Question: Given an isomorphism of fields, and u (resp. v) in some extension of K (resp. L), when can we extend to an isomorphism $K(u) \to L(v)$? In particular with $u \to v$.

Theorem: Let $K \simeq L$ as fields, and $K(u), L(v)$ be some extensions of K and L. TFAE:

(a) There exists an extension of ϕ to $\phi: K(u) \to L(v)$ with $\phi(u) = v$.

(b) Either

(i) u is transcendental over K and v is transcendental over L.

(ii) u is algebraic over K with minimal polynomial $f(x) \in K[x]$ and v is algebraic over L with minimal polynomial $(\phi f)(x)$, where

$$\phi(a_0 + \cdots + a_n x^n) = \phi(a_0) + \cdots + \phi(a_n) x^n$$

Sketch of Proof:

(a) $\Rightarrow$ (b) If ϕ extends to an isomorphism $\phi: K(u) \to L(v)$ and to an isomorphism $\phi: K(u) \to L(v)$

- If u and v are both transcendental, then $K(u) \simeq K(x) \simeq L(x) \simeq L(v)$.
- If u is algebraic, i.e. $f(u) = 0$, then if we have an extension $\phi: K(u) \to L(v)$, then

$0 = \phi(0) = \phi(f(u)) = (\phi f)(\phi(u)) = (\phi f)(u)$, so one algebraic and one transcendental implies no extension.

Suppose u is algebraic over K and v is algebraic over L and there is an extension $\phi: K(u) \to L(v)$ we get $f(u) = 0$ if and only if $(\phi f)(v) = 0$, so if $f(x)$ is the minimal polynomial of u, the minimal polynomial of v must be ϕf.

(b)(i) $\Rightarrow$ (a) If u is algebraic with min. polynomial f and v is algebraic with polynomial ϕf, then

$$K(u) \simeq K[x]/\langle f(x)\rangle \simeq L[x]/\langle(\phi f)(x)\rangle \simeq L(v)$$

extends $\phi: K(u) \to L(v)$.

Example: If u and v have the same minimal polynomial in $K[x]$, there is an isomorphism $\phi: K(u) \to K(v)$ with $\phi(u) = v$ and $\phi|_K = id$.

Take $\phi: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ to be an automorphism which satisfies $\phi(\sqrt{2}) = -\sqrt{2}$. Also, there exists $\phi: \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ automorphism, which satisfies $\phi(\sqrt{2}) = -\sqrt{2}$, $\phi(\sqrt{3}) = -\sqrt{3}$

Theorem: If K is a field and $f(x) \in K[x]$ of degree at least one, then there exists a simple extension $F = K(u)$ s.t.

(i) $f(u) = 0$

(ii) $[K(u) : K] \leq n$

(iii) If $f(x)$ is irreducible, then $[K(u) : K] = n$ and $K(u)$ is unique up to isomorphism.

Proof: Let $g(x)$ be an irreducible factor of $f(x)$ of degree $d \geq 1$, and $F = K[x]/\langle g(x)\rangle$. Then F is a field and (identifying $a \in K$ with $a + \langle g(x)\rangle \in F$) an extension of K. This contains a root $u = a + \langle g(x)\rangle$ of g, which is also a root of f. Also $F = K(u)$. and $[F : K] = d \leq n$.

If $f(x)$ was irreducible, $g = cf$ for some $c \in K^*$ then $[F : K] = n$.

Theorem: If $[F : K] < \infty$, then F is algebraic, and finitely generated over K.

Proof: If $[F : K] = n \in \mathbb{N}$, we have a K-basis $u_1, \ldots, u_n \in F$ and $F = \langle \{u_1, \ldots, u_n\} \rangle \subset K(u_1, \ldots, u_n) \subset F$. Therefore, $F = K(u_1, \ldots, u_n)$. If $\alpha \in F$, $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent over K, so

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0 \quad \text{for some } a_i \in K \text{ not all } 0.$$

Theorem: If $F = K(X)$ with $X \subset F$ and each $\alpha \in X$ algebraic over K, then F is algebraic over K. If X is finite, then X is finite over K.

Proof: If X is finite, say $X = \{u_1, \dots, u_n\}$, then u_1 is algebraic over K implies $[K(u_1) : K] < \infty$. Also, if u_2 is algebraic over K, u_2 is algebraic over $K(u_1)$, so $[K(u_1, u_2) : K(u_1)] < \infty$.

$$[K(u_1, u_2) : K] = [K(u_1, u_2) : K(u_1)][K(u_1) : K]$$

Proceed inductively.

If X is arbitrary, let $\alpha \in F = K(X)$. Then α is a rational function in some $u_1, \dots, u_n \in X$ with coefficients in K. Thus, $\alpha \in K(u_1, \dots, u_n)$ which is a finite extension of K, so α is algebraic over K

Example: $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)$ is an infinite algebraic extension of $\mathbb{Q}$.

Theorem: An algebraic extension of an algebraic extension is algebraic extension. That is, if $K \subset E \subset F$ E/K algebraic and F/E algebraic, then F/K is algebraic

Proof: Let $K \subset E \subset F$, let $\alpha \in F$. We want to show that α is algebraic over K. Because α is algebraic over E, there exists a nonzero polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

with $f(\alpha) = 0$, $a_i \in E$. Then $K(a_0, \dots, a_n) \subset E$ is a finite extension of K, as the a_i are algebraic over K.

So since α is algebraic over $K(a_0, \dots, a_n)$, so $K(a_0, \dots \alpha)$ is a finite extension of K, therefore, α is algebraic over F/K.

Theorem: If F/K is any extension, then

$$\mathbb{A} = \{ \alpha \in F : \alpha \text{ is algebraic over } K \}$$

is a subfield and $K \subset \mathbb{A} \subset F$. $\mathbb{A}$ is called the **relative algebraic closure**.

Proof: $K \subset \mathbb{A} \subset F$ is easy to note. If $\alpha, \beta \in \mathbb{A}$, then $[K(\alpha) : K] < \infty$ and $[K(\alpha, \beta) : K(\alpha)] < \infty$, so $[K(\alpha, \beta) : K] < \infty$, so $\alpha + \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$, $\beta \neq 0 \in K(\alpha, \beta)$ are all algebraic, so $\mathbb{A}$ is a subfield of F.

Example: $\overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q} \}$.

Galois Theory

Let F/K be an extension of fields. Consider

$$\text{Gal}(F/K) = \text{Aut}_K(F) = \{ \sigma : F \to F \text{ isomorphism such that } \sigma(a) = a \text{ for all } a \in K \}.$$

Example: $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{ \text{id}, \bar{z} \}$.

$$\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i)$$

$$i^2 = -1 \Rightarrow \sigma(i)^2 = -1 \Rightarrow \sigma(i) = \pm 1$$

$\text{Gal}(F/K)$ is always a group under composition.