which keep K^H constant, meaning the kernel is $\mathrm{Gal}\big(K/K^H\big) = H$. Thus by the first isomorphism theorem, $G/H \cong \mathrm{Gal}\big(K^H/F\big)$. Furthermore,

$$\begin{aligned}
(K^H)^{\mathrm{Gal}\left(K^H/F\right)} = \left\{\alpha \in E^H \;\middle|\; \forall \sigma \in G \colon \sigma\big|_{E_H}(\alpha) = \alpha\right\} &= \left\{\alpha \in E^H \;\middle|\; \forall \sigma \in G \colon \sigma(\alpha) = \alpha\right\} \\
&= E^G \cap E^H = F \cap E^H = F
\end{aligned}$$

So by theorem 2.1.12, K^H/F is Galois.

Conversely, let $L = K^H$ and suppose that L/F is Galois and let $L = F[\alpha_1, \ldots, \alpha_n]$. Let h_i be the minimal polynomial of α_i, then for all $\sigma \in G$, $\sigma(\alpha_i)$ is still a root of h_i. Since L/F is Galois and thus normal, this means that $\sigma(\alpha_i) \in L$ for all i and so $\sigma(L) = L$ for all $\sigma \in G$. By (2) this means that

$$\sigma H \sigma^{-1} = \sigma \,\mathrm{Gal}(K/L)\sigma^{-1} = \mathrm{Gal}(K/\sigma(L)) = \mathrm{Gal}(K/L) = H$$

so H is normal, as required. ■

2.2 Galois Closure and Compositum of Fields

Proposition 2.2.1

Every finite separable extension K/F is contained in some finite Galois extension.

Proof: suppose $K = F[\alpha_1, \dots, \alpha_n]$, and let h_i be the minimal polynomial of α_i. Since K/F is separable, h_i only has simple roots (roots of multiplicity 1) in K. Let $f(x) = \prod_i h_i(x)$ where repetitions are removed, so that $f(x)$ is still separable. Let E be f's splitting field, so it is the splitting field of a separable polynomial, so by theorem 2.1.12, E/F is Galois. ■

Proposition 2.2.2

Let $K/L/F$ be finite extensions such that K/F is Galois. Let $G = \mathrm{Gal}(K/F)$ and $H = \mathrm{Gal}(K/L)$. Define $N = \mathrm{core}_G(H) = \bigcap_{\sigma\in G} \sigma H \sigma^{-1}$. Then K^N/F is Galois, and moreso it is the smallest Galois extension in K/F that contains L.

Proof: we know that the core of a subgroup is normal, meaning $N \trianglelefteq G$ and so by corollary 2.1.16 E^N/F is Galois. Since $N \leq H$, $E^N \supseteq E^H = M$ by the fundamental theorem. Furthermore, if $M = K^{N_0} \supseteq L$ such that M/F is Galois, then by corollary 2.1.16 again, N_0 is normal in G. And by the correspondence, $N_0 \leq H$. So N_0 is a normal subgroup of G contained in H, but N is the core which is the largest such normal group, so $N_0 \leq N$. And so $K^N \subseteq E^{N_0} = M$. So K^N is minimal. ■

Definition 2.2.3

Given finite extensions $K/L/F$ such that K/F is Galois, and for every $L \subseteq M \subset K$, M/F is not Galois, then K is called the **Galois closure** of L/F.

Proposition 2.2.4

The Galois closure of a separable extension L/F is unique up to isomorphism.

Proof: suppose $L = F[\alpha_1, \dots, \alpha_n]$ and let h_i be the minimal polynomial of α_i which is separable. Then define $f = \prod_i h_i$ without repetitions, and this is still separable. We claim that E^N (where N is defined in the above proposition) is the splitting field of f. Since E^N/F is Galois, f splits into distinct linear factors over E^N. Let K be the splitting field of f, so $K \subseteq E^N$ and since K is the splitting field of a separable polynomial, K/F is Galois. But E^N is minimal so $E^N \subseteq K$, meaning $E^N = K$. ■

Proposition 2.2.5

Let K/F be separable, then there exist only finitely many intermediate fields.

