A note in inverse Galois theory

Orges Leka, firstname.lastname@gmail.com

November 24, 2023

Abstract

The note explores connections between inverse Galois theory and Hilbert irreducibility, presenting results in the form of theorems and lemmas. The main focus is on establishing conditions under which a finite group can be realized as a Galois group over the rational numbers. The note introduces a corresponding polynomial associated with a finite group and explores its irreducibility over specific varieties. The main results include Theorem 1, which establishes conditions for a group to be a Galois group, and Theorem 2, which demonstrates the equivalence between the applicability of Hilbert irreducibility to the corresponding polynomial and the realizability of every finite group as a Galois group over the rational numbers. The note concludes with corollaries and lemmas supporting the main theorems.

Theorem 1

Let $\mathbb{G} = \{\sigma_1, \cdots, \sigma_n\}$ be a finite group, $x_1, \cdots, x_n$ be indeterminates and let ρ be the regular representation of $\mathbb{G}$. Let $x = (x_1, \cdots, x_n)^T$ and $G = (\rho(\sigma_1)x, \cdots, \rho(\sigma_n)x)$, $A' = \text{diag}(x_1, \cdots, x_n)$. Set $A = GA'G^{-1}$. Suppose there exists $\alpha := (\alpha_1, \cdots, \alpha_n) \in \mathbb{C}^n$ such that:

1. $\det(G(\alpha)) \neq 0$
2. $A = A(\alpha)$ has rational coefficients
3. the characteristic polynomial $\chi_A(t)$ is irreducible over $\mathbb{Q}$.

Then $\text{Gal}(\chi_A(t)/\mathbb{Q}) = \mathbb{G}$.

Proof:

On the one hand we have

$$GA' = AG = GA' = (x_1\rho(\sigma_1)x, \cdots, x_n\rho(\sigma_n)x)$$

On the other hand we have

$$GA' = AG = A(\rho(\sigma_1)x, \cdots, \rho(\sigma_n)x) = (A\rho(\sigma_1)x, \cdots, A\rho(\sigma_n)x)$$

and it follows that

$$(A\rho(\sigma_1)x, \cdots, A\rho(\sigma_n)x) = GA' = (x_1\rho(\sigma_1)x, \cdots, x_n\rho(\sigma_n)x)$$

and so we get

$$A\rho(\sigma_i)x = x_i\rho(\sigma_i)x \text{ for } i = 1, \cdots, n \tag{1}$$

Let $K := \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$. From $A\rho(\sigma_i)\alpha = \alpha_i\rho(\sigma_i)\alpha$ follows for $i = 1$, $\rho(\sigma_1) = 1$ that $A\alpha = \alpha_1\alpha$. Application of $\tau \in Gal(K/\mathbb{Q})$ at the coefficients of the last equation gives us with $\tau(A) = A$ (since A has rational coefficients) that

$$A\tau(\alpha) = \tau(\alpha_1)\tau(\alpha) = \alpha_\tau\tau(\alpha) \tag{2}$$

where we have set $\alpha_\tau = \tau(\alpha_1)$. This means that $\tau(\alpha)$ is an eigenvector of A to the eigenvalue α_τ. But because of equation (1) we have:

$$A\rho(\sigma_\tau)\alpha = \alpha_\tau\rho(\sigma_\tau)\alpha \tag{3}$$

Since the eigenvectors $\rho(\sigma_1)\alpha, \cdots, \rho(\sigma_n)\alpha$ of A build a basis of K^n, it means that every eigenspace has dimension 1. Especially there exists $a_\tau \in K$ such that

$$\tau(\alpha) = a_\tau\rho(\sigma_\tau)\alpha \tag{4}$$

If we build the polynomials with roots from the coefficients of the left and right side of (4), then they must be because of (4) be equal:

$$\chi_A(t) = \prod_{i=1}^{n}(t - \alpha_i) =^{(4)} \prod_{j=1}^{n}(t - a_\tau\alpha_j) \tag{5}$$

