SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Hilbert's Irreducibility Theorem and Applications to the Inverse Galois Problem

av

Victor Lisinski

2015 - No 12

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Hilbert's Irreducibility Theorem and Applications to the Inverse Galois Problem

Victor Lisinski

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Antoine Chambert-Loir och Rikard Bøgvad

2015

HILBERT'S IRREDUCIBILITY THEOREM AND APPLICATIONS TO THE INVERSE GALOIS PROBLEM

VICTOR LISINSKI

SUPERVISORS:

ANTOINE CHAMBERT-LOIR

RIKARD BØGVAD

Date: June 16, 2015.

Abstract. In this text we will explore a powerful and very useful result in Number Theory called Hillbert's Irreducibility Theorem. In its most basic form, this theorem states that for any irreducible polynomial $P(T, X)$ with coefficients in the field of rational functions over $\mathbb{Q}$, there is always an element $t \in \mathbb{Q}$ for which the polynomial $P(t, X)$ with coefficients in $\mathbb{Q}$ is irreducible (i.e. the polynomial obtained by evaluating the coefficients of P at t is still irreducible). We will apply this theorem to obtain some fundamental results regarding the still unsolved question if all finite groups appear as Galois groups of some Galois extension $K/\mathbb{Q}$. It turns out that Hilbert's Irreducibility Theorem can reduce this problem to the question whether or not every finite group is realizable as a Galois group of some Galois extension of $\mathbb{Q}(T_1, \ldots, T_n)$. Finally, we show that the alternating group has this property.

Contents

1. Introduction

In this text we will prove a powerful and very useful result in Number Theory called Hillbert's Irreducibility Theorem. In its most basic form, this theorem states that for any irreducible polynomial $P(T, X)$ with coefficients in the field of rational functions over $\mathbb{Q}$, there is always an element $t \in \mathbb{Q}$ for which the polynomial $P(t, X)$ with coefficients in $\mathbb{Q}$ is irreducible (i.e. the polynomial obtained by evaluating the coefficients of P at t is still irreducible). We will apply this theorem to obtain some fundamental results regarding the still unsolved question if all finite groups appear as Galois groups of some Galois extension $K/\mathbb{Q}$. The text assumes some basic knowledge in Galois theory, but the most important results regarding this are also included, though not proved. We will be working a lot with fields, and we will only consider fields with characteristic zero. For any field K, we will write $K[X]$ for the ring of polynomials in variable X with coefficients in K, and $K(T)$ for the field of rational functions in variable T over K.

An important result worth stating that any field K with characteristic zero is perfect, i.e. all irreducible polynomials in $K[X]$ are separable (have no repeated roots) [1, p. 57]. This result will be particularly important when we explore the Inverse Galois Problem. But first something (seemingly) completely different.

2. The Puiseux Theorem

To prove the irreducibility theorem, it turns out that we need a very fundamental result from Complex Analysis regarding a generalization of power series called Puiseux series.

Definition 2.1.
*A **Puiseux Series** in the variable z is a Laurent series on the form*

$$\sum_{i=k}^{\infty} a_i z^{i/n}$$

for some integer k and some positive integer n.

There is a theorem, the Newton-Puiseux Theorem, which states that the field of Puiseux series over an algebraically closed field of characteristic zero is algebraically closed.[1] We will look at a related result, called Puiseux's Theorem. This theorem will show that the roots of a polynomial whose coefficients are analytic functions in z can be regarded as analytic functions in $z^{1/n}$. To show this, we first need some properties for the set of analytic functions.

Proposition 2.2.
The following properties holds for $\mathscr{A}(r)$, the set of functions that are analytic on the open disc $D(0, r)$ and continuous on its closure $\bar{D}(0, r)$:

[1] If the reader is unfamiliar with the term *algebraically closed*, it is defined in part 5 of this text.

(1) $\mathscr{A}(r)$ *is an integral domain.*
(2) $\mathscr{A}(r)$ *is a Banach algebra, given the norm* $\|f\| = \sup_{|z|\leq r} |f(z)|$ *for* $f \in \mathscr{A}(r)$

Proof. Since addition and multiplication of functions preserve continuity, $\mathscr{A}(r)$ is a ring (additive inverses, identity and zero being trivial). We will show that it is also an integral domain. Let $f, g \in \mathscr{A}(r)$ and $f(z)g(z) = 0$ for all $|z| \leq r$. For any $z_0 \in D(0,r)$, we have that $fg(z_0) = 0$, so $f(z_0) = 0$ or $g(z_0) = 0$. Without loss of generality, we may assume that $f(z_0) = 0$. Consider $D(z_0, \delta)$ where δ is small enough so that $D(z_0, \delta) \subset D(0,r)$. From the principle of isolated zeros [4, p. 278], f has no roots except z_0 in $D(z_0, \delta)$ for a sufficiently small δ. But then, g must be constantly zero on $D(z_0, \delta)$ and so $g = 0$. Hence, $\mathscr{A}(r)$ is an integral domain.