Proof: let E be the Galois closure of K/F. Then E/F is Galois and thus has finitely many intermediate fields, and therefore so does K/F (every intermediate field of K/F is an intermediate field of E/F). ■

Theorem 2.2.6 (Steinitz's Theorem)

Every finite dimension separable field extension K/F is generated by a single element.

Proof: we assume for the sake of this proof that the fields are infinite, and we induct on the number of generators of K. It is sufficient to prove this for the case of two generators, $K = F[x, y]$, as we can then go from $F[x_1, \dots, x_n] = F[x_1, \dots, x_{n-2}][x_{n-1}, x_n]$ to $F[x_1, \dots, x_{n-1}]$ and continue inductively.

Let us focus on elements of the form $x + \alpha y$ for $\alpha \in F$. And so we have infinitely many intermediate fields $F[x + \alpha y]$ (counting repetitions). By the above proposition, there are finitely many intermediate fields of K/F, and so there must be $\alpha \neq \beta \in F$ such that $L = F[x + \alpha y] = F[x + \beta y]$. But then

$$(x + \alpha y) - (x + \beta y) = (\alpha - \beta)y \in L \implies y \in L$$

and similarly we can show that $x \in L$. Thus we have that $L = F[x, y] = K$, meaning we can generate K using a single element. ■

Definition 2.2.7

Suppose F, L are fields contained in some larger field K. The **compositum** of F and L is defined to be the smallest field containing both L and F. This can be shown to be

$$FL = \left\{ \sum_{i=1}^{n} \alpha_i \beta_i \;\middle|\; \alpha_i \in F, \beta_i \in L \right\}$$

the compositum is also denoted $F \vee L$.

Proposition 2.2.8

If K/F is Galois and L/F is a finite extension, then KL/F is also Galois, and

$$\mathrm{res}\colon \mathrm{Gal}(KL/L) \longrightarrow \mathrm{Gal}(K/K \cap L), \qquad \sigma \mapsto \sigma\big|_K$$

is a well-defined isomorphism.

Proof: since K/F is Galois, K is the splitting field of some separable polynomial $f \in F[x]$. This means that KL is the splitting field of $f \in L[x]$ since it is the smallest field containing both L and the roots of f, which is by definition the splitting field of f over L. Since f is separable, this means KL/L is Galois.

Now, res is well-defined since if $\sigma \in \mathrm{Gal}(KL/L)$ then σ permutes the roots of f, which generates K, and so $\sigma(K) = K$. And since it also fixes L, we must have that it fixes $K \cap L$. So $\sigma\big|_K$ is a $K \cap L$-automorphism. res is clearly a homomorphism.

Now we prove that res is injective: if $\sigma\big|_K = 1$, then σ is the identity on K and L (since it is a L-automorphism), so it is the identity on KL. Thus the kernel of res is trivial, meaning it is injective.

Finally, we prove that res is surjective. If $\alpha \in K^{\mathrm{Im}\,\mathrm{res}}$ then $\sigma(\alpha) = \alpha$ for every $\sigma \in \mathrm{Gal}(KL/L)$, then since $KL^{\mathrm{Gal}(KL/L)} = L$, we have that $\alpha \in L$. So $\alpha \in K \cap L$, meaning $K^{\mathrm{Im}\,\mathrm{res}} \subseteq K \cap L$. Conversely, $\mathrm{Im}\,\mathrm{res} \subseteq \mathrm{Gal}(K/K \cap L)$ so $K^{\mathrm{Im}\,\mathrm{res}} \subseteq K \cap L$. Thus we have the equality, $K \cap L = K^{\mathrm{Im}\,\mathrm{res}}$. But then by taking $\mathrm{Gal}(K/\bullet)$, we have that $\mathrm{Gal}(K/K \cap L) = \mathrm{Im}\,\mathrm{res}$ as required. ■

Notice then that we get, by the Galois correspondence,

$$[K : F] = [K : K \cap L][K \cap L : F], \qquad [KL : F] = [KL : L][L : F] = [K : K \cap L][L : F]$$

So $[K : K \cap L] = \frac{[K:F]}{[K \cap L:F]}$ and thus

$$[KL : F] = \frac{[K : F][L : F]}{[K : K \cap L]}$$

when K/F is Galois and L/F is finite.