This means that the coefficients of both polynomials must be equal, especially we get

$$\sum_{i=1}^{n}\alpha_i = a_\tau\sum_{i=1}^{n}\alpha_i \tag{6}$$

By a theorem of Frobenius concerning the factorization of the group determinant, we have

$$\det(G(x_1, \cdots, x_n)) = (x_1 + \cdots + x_n)p(x_1, \cdots, x_n) \tag{7}$$

for some polynomial p. From (7) follows by assumption

$$0 \neq \det(G(\alpha_1, \cdots, \alpha_n)) = (\alpha_1 + \cdots + \alpha_n)p(\alpha_1, \cdots, \alpha_n)$$

which means that $0 \neq \alpha_1 + \cdots + \alpha_n$ and because of (6) we get

$$a_\tau = 1 \tag{8}$$

From (4) and (8) it follows that

$$P_\tau\alpha = \tau(\alpha) = \rho(\sigma_\tau)\alpha \tag{9}$$

where P_τ is the permutation matrix which corresponds to τ. Since

$$\chi_A(t) = \prod_{i=1}^{n} t - \alpha_i$$

is separable, it follows that $\alpha_k \neq \alpha_l$ for $k \neq l$. This means that the two permutation matrices P_τ and $\rho(\sigma_\tau)$ from (9) must be equal, that is

$$P_\tau = \rho(\sigma_\tau) \tag{10}$$

From this we get a mapping:

$$\phi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{G}, \tau \mapsto \sigma_\tau$$

ϕ is injective: Let $\sigma_\tau = \phi(\tau) = \phi(\tau') = \sigma_{\tau'}$. Then we get

$$P_\tau =^{(10)} \rho(\sigma_\tau) = \rho(\sigma_{\tau'}) =^{(10)} P_{\tau'}$$

and since the regular representation P is faithful, it follows that $\tau = \tau'$.

ϕ is surjective: Let $m = |\mathrm{Gal}(K/\mathbb{Q})|$, $n = |\mathbb{G}| = deg(\chi_A(t))$. Since $\chi_A(t)$ is irreducible, $deg(\chi_A(t)) = n$ is a divisor of $m = |\mathrm{Gal}(K/\mathbb{Q})|$ and it follows that $n \leq m$. Since ϕ is injective it follows that $m \leq n$, which means that $m = n$. Since the mapping ϕ is injective on two finite sets of equal size, this means that ϕ must also be surjective.

ϕ is an antihomomorphism of groups:

$$\tau(\alpha) = \rho(\sigma_m)\alpha \to \phi(\tau) = \sigma_m$$

$$\tau'(\alpha) = \rho(\sigma_k)\alpha \to \phi(\tau') = \sigma_k$$

$$(\tau\tau')(\alpha) = \rho(\sigma_l)\alpha \to \phi(\tau\tau') = \sigma_l$$

From this it follows that:

$$\rho(\sigma_l)\alpha = (\tau\tau')(\alpha) = \tau(\tau'(\alpha)) = \tau(\rho(\sigma_k)\alpha) = \rho(\sigma_k)\tau(\alpha) = \rho(\sigma_k)\rho(\sigma_m)\alpha$$

Since α_i are separable, it follows that the permutation matrices $\rho(\sigma_l)$ and $\rho(\sigma_k\sigma_m)$ must be equal:

$$\rho(\sigma_l) = \rho(\sigma_k\sigma_m)$$

and from this, since the regular representation is faithful, it follows that $\sigma_l = \sigma_k\sigma_m$. From this we get:

$$\phi(\tau\tau') = \sigma_l = \sigma_k\sigma_m = \phi(\tau')\phi(\tau)$$

Since for two finite groups which are antiisomorph it follows that they are isomorph (if $\phi(xy) = \phi(y)\phi(x)$ is an antihomomorphism, then $\Phi(x) := \phi(x)^{-1}$ is a homomorphism), we conclude that

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{G}$$

Definition:

Let $\mathbb{G}$ be a finite group with n elements. Let $\mathbb{Q}[x_1, \cdots, x_n]^{\mathbb{G}} = \mathbb{Q}[g_1, \cdots, g_m]$. Then there exist polynomials $s_j \in \mathbb{Q}[y_1, \cdots, y_m]$ for $j = 1, \cdots, n$ such that $e_j(x_1, \cdots, x_n) = s_j(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$ for $j = 1, \cdots, n$ where e_j is the j-elementary symmetric polynomial in x_k. Consider the polynomial $p(t, y_1, \cdots, y_m) = t^n - s_1(y_1, \cdots, y_m)t^{n-1} + \cdots + (-1)^n s_n(y_1, \cdots, y_m)$ which is a polynomial in $\mathbb{Q}[t, y_1, \cdots, y_m]$. We call p the corresponding polynomial of the group $\mathbb{G}$ to the invariants $g_1, \cdots, g_m$. Let $I = \{h \in \mathbb{Q}[y_1, \cdots, y_m] | h(g_1, \cdots, g_m) = 0\}$. Define the variety $V_{\mathbb{G}} = \{a \in \mathbb{Q}^m | h(a) = 0 \forall h \in I\}$. We say that a polynomial is Hilbert irreducible over some variety, if it is irreducible and there exists a point in the variety such that the polynomial remains irreducible after specializing to the point of the variety and that other polynomials are not zero on this point.

Lemma 1:

The corresponding polynomial is irreducible in $\mathbb{Q}[t, y_1, \cdots, y_m]$.

1 Proof:

If the polynomial factored in a non-trivial way, then because of the t^n term the factors must have degree less than n in t (consider the factorization in $R = \mathbb{Q}(y_1, y_2, \ldots, y_n)[t]$; note also that we can assume that the factors over R are monic polynomials in t). Now specialise via $y_i \mapsto g_i$ and we get a non-trivial factorization of the specialised polynomial in $\mathbb{Q}[g_1, \ldots, g_m][t]$ and hence in $\mathbb{Q}[x_1, \ldots, x_n][t]$ and so in $\mathbb{Q}(x_1, \ldots, x_n)[t]$. But we know the complete factorization in this ring, it's just $\prod(t - x_i)$, so our given factorization must specialise into factors of the form $\prod_{i \in I}(t - x_i)$ for some subsets I of $\{1, 2, \ldots, n\}$ (with each I not empty or the whole thing), and the constant term of each factor must be in $\mathbb{Q}[g_1, \ldots, g_m]$ and hence G-invariant. This is a contradiction.

2 Lemma 2:

Let $f_1, \cdots, f_r \in \mathbb{Q}(x_1, \cdots, x_n)^{\mathbb{G}}$ and suppose that the corresponding polynomial of $\mathbb{G}$ is Hilbert irreducible over the variety V_G. Then there exists $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{C}^n$ such that:

1. $f_1(\alpha), \cdots, f_r(\alpha)$ are rational numbers.
2. $\prod_{i=1}^n t - \alpha_i$ is irreducible in $\mathbb{Q}[t]$.

3 Proof:

We can write

$$f_i = \frac{P_i(g_1, \cdots, g_m)}{Q_i(g_1, \cdots, g_m)} \text{ for } P_i, Q_i \in \mathbb{Q}[y_1, \cdots, y_m]$$

The corresponding polynomial $p(t, y_1, \cdots, y_m)$ is irreducible in $\mathbb{Q}[t, y_1, \cdots, y_m]$ by Lemma 1. By assumption, we can find $(a_1, \cdots, a_m)$ in $V_{\mathbb{G}}$ such that:

1. $p(t, a_1, \cdots, a_m)$ is irreducible in $\mathbb{Q}[t]$.
2. $Q_i(a_1, \cdots, a_m) \neq 0$ for $i = 1, \cdots, r$.

By application of the Hilbert Nullstellensatz we can find $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{C}^n$ such that $g_i(\alpha) = a_i$ for $i = 1, \cdots, m$. Then

$$e_j(\alpha) = s_j(g_1(\alpha), \cdots, g_m(\alpha)) = s_j(a_1, \cdots, a_m)$$

and the polynomial $p(t, a_1, \cdots, a_m)$ factors over $\mathbb{C}$ as
$p(t, a_1, \cdots, a_m) = \prod_{i=1}^{n} t - \alpha_i$. Then we get

$$f_i(\alpha) = \frac{P_i(g_1(\alpha), \cdots, g_m(\alpha))}{Q_i(g_1(\alpha), \cdots, g_m(\alpha))} = \frac{P_i(a_1, \cdots, a_m)}{Q_i(a_1, \cdots, a_m)}$$

is a rational number, which was to be shown.

4 Lemma 3:

Let the notation be as in Theorem 1. Then the entries a_{ij} of the matrix A are elements of $\mathbb{Q}(x_1, \cdots, x_n)^{\mathbb{G}}$.

5 Proof:

We have $A(x) = G(x)A'(x)G(x)^{-1}$ and want to show that $A(\rho(\sigma)x) = A(x)$ for all $\sigma \in \mathbb{G}$. For this, it is sufficient to show that

$$A'(\rho(\sigma)x) = \rho(\sigma)A'(x)\rho(\sigma)^{-1}$$

and

$$G(\rho(\sigma)x) = G(x)\rho(\sigma)^{-1}$$

as it follows that

$$\begin{aligned} A(\rho(\sigma)x) &= G(\rho(\sigma)x)A'(\rho(\sigma)x)G(\rho(\sigma)x)^{-1} \\ &= G(x)\rho(\sigma)^{-1}\rho(\sigma)A'(x)\rho(\sigma)^{-1}\rho(\sigma)G(x)^{-1} \\ &= G(x)A'(x)G(x)^{-1} = A(x) \end{aligned}$$

Corollary 1:

Let $\mathbb{G}$ be a finite group such that the correspoding polynomial is Hilbert irreducible over $V_{\mathbb{G}}$. Then $\mathbb{G}$ is realizable over $\mathbb{Q}$ as a Galois group.

Proof:

Consider the regular representation of $\mathbb{G}$ and let $A = (a_{ij})$ be defined as in Theorem 1. Then by Lemma 3 we have $a_{ij} \in \mathbb{Q}(x_1, \cdots, x_n)^{\mathbb{G}}$. Hence by Lemma 2 there exists $\alpha \in \mathbb{C}^n$ such that

1. $a_{ij}(\alpha)$ are rational numbers.
2. The characteristic polynomial $\chi_A(t) = \prod_{i=1}^{n} t - \alpha_i$ is irreducible in $\mathbb{Q}[t]$.

Since $a_{ij}(\alpha)$ are rational numbers, the matrix $A(\alpha) = G(\alpha)A'(\alpha)G(\alpha)^{-1}$ is defined for α, hence $\det(G(\alpha)) \neq 0$. By Theorem 1 therefore it follows that $\mathrm{Gal}(\chi_A(t)/\mathbb{Q}) = \mathbb{G}$.

Theorem 2:

The following are equivalent:

1. Hilbert Irreducibility can be applied to the corresponding polynomial $p(t, y_1, \cdots, y_m)$ over the variety $V_{\mathbb{G}}$
2. Every finite group $\mathbb{G}$ is Galois over $\mathbb{Q}$.

Proof:

1) $\rightarrow$ 2): Corollary 1.

2) $\rightarrow$ 1) Let $\mathbb{G} = Gal(K/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_n\}$ be a Galois group. By the normal basis theorem there exists a $\theta \in K$ such that $\sigma_1(\theta), \cdots, \sigma_n(\theta)$ build a basis of K over $\mathbb{Q}$. Let $\mathbb{Q}[x_1, \cdots, x_n]^{\mathbb{G}} = \mathbb{Q}[g_1, \cdots, g_m]$ where $\mathbb{G}$ acts through the regular representation. Let $I = \{h \in \mathbb{Q}[y_1, \cdots, y_m] | h(g_1, \cdots, g_m) = 0\}$ and $V_{\mathbb{G}} = \{a \in \mathbb{Q}^m | h(a) = 0 \forall h \in I\}$. Let now $Q_1, \cdots, Q_r \in \mathbb{Q}[y_1, \cdots, y_m]$ be given, such that $Q_i \notin I$ for $i = 1, \cdots, r$. Let $Q := Q_1 \cdots Q_r$. Since I is a prime ideal and $Q_i \notin I$, we must have $Q \notin I$, which means that there exists $b \in \mathbb{Q}^n$ such that

$$Q(g_1(b), \cdots, g_m(b)) \neq 0$$

that is $\hat{f}(x_1, \cdots, x_n) = Q(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$ is a reduced polynomial (since $\mathbb{Q}$ has infinite elements) (see Algebra, Lang, p. 177, p. 312). Since the σ_i by Artin (p. 311, Th. 12.2 Algebra, Lang) are algebraically independent and $\hat{f}$ is reduced, there exists $\alpha \in K$, such that

$$0 \neq Q(g_1(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)), \cdots, g_m(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)))$$

Let $\alpha = \sum_{i=1}^{n} \alpha_i \sigma_i(\theta)$ with $\alpha_i \in \mathbb{Q}$

Then we have for $i = 1, \cdots, m$ that $g_i(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)) = p_i(\alpha_1, \cdots, \alpha_n)$ is a rational number, where p_i is some polynomial in $\mathbb{Q}[x_1, \cdots, x_n]$. But then also

$$\begin{aligned} 0 \neq Q(g_1(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)), \cdots, g_m(\sigma_1(\alpha), \cdots, \sigma_n(\alpha))) \\ = Q(p_1(\alpha_1, \cdots, \alpha_n), \cdots, p_m(\alpha_1, \cdots, \alpha_n)) \\ = q(\alpha_1, \cdots, \alpha_n) \end{aligned}$$

for some polynomial $q \in \mathbb{Q}[x_1, \cdots, x_n]$. We can choose the α_i such that $\alpha_i \neq \alpha_j$ for $i \neq j$, otherwise replace $\hat{\alpha}_j = \alpha_i + u$ for some rational number $u \neq 0$ and we get the polynomial in u:

$$q(u) := q(\alpha_1, \cdots, \alpha_{j-1}, \alpha_i + u, \alpha_{j+1}, \cdots, \alpha_n)$$

Since $q(0) \neq 0$, q is not the zero polynomial in $\mathbb{Q}[u]$. By choosing $u \neq 0$ as a rational number to avoid the finitely many roots of q, we get $q(u) \neq 0$ and $\hat{\alpha}_j = \alpha_i + u \neq \alpha_i$. But then also $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$, since α has pairwise distinct coordinates $\alpha_k \neq \alpha_l$ to the given basis $\sigma_1(\theta), \cdots, \sigma_n(\theta)$. The rational and separable polynomial

$$\prod_{i=1}^{n} (x - \sigma_i(\alpha))$$

is irreducible in $\mathbb{Q}[x]$, since the Galois group operates transitively on the roots. Let $a_i := g_i(\sigma_1(\alpha), \cdots, \sigma_n(\alpha))$ for $i = 1, \cdots, m$. Then we have $a := (a_1, \cdots, a_m)$ is an element of $V_{\mathbb{G}}$ and also

$$p(t, a_1, \cdots, a_m) = \sum_{i=0}^{n} (-1)^i s_i(a_1, \cdots, a_m) t^{n-i}$$

$$= \sum_{i=0}^{n} (-1)^i s_i(g_1(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)), \cdots, g_m(\sigma_1(\alpha), \cdots, \sigma_n(\alpha))) t^{n-i}$$

$$= \sum_{i=0}^{n} (-1)^i e_i(\sigma_1(\alpha), \cdots, \sigma_n(\alpha)) t^{n-i}$$

$$= \prod_{i=1}^{n} (t - \sigma_i(\alpha))$$

is an irreducible polynomial in $\mathbb{Q}[t]$. Furthermore we have $Q(a_1, \cdots, a_m) \neq 0$, which means that $Q_j(a_1, \cdots, a_m) \neq 0$ for all $j = 1, \cdots, r$, which was to be shown.