If $f_1, f_2, f_3, \ldots$ is Cauchy sequence with the norm $\|f\| = \sup_{|z|\leq r} |f(z)|$ the limit of f_n in this sequence as $n \to \infty$ is a uniform limit, since the norm is independent of z. A uniform limit of analytic functions is analytic, and a uniform limit of continuous functions is continuous [1, p. 46], so the Cauchy sequence converges to an element in $\mathscr{A}(r)$ and so $\mathscr{A}(r)$ is a Banach space. To see that it is a Banach algebra, we simply note that

$$\sup_{|z|\leq r} |fg(z)| \leq \sup_{|z|\leq r} |f(z)| \sup_{|z|\leq r} |g(z)|,$$

since the z that yields the largest value of $|fg(z)|$ not necessarily gives us the highest possible value for of $|f(z)|$ and $|g(z)|$ separately. □

Proposition 2.3.
Let $P \in \mathscr{A}(r)[X]$ *be a monic polynomial with degree* n. *Let* $Q_0, R_0 \in \mathbb{C}[X]$ *be two monic polynomials with degree less than* n, *such that* $P(0,X) = Q_0(X)R_0(X)$. *Suppose* Q_0 *and* R_0 *are coprime. Then there exists* $\rho \in (0,r]$ *and two monic polynomials* $Q, R \in \mathscr{A}(\rho)[X]$ *such that* $Q(0,X) = Q_0$, $R(0,X) = R_0$ *and* $P = QR$.

Proof. Denote $P_0 = P(0,X)$ and let $P_1 \in \mathscr{A}(r)[X]$ be such that $P = P_0 + zP_1$. Since P is monic we have that $P(0,X)$ has degree n, and if we let $m = \deg(Q_0)$ and $p = \deg(R_0)$ we get $m + p = n$. By defining Q and R as polynomials such that $Q = Q_0 + zU$ and $R = R_0 + zV$, with $\deg(U) < m$ and $\deg(V) < p$ we reduce the problem of solving $P = QR$ to solving

$$P_1 = UR_0 + VQ_0 + zUV. \tag{1}$$

For any $a \in \mathbb{N}$, we can identify $\mathbb{C}^a$ with the set of polynomials in $\mathbb{C}[X]$ with degree less than a, by letting $\{1, X, \ldots, X^{a-1}\}$ represent the base vectors of $\mathbb{C}^a$. We let the map $\varphi : \mathbb{C}^m \times \mathbb{C}^p \to \mathbb{C}^{m+p}$ be defined by $\varphi(U,V) = UR_0 + VQ_0$. Since

$$\begin{aligned}\varphi((U_1,V_1) + (U_2,V_2)) &= \varphi(U_1 + U_2, V_1 + V_2) = \\ &= (U_1 + U_2)R_0 + (V_1 + V_2)Q_0 = \\ &= U_1R_0 + V_1Q_0 + U_2R_0 + V_2Q_0 = \\ &= \varphi(U_1,V_1) + \varphi(U_2,V_2)\end{aligned}$$

and

$$\begin{aligned}\varphi(\alpha(U,V)) &= \varphi(\alpha U, \alpha V) = \\ &= \alpha U R_0 + \alpha V Q_0 = \\ &= \alpha(U R_0 + V Q_0) = \\ &= \alpha \varphi(U,V),\end{aligned}$$

this is a linear map. Furthermore, if $\varphi(U,V) = 0$, then $UR_0 = -VQ_0$. So R_0 divides $-VQ_0$, but since it is coprime with Q_0 it must divide $-V$. Since $V \in \mathbb{C}^p$ we have that $\deg(-V) = \deg(V) < p = \deg(R_0)$ we have that $V = 0$. Similarly, Q_0 divides UR_0 which means that $U = 0$. In conclusion we have that $\ker(\varphi) = \{0\}$, and so φ is injective. An injective linear map between vector spaces of the same finite dimension is also a bijection, so we have in fact that φ is an isomorphism. The inverse of a linear map is also linear, so $\varphi^{-1} : \mathbb{C}^{m+p} \to \mathbb{C}^m \times \mathbb{C}^p$ is a linear bijection. If $U = u_0 + u_1 X + \cdots + u_{m-1}X$, $V = v_0 + v_1 X + \cdots + v_{p-1}X^{p-1}$ and $\varphi(U,V) = a_0 + a_1 X + \cdots + a_{m+p-1}X^{m+p-1}$ we can see that φ^{-1} is defined by

$$\begin{gathered}\varphi^{-1}(a_0 + a_1 X + ... + a_{m+p-1}X^{m+p-1}) = \\ = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{m+p-1} \hat{u}_{i,j}(a_j) X^i, \sum_{k=0}^{p-1} \sum_{\ell=0}^{m+p-1} \hat{v}_{k,\ell}(a_\ell) X^k \right)\end{gathered}$$

where the $\hat{u}_{i,j}, \hat{v}_{k,\ell}$ are some linear functions such that

$$\sum_{j=0}^{m+p-1} \hat{u}_{i,j}(a_j) = u_i \quad \text{and} \quad \sum_{\ell=0}^{m+p-1} \hat{v}_{k,\ell}(a_j) = v_k.$$

Now, we identify the set $\mathscr{A}(r)^a$ with the set of polynomials in $\mathscr{A}(r)[X]$ with degree less than a. Let the map $\Phi : \mathscr{A}(r)^m \times \mathscr{A}(r)^p \to \mathscr{A}(r)^{m+p}$ be defined by

$$\Phi(U,V) = UR_0 + VQ_0,$$

If U and V are polynomials with coefficients in $\mathscr{A}(r)$ with $\deg(U) < m$ and $\deg(V) < p$, we note that for any $z \in \bar{D}(0,r)$ we have

$$\begin{aligned}\Phi(U,V)(z) &= (UR_0 + VQ_0)(z) = \\ &= U(z)R_0 + V(z)Q_0 = \\ &= \varphi(U(z), V(z)).\end{aligned}$$

For $\tilde{a}_0, \ldots, \tilde{a}_{m+p-1} \in \mathscr{A}(r)$, let the mapping $\Psi : \mathscr{A}(r)^{m+p} \to \mathscr{A}(r)^m \times \mathscr{A}(r)^p$ be defined by

$$\begin{gathered}\Psi(\tilde{a}_0 + \tilde{a}_1 X + \cdots + \tilde{a}_{m+p-1}X^{m+p-1}) = \\ = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{m+p-1} \hat{u}_{i,j}(\tilde{a}_j) X^i, \sum_{k=0}^{p-1} \sum_{\ell=0}^{m+p-1} \hat{v}_{k,\ell}(\tilde{a}_\ell) X^k \right),\end{gathered}$$

where $\hat{u}_{i,j}, \hat{v}_{k,\ell}$ are the same as in the definition of φ^{-1}. Again, for any $z \in \bar{D}(0,r)$, let

$$\begin{aligned}U(z) &= \tilde{u}_0(z) + \tilde{u}_1(z)X + \cdots + \tilde{u}_{m-1}X^{m-1}, \\ V(z) &= \tilde{v}_0(z) + \tilde{v}_1(z)X + \cdots + \tilde{v}_{p-1}X^{-1} \quad \text{and} \\ \varphi(U(z), V(z)) &= \tilde{a}_0(z) + \tilde{a}_1(z)X + \cdots + \tilde{a}_{m+p-1}(z)X^{m+p-1},\end{aligned}$$

where $\tilde{u}_i, \tilde{v}_j, \tilde{a}_k \in \mathscr{A}(r)$. Then we get

$$\begin{aligned}\Psi(\Phi(U,V)(z)) &= \Psi(\varphi(U(z),V(z)) = \\ &= \Psi\left(\tilde{a}_0(z) + \tilde{a}_1(z)X + \cdots + \tilde{a}_{m+p-1}(z)X^{m+p-1}\right) = \\ &= \left(\sum_{i=0}^{m-1}\sum_{j=0}^{m+p-1} \hat{u}_{i,j}(\tilde{a}_j(z))X^i, \sum_{k=0}^{p-1}\sum_{\ell=0}^{m+p-1} \hat{v}_{k,\ell}(\tilde{a}_\ell(z))X^k\right).\end{aligned}$$

Since

$$\sum_{j=0}^{m+p-1} \hat{u}_{i,j}(\tilde{a}_j) = \tilde{u}_i(z) \quad \text{and} \quad \sum_{\ell=0}^{m+p-1} \hat{v}_{k,\ell}(\tilde{a}_j) = \tilde{v}_k(z)$$

this gives us that $\Psi(\Phi(U,V)(z)) = (U,V)(z)$ for all $z \in \bar{D}(0,r)$. This shows that Φ is a bijection and Ψ is its inverse. From (1) we now get that

$$\begin{aligned} & P_1 - zUV = UR_0 + VQ_0 \Leftrightarrow \\ \Leftrightarrow\ & P_1 - zUV = \Phi(U,V) \Leftrightarrow \\ \Leftrightarrow\ & \Psi(P_1 - zUV) = (U,V) \end{aligned} \tag{2}$$

In other words, the problem of solving $P = QR$ can be rewritten as (2). We will denote the left hand side of (2) by $T(U,V)$.

For any $a \in \mathbb{N}$ define a norm on $\mathscr{A}(r)^a$ in the following way

$$\|\boldsymbol{f}\| = \|(f_1, \ldots, f_a)\| = \|f_1\| + \cdots + \|f_a\|.$$

We say that $\boldsymbol{f}$ is continuous precisely if all $f_1, \ldots, f_a$ are continuous, and analytic if all$f_1, \ldots, f_a$ are analytic. A Cauchy sequence on $\mathscr{A}(r)^a$ with this norm is a sequence $\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3, \ldots$ such that for every real number $\epsilon > 0$, there is a positive integer N such that for all numbers $m, n > N$ we get

$$\|\boldsymbol{f}_m - \boldsymbol{f}_n\| < \epsilon.$$

Furthermore,

$$\|\boldsymbol{f}_m - \boldsymbol{f}_n\| = \|f_{m_1} - f_{n_1}\| + \cdots + \|f_{m_a} - f_{n_a}\|$$

so for every term in this expression and every $\epsilon > 0$ we have that $\|f_{m_k} - f_{n_k}\| < \epsilon$. This is a Cauchy sequence in $\mathscr{A}(r)$, and so it converges to an element in $\mathscr{A}(r)$. This is true for all terms in $\|\boldsymbol{f}_m - \boldsymbol{f}_n\|$, so the Cauchy sequence $\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3, \ldots$ converges to an element in $\mathscr{A}(r)^a$, and so $\mathscr{A}(r)^a$ is a Banach space. The linear maps Φ and Ψ are continuous and Lipschitz with this norm [1, p.48]. Let A be the Lipschitz constant of Ψ, i.e. $\|\Psi(P_1) - \Psi(P_2)\| \leq A\|P_1 - P_2\|$.

For any

$$U = f_0 + f_1X + \cdots + f_{m-1}X^{m-1} \in \mathscr{A}(r)^m$$

and

$$V = g_0 + g_1X + \cdots + g_{p-1}X^{p-1} \in \mathscr{A}(r)^p$$

we have by the triangle inequality that

$$\begin{aligned}\|UV\| &= \sum_{j=0}^{m+p-1} \left\| \sum_{k+\ell=j} f_k g_\ell \right\| \leq \\ &\leq \sum_{j=0}^{m+p-1} \sum_{k+\ell=j} \|f_k\| \|g_\ell\| \leq \\ &\leq \sum_{k=0}^{m-1} \|f_k\| \sum_{\ell=0}^{p-1} \|g_\ell\| \leq \|U\| \|V\|.\end{aligned}$$

From this we can conclude that

$$\begin{aligned}\|T(U,V)\| &= \|\Psi(P_1 - zUV)\| \leq \\ &\leq A\|P_1 - zUV\| \leq \\ &\leq A(\|P_1\| + \|zUV\|) \leq \\ &\leq A\|P_1\| + Ar\|U\|\|V\|. \qquad (3)\end{aligned}$$

Let R and r be real numbers such that

$$R > A\|P_1\|$$

and

$$r < r_1 = (R - A\|P_1\|)/AR^2.$$

Then, if B_R is a ball in $\mathscr{A}^{m+p}$ defined by $\|U\| + \|V\| \leq R$, we have from (3) that

$$\begin{aligned}\|T(U,V)\| &\leq A\|P_1\| + \frac{R - A\|P_1\|}{R^2}\|U\|\|V\| \leq \\ &\leq A\|P_1\| + \frac{R - A\|P_1\|}{R^2}R^2 \leq R.\end{aligned}$$

In other words, the ball B_R is stable under T.

Now, if $(U,V), (U'V') \in B_R$, then $\|U\| \leq R$ and $\|V'\| \leq R$, so $\|U\| + \|V'\| \leq 2R$ This gives us

$$\begin{aligned}\|T(U,V) - T(U',V')\| &= \|\Psi(P_1 - zUV) - \Psi(P_1 - zU'V')\| = \\ &= \|\Psi(-zUV + zU'V')\| \leq \\ &\leq Ar\|UV - U'V'\| \leq \\ &\leq Ar\|U(V - V') + V'(U - U')\| \leq \\ &\leq Ar(\|U\|\|(V - V')\| + \|V'\|\|(U - U')\|) \leq \\ &\leq Ar(\|U\| + \|V'\|)(\|(V - V')\| + \|(U - U')\|) \leq \\ &\leq 2ArR(\|(U - U')\| + \|(V - V')\|)\end{aligned}$$

So, if $r < r_2 = 1/2AR$, then T is a contracting map. If we now fix $R > A\|P_1\|$, we can choose $\rho < \min(r, r_1, r_2)$. By the reasoning above, we get that for such ρ, the restriction of the map T to B_R is a contracting self-map. Hence, by the Banach fixed point theorem [5, p. 1], there is a unique point $(U,V) \in B_r$ such that $T(U,V) = (U,V)$. By relation (2), this proves the proposition. □

Theorem 2.4 (Puiseux's Theorem)**.**
Let $P \in \mathscr{A}(r)[X]$ be a monic polynomial of degree n. Then, there exists a positive integer e, a real number $\rho \in (0, r^{1/m}]$, and functions $x_1, \ldots, x_n \in \mathscr{A}(\rho)$ such that

$$P(z^e, X) = \prod_{i=1}^{n}(X - x_i(z)).$$

Proof. Assume that P has more than one root and let $P(0, X) = \prod_j (X - z_j)^{n_j}$ be a factorization such that $z_i \neq z_j$ for any i, j in the factorization. By repeated use of Proposition 2.3, this gives us a factorization $P = \prod_j P_j$, where $P_j \in \mathscr{A}(\rho)[X]$ and $P_j(0, X) = (X - z_j)^{n_j}$. We will now continue by induction on the degree of P. If P has degree $n \leq 1$ the theorem is trivially true. Our induction hypothesis is that the theorem holds for all monic polynomials of degree $k < n$ with coefficients in $\mathscr{A}(r)$. Since all factors P_j have degree $n_j < n$, we have by the induction hypothesis that for any factor P_j of P, there exists an integer $e_j \geq 1$ and functions $x_{j,i} \in \mathscr{A}(\rho_j)$, $1 \leq i \leq n_j$, such that

$$P_j(z^{m_j}, X) = \prod_{j=1}^{n_j}(X - x_{j,i}(z)).$$

Let e be the least common multiple of all e_j and let $f_j = e/e_j$. Then we have that

$$P(z^e, X) = \prod_j P_j((z^{f_j})^{e_j}, X) = \prod_j \prod_{i=1}^{n_j}(X - x_{j,i}(z^{f_j})).$$

So if we let $\rho = \min(\rho_j^{1/f_j})$, the theorem is proved under the assumption that $P(0, X)$ has distinct roots. If $P(0, X)$ only has one root, the factorization above is simply the linear factors of P and we won't be able to use induction like we did, as $n_j = n$.

Assume now that $P(0, X)$ has a unique root α, i.e. $P(0, X) = (X - \alpha)^n$. Using the binomial formula, we get that

$$(X - \alpha)^n = \sum_{k=0}^{n} \binom{n}{k} X^{n-k}(-\alpha)^k$$

By setting $k = 1$, we get that the coefficient in front of X^{n-1} in $P(0, X)$ is equal to

$$\binom{n}{1}(-\alpha) = -n\alpha.$$

If we call this coefficient $a_{n-1}(0)$ then $\alpha = -a_{n-1}(0)/n$ and we can write

$$P(0, X) = (X + a_{n-1}(0)/n)^n \tag{4}$$

With $P(z, X) = X^n + a_{n-1}(z)X^{n-1} + \cdots + a_1(z)X + a_0$ we can make variable change $Y = X - a_1(z)/n$ and use the Tschirnhaus Transformation to get that

$$P(z, Y) = Y^n + b_2(z)Y^{n-2} + \cdots + b_n(z).$$

By (4), we have that $P(0, Y) = Y^n$. The rest of the proof will continue with this transformation in mind, letting us regard P as a polynomial without any term containing X^{n-1}. This can be done without loss of generality, because if we prove that the theorem holds for $P(z, Y) = P\left(z, X - a_1(z)/n\right)$, the roots of $P\left(z, X - a_1(z)/n\right)$ are

$$\{x_i(z) + a_1(z)/n \mid 1 \leq i \leq n\}$$

and they are in $\mathscr{A}(\rho)$ since $a_1(z)/n \in \mathscr{A}(r)$ and $\mathscr{A}(\rho) \subset \mathscr{A}(r)$.

Now, for any function as a power series $f = \sum_{n\geq 0} a_n z^n \in \mathscr{A}(r)$, the order of f is the smallest integer n such that $a_n \neq 0$. Or equivalently, the highest power of z dividing f. We denote it $o(f)$. With $P = X^n + a_2 X^{n-2} + \cdots + a_n$, we now make the following claim (which we will prove after finishing the proof of the theorem):

Claim 2.4.1.
Let $\nu = \min_{2\leq j\neq n} (o(a_j)/j)$ with $\nu = m/e$ being its simplest form (i.e. m and e are two nonnegative coprime integers). Then, there is a monic polynomial $Q \in \mathscr{A}(r^{1/e})$ of degree n such that

$$z^{mn} Q(z, X) = P(z^e, z^m X).$$

Furthermore, $Q(0, X) \neq X^n$.

Since the coefficient of X^{n-1} in $Q(0, X)$ is zero, the sum of all the roots of $Q(0, X)$ is zero. And as $Q(0, X) \neq X^n$, Q has distinct roots. As shown above, Puiseux's Theorem then holds for Q and so there exists an integer $f \geq 1$, a real number $\rho < r^{1/m}$ and power series $y_j(z) \in \mathscr{A}(\rho)$ such that

$$Q(z^f, X) = \prod_{j=1}^{n} (X - y_j(z)).$$

Therefore,

$$\begin{aligned}
&P(z^{ef}, z^{mf} X) = z^{mnf} \prod_{j=1}^{n} (X - y_j(z)) \Leftrightarrow \\
\Leftrightarrow\ & P\left(z^{ef}, z^{mf} \frac{X}{z^{mf}}\right) = z^{mnf} \prod_{j=1}^{n} \left(\frac{z^{mf}}{z^{mf}} \left(\frac{X}{z^{mf}} - y_j(z)\right)\right) \Leftrightarrow \\
\Leftrightarrow\ & P(z^{ef}, X) = z^{mnf} \prod_{j=1}^{n} \left(\frac{1}{z^{mf}} \left(X - z^{mf} y_j(z)\right)\right) \Leftrightarrow \\
\Leftrightarrow\ & P(z^{ef}, X) = \prod_{j=1}^{n} \left(X - z^{mf} y_j(z)\right).
\end{aligned}$$

With $x_j = z^{mf} y_j(z))$, we have that $x_j \in \mathscr{A}(\rho)$. And as ef is a positive integer, this proves the theorem.

Proof of Claim 2.4.1. For

$$P(z^e, z^m X) = \sum_{j=0}^{n} a_j(z^e) z^{m(n-j)} X^{n-j}$$

the coefficient $a_j(z^e) z^{m(n-j)}$ is a power series with order

$$\begin{aligned}
eo(a_j) + m(n-j) &= mn + e\left(o(a_j) - j\frac{m}{e}\right) \\
&= mn + e\left(o(a_j) - j\nu\right) \geq mn.
\end{aligned}$$

Since the order of a power series also is the highest power of z dividing the power series, there is a $b_j \in \mathscr{A}(r^{1/e})$ such that $a_j(z^e) z^{m(n-j)} = z^{mn} b_j$. This lets us define Q as

$$Q = \sum_{j=0}^{n} b_j X^{n-j} \in \mathscr{A}(r^{1/e})[X],$$

which gives the equality $z^{mn}Q(z,X) = P(z^e, z^m X)$. Now choose the particular $j \geq 2$ such that $o(a_j)/j = \nu$. Then

$$o(z^{mn}b_j) = mn + e\,(o(a_j) - o(a_j)) = mn,$$

so $o(b_j) = 0$ and $Q(0,X) \neq X^n$. This concludes the proof of the theorem. □

The reasons why we need this result may not be obvious at the moment. However, for any irreducible polynomial $P \in \mathbb{Q}(T)[X]$, it turns out that this theorem will let us determine the complex roots of $P(t,X)$, for $t \in \mathbb{C}$ and $|t|$ large enough, in a particularly useful way.

3. Hilbert's Irreducibility Theorem

We will now begin the somewhat technical process of proving Hilbert's Irreducibility Theorem. In Proposition 3.2 we will show a particularly important result for nonpolynomial Laurent series with finite order. In its most basic form, this proposition says that there are infinitely many $t \in \mathbb{Z}$ such that the Laurent series evaluated at t is not an integer.

Lemma 3.1.
Let I be an interval in $\mathbb{R}$, with $x_0, \ldots, x_n \in I$. Let $f : I \to \mathbb{R}$ a $\mathscr{C}^n$-function. Then, there exists an element $\xi \in I$ such that

$$\begin{vmatrix} 1 & \ldots & 1 \\ x_0 & \ldots & x_n \\ \vdots & & \vdots \\ x_0^{n-1} & \ldots & x_n^{n-1} \\ f(x_0) & \ldots & f(x_n) \end{vmatrix} = \frac{f^{(n)}(\xi)}{n!} \prod_{i>j} (x_i - x_j).$$

Proof. Suppose $x_i = x_j$ for some $i, j \in \{0, \ldots n\}$. Then column i in the matrix is equal to column j, and the determinant is zero and the formula is obviously true for any $\xi \in I$. It is therefore enough to prove for the case where all x_i are distinct. Consider now the determinant

$$D(t) = \begin{vmatrix} 1 & \ldots & 1 \\ t & \ldots & x_n \\ \vdots & & \vdots \\ t^{n-1} & \ldots & x_n^{n-1} \\ f(t) & \ldots & f(x_n) \end{vmatrix}.$$

Then $D(x_0)$ is the determinant in the lemma. Define for $A \in \mathbb{R}$ the function

$$F_A : \begin{cases} I \to \mathbb{R} \\ x \mapsto D(x) - A \prod_{i=1}^{n} (x - x_i) \end{cases}$$

For any $x_j \in \{x_1, \ldots, x_n\}$ we get $F_A(x_j) = D(x_j) - A \prod_{i=1}^{n} (x_j - x_i) = 0$, since the first column in $D(x_j)$ will be equal to the j:th column, and since $A \prod_{i=1}^{n} (x_j - x_i)$

will vanish at the factor $x_j - x_j$. By letting $A = \frac{D(x_0)}{\prod_{i=1}^{n}(x_0 - x_i)}$, we also get that $F_A(x_0) = 0$, so F_A vanishes at $x_0, \dots, x_n$. Consider now the intervals $[x_i, x_{i+1}]$, $0 \leq i \leq n-1$. Since F_A is a polynomial function it is continuous, and so by Rolle's Lemma, the derivative of F_A vanishes at a point in (x_i, x_{i+1}), for each such interval. In particular, the derivative of F_A vanishes at n distinct points on I. By induction, the i:th derivative vanishes at $n+1-i$ distinct points, and so the n:th derivative vanishes at one point, say $\xi \in I$.

Now, $A \prod_{i=1}^{n}(x - x_i) = A(x^n + P(x))$, where $P(x)$ is a polynomial of degree $n-1$. So

$$0 = F_A^{(n)}(\xi) = D^{(n)}(\xi) - An! = \begin{vmatrix} 0 & 1 & \dots & 1 \\ \vdots & x_1 & \dots & x_n \\ \vdots & \vdots & & \vdots \\ 0 & x_1^{n-1} & \dots & x_n^{n-1} \\ f^{(n)}(\xi) & f(x_1) & \dots & f(x_n) \end{vmatrix} - An! =$$

$$= (-1)^n f^{(n)}(\xi) \begin{vmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{vmatrix} - An!.$$

Using the formula for the Vandermonde determinant gives us that

$$A = (-1)^n \frac{f^{(n)}(\xi)}{n!} \prod_{i>j\geq 1} (x_i - x_j)$$

And by the choice of A we get

$$D(x_0) = A \prod_{i=1}^{n}(x_0 - x_i) = \frac{f^{(n)}(\xi)}{n!} \prod_{i>j}(x_i - x_j),$$

which proves the lemma. □

Proposition 3.2.
Let e be a positive integer and let $\varphi(u) = \sum_{n \geq -n_0} a_n u^{-n/e}$ be a Laurent series which is not a polynomial in u. Assume that $\varphi(u)$ converges for $|u| \geq B_0$. Let $N(B)$ be the number of integers $u \in [B_0, B]$ such that $\varphi(u)$ is also an integer. Then there exists a real number $\alpha < 1$ such that $N(B)/B^\alpha$ remains bounded when $B \to \infty$.

Proof. If both the real and the imaginary part of φ would be a polynomial, then φ would be a polynomial.

Note that $\mathrm{Re}(\varphi(u)) : (B_0, \infty) \to \mathbb{R}$ is $\mathscr{C}^\infty$. We get the derivatives of φ by deriving each term separately. The derivative of order m of the n^{th} term has the form $cu^{-n/e-m}$ for some $c \neq 0$. Furthermore, since $n \geq -n_0$ we get that $-n/e - m \leq n_0/e - m$. Hence, for $m > n_0/e$ the derivative of each term has the form $cu^{-\mu}$ for some $\mu > 0$ and the derivative $\varphi^{(m)}(u) \to 0$ as $u \to \infty$. Since φ is not a polynomial the derivative is note $\varphi^{(m)}$ is not zero, and for u large enough $\varphi^{(m)}(u)$

will be arbitrarily close to its first term, which as noted is on the form $cu^{-\mu}$. We write $\varphi^{(m)}(u) = u^{-\mu}\psi(u)$, where $\psi(u)$ is a power series converging for large enough u. With the change of variable $u = 1/v$ we get that $\tilde{\psi}(v) = \psi(1/v)$ is a power series converging for v close enough to zero and with $\tilde{\psi}(0) = c$. For v in a small neighborhood around 0 we then get that $\tilde{\psi}(v)$ is arbitrarily close to c. Going back to the variable u gives us $|\tilde{\psi}(v)| = |\psi(u)|$. Therefore, for large enough u, say $u \geq B_1$, there exists constants c_1 and c_2 such that

$$c_1 \leq |\psi(u)| \leq c_2 \;\Leftrightarrow\; c_1 u^{-\mu} \leq |\varphi^{(m)}(u)| \leq c_2 u^{-\mu}. \tag{1}$$

Let $S = \{u \in \mathbb{Z} : u \geq B_0, \varphi(u) \in \mathbb{Z}\}$. Now let $u_0 < \dots u_m$ be $m+1$ elements in S with $u_0 > B_1$. Consider the determinant

$$D = \begin{vmatrix} 1 & \dots & 1 \\ u_0 & \dots & u_m \\ \vdots & & \vdots \\ u_0^{m-1} & \dots & u_m^m \\ \varphi(u_0) & \dots & \varphi(u_m) \end{vmatrix}$$

By the preceding lemma, there exists a real number $\xi \in (u_0, u_m)$ such that

$$D = \frac{1}{m!}\varphi^{(m)}(\xi)\prod_{i>j}(u_i - u_j).$$

By relation (1) we have that $\varphi^{(m)}(\xi) \neq 0$, since $u_0 \geq B_1$. And since all u_i, u_j are distinct, this also implies that $D \neq 0$. Since D is a determinant of a matrix with integer coefficients, it is an integer and so $|D| \geq 1$. This gives us

$$|D| = \frac{1}{m!}\left|\varphi^{(m)}(\xi)\right|\prod_{i>j}(u_i - u_j) \geq 1 \Leftrightarrow$$

$$\Leftrightarrow \prod_{i>j}(u_i - u_j) \geq \frac{m!}{\left|\varphi^{(m)}(\xi)\right|} \geq \frac{m!}{c_2}\xi^{\mu}$$

The number of factors in $\prod_{i>j}(u_i - u_j)$ can combinatorially be regarded as the number of ways to choose two elements from $m+1$ without taking order into consideration, which can be done in $m(m+1)/2$ ways. Since $u_m - u_0 \geq u_i - u_j$ we get $(u_m - u_0)^{m(m+1)/2} \geq \prod_{i>j}(u_i - u_j)$. Since $u_0 < \xi$, we now get the inequality

$$(u_m - u_0)^{m(m+1)/2} \geq \frac{m!}{c_2}u_0^{\mu}.$$

By solving this inequality for $u_m - u_0$ we get that

$$u_m - u_0 \geq bu_0^{\beta} \Leftrightarrow u_m \geq u_0 + bu_0^{\beta} \tag{2}$$

for some positive real numbers b and β. Let $\alpha = 1/(1+\beta)$ and note that $[B_0, B] = [B_0, B^{\alpha}] \cup [B^{\alpha}, B]$. The interval $[B_0, B^{\alpha}]$ contains at most B^{α} elements of S. Now, choose B large enough so that $B^{\alpha} \geq B_1$ and let u_j, u_i be any two consecutive elements of S in $[B^{\alpha}, B]$, with $u_i < u_j$. By relation (2) we get that

$$u_j - u_i \geq bu_i^{\beta} \geq bB^{\alpha\beta}.$$

In other words, the distance between to consecutive elements of S in $[B^{\alpha}, B]$ is at least $bB^{\alpha\beta}$ Suppose that there are k elements of S in $[B^{\alpha}, B]$. Since B is an upper

bound of S, we get that

$$\begin{aligned} B^\alpha + kbB^{\alpha\beta} \leq B \Leftrