and since $[E : E^{\langle \tau \rangle}] = 3$ this

implies $E^{\langle \tau \rangle} = \mathbb{Q}(w)$.

Now we'll examine a certain number of consequences of the Galois correspondence. The most straightforward is:

Corollary IV.18. A (finite) Galois extension has only finitely many intermediate subfields.

Proof: $G = Gal(E/k)$ is finite and has therefore only finitely many subfields. ∎

Def. IV.19: An extension E/k is simple if there is $u \in E$ with $E = k(u)$.

The following will immediately imply that Galois extensions are simple:

Prop. IV. 20. *A finite extension E/k is simple iff it has finitely many intermediate fields.*

Proof:

($\Rightarrow$) Assume $E = k(x)$. Let $E \supset F \supset k$ be an intermediate field and consider

$$f_F(T) = \operatorname{irr}(x, F)(T) \in F[T]$$
$$= T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

the minimal polynomial of x over F.

Clearly $F_0 := k(a_{n-1}, \ldots, a_0) \subset F$.

Now f_F is irreducible over F hence over F_0

thus $[E : F] = [F(x) : F] = n$

$$[E : F_0] = [F_0(x) : F_0] = n$$

which implies $F_0 = F$.

Next observe that $\mathrm{irr}(\alpha, F)$ divides $\mathrm{irr}(\alpha, k)$ and hence there are at most as many intermediate fields as there are factors of $\mathrm{irr}(\alpha, k) \in E[T]$.

($\Leftarrow\!=$) If k is a finite field then $k = \mathbb{F}_q$, $E = \mathbb{F}_{q^n}$ and $E = k(w)$ where w is a generator of $\mathbb{F}_{q^n}^{\times}$.

Thus we may assume k infinite.

Claim: Let V be a finite dimensional k-vector space with $\dim V \geq 1$.

Then V is not the finite union of proper vector subspaces.

Indeed: assume $\dim V \geq 1$ is minimal such that $V = \bigcup_{i=1}^{m} V_i$, $\dim V_i < \dim V$.

Let $W \subset V$ be any subspace of codimension 1

Then $W = \bigcup_{i=1}^{m} (V_i \cap W)$ and since

$\dim W < \dim V$, we have $V_i \supset W$ for

some $1 \leq i \leq m$. Hence: any codimension

1 subspace is among the $V_1, \ldots, V_m$.

Let $\lambda \in V^* \setminus (0)$; then $\ker \lambda = V_i$

and hence choosing $\lambda_1, \ldots, \lambda_m$ with

$\ker \lambda_i = V_i$ we have $V^* = \bigcup_{i=1}^{m} k\lambda_i$

which since $\dim V = \dim V^*$ implies

$\dim V = \dim V^* = 2$. But take now

$\ell \subset V^*$ an affine line <u>not</u> through 0^*.

Then $|\ell \cap k\lambda| \leq 1 \quad \forall \lambda \in V^*$, hence

$|\ell| \leq m$ which implies $|k| \leq m$, a contradiction.

Apply this to E seen as f.d. k-vector space. If $F_1, \ldots, F_m$ are the (proper) intermediate fields, then since k is infinite there is $x \in E \setminus (\bigcup_{i=1}^{m} F_i)$ which implies $k(x) = E$. ∎.

In fact using lemma III.6 we deduce:

Corollary IV.21: If B/k is a finite separable extension then $\exists\, x \in B$ with $B = k(x)$.

Proof: In fact lemma III.6 shows that there is a normal separable extension $B \subset E$ with $k \subset B \subset E$. Then E/k is Galois and hence there are in particular only

finitely many intermediate fields between K and B, which implies B is simple. ∎

The next application of the Galois correspondence is to the converse, in char = 0, of Galois' theorem concerning the Galois group of a polynomial solvable by radicals. Namely, in char = 0, if Gal(E/k) is solvable then E is contained in a radical extension of k.

The first step involves the study of the norm map. Namely let E/k be Galois.

Def. IV.22 : the norm $N(x)$ of an element $x \in E$ is: $N(x) = \prod_{\sigma \in G} \sigma(x)$,

where $G = \mathrm{Gal}(E/k)$.

The first observation is that $\forall \tau \in G$:

$$\tau(N(x)) = \tau\left(\prod_\sigma \sigma(x)\right) = \prod_\sigma \sigma(x) = N(x)$$

and hence $N(x) \in E^G = k$.

In addition

(1) $N(xy) = N(x)N(y)$, in particular

$N: E^\times \to k^\times$ is a group homomorphism.

(2) $N(\sigma(x)) = N(x) \quad \forall x, \forall \sigma$

(3) $N(\beta) = \beta^n \quad \beta \in k, \ n = [E:k]$.

Examples

(1) $E = \mathbb{Q}(i)$, $N(x+iy) = (x+iy)(x-iy)$

$= x^2 + y^2$

(2) $E = \mathbb{Q}(\sqrt{2})$: $N(x+\sqrt{2}y) = x^2 - 2y^2$.

Thm IV.23 (Hilbert 90): Assume E/k is a (finite) Galois extension with $G = Gal(E/k)$ cyclic. Then

$$N(u) = 1 \iff \text{there is } v \in E^\times \text{ with } u\,\sigma(v)^{-1} = v.$$

Proof:

($\Leftarrow$) Follows from $N(u) = N(v)\,N(\sigma(v))^{-1}$
$= N(v)\,N(v)^{-1} = 1.$

($\Rightarrow$) Let $G = \{id, \sigma, \ldots, \sigma^{n-1}\}$ and let $u \in E^\times$ with $u\,\sigma(u)\cdots\sigma^{n-1}(u) = 1$.

Define $\delta_i :=$ ($i+1$)'th partial product, that is:

$$\delta_0 = u$$
$$\delta_1 = u\,\sigma(u)$$
$$\vdots$$
$$\delta_i = u\cdots\sigma^i(u) \qquad 0 \le i \le n-1$$

so that $\delta_{n-1} = 1$.

Now given $y \in E$, consider

$$\zeta := \delta_0 y + \delta_1 \sigma(y) + \cdots + \delta_{n-2} \sigma^{n-2}(y) + \delta_{n-1} \sigma^{n-1}(y)$$

and let's compute $\sigma(\zeta)$:

$$\sigma(\zeta) = \sigma(\delta_0)\sigma(y) + \sigma(\delta_1)\sigma^2(y) + \cdots + \sigma(\delta_{n-2})\sigma^{n-1}(y)$$

$$+ \sigma(\delta_{n-1})\sigma^n(y)$$

First $\sigma(\delta_i) = \sigma(u) \cdots \sigma^{1+i}(u)$

$$= u^{-1}\delta_{i+1} \qquad 0 \le i \le n-2$$

While $\sigma(\delta_{n-1}) = 1$, $\sigma^n(y) = y$.

All in all we get

$$\sigma(\zeta) = u^{-1}\delta_1\sigma(y) + u^{-1}\delta_2\sigma^2(y) + \cdots + u^{-1}\delta_{n-1}\sigma^{n-1}(y)$$

$$+ u^{-1}\delta_0 y$$

$$= u^{-1}\zeta.$$

Now observe that by independence of characters, there always exists $y \in E^\times$ with $z \neq u$ which implies $u = z\sigma(z)^{-1}$. ∎

The following Corollary is then an important step towards our goal:

Corollary IV.24 Let E/k be a Galois extension of prime degree p. If k contains a p'th primitive root of 1, then there is $z \in E$ with $E = k(z)$ and $z^p \in k$.

Proof: Since $\mathrm{Gal}(E/k) \cong \mathbb{Z}/p\mathbb{Z}$ there are (by Galois corr.) no intermediary fields other than k and E; hence $E = k(y)$

$\forall y \notin k$.

Let now $\omega \in k$ be a primitive p'th root of 1:

$$N(\omega) = \omega^p = 1 .$$

Hence by Hilbert 90 there is $z \in E^*$,

$$z\sigma(z)^{-1} = \omega .$$

Thus $$z^p \sigma(z)^{-p} = \omega^p = 1$$

that is $z^p = \sigma(z^p)$ and since σ generates G we have $z^p \in k$. Now observe that since $\omega \neq 1$, we must have $\sigma(z) \neq z$ hence $z \notin k$ which implies $E = k(z)$. ∎

Now we are ready to prove:

Thm IV.25 Assume $\mathrm{char}\, k = 0$. Let E/k be a Galois extension and assume that $G = \mathrm{Gal}(E/k)$ is solvable. Then E is contained in a radical extension of k.

Proof: We proceed by induction on $[E:k]$, the case $[E:k] = 1$ being clear. Thus assume $[E:k] > 1$; since $|G| > 1$ and G is solvable, there is a normal subgroup $N \lhd G$ of prime index p. Let k^* be a splitting field of $X^p - 1$ over k and $w \in k^*$ a non-trivial root.

We distinguish two cases:

Case 1: $\omega \in k$. Then $E^H : k$ is a pure extension of type p; E/E^H is a Galois extension with solvable Galois group ($Gal(E|E^H) \subset Gal(E|k)$) and $[E:E^H] < [E:k]$; by recurrence there is a tower

$$K_1 = E^H \subset K_2 \subset \cdots \subset K_t$$

of pure extensions with $K_t \supset E$.

Now complete the tower by adding

$$k \subset K_1 = E^H$$

to it.

Case 2: Let $E^* = E(\omega)$; then since $E|k$ is the splitting field of some (separable) $f \in k[x]$, E^* is the splitting field of $f(x)(x^p - 1)$, hence E^*/k is Galois.

Therefore E^*/k^* is Galois as well and we have an injection:

$$Gal(E^*/k^*) \longrightarrow Gal(E/k)$$

which implies $Gal(E^*/k^*)$ solvable.

If $E^* = k^*$, then $E \subset k^*$ and is hence a pure extension of k; thus we may assume $[E^* : k^*] > 1$ and by the same argument as above construct an intermediary $k^* \subset F^{*H} \subset E^*$ that is a pure extension of k^* of prime type. By recurrence there is a tower

$$K_1 = F^{*H} \subset \cdots \subset K_t$$

of pure extensions with $E^* \subset K_t$.

Now complete it to a tower:

$$k \subset k^* = k(w) \subset E^* = K_1 \subset \cdots \subset K_t$$
$$\cup$$
$$E$$

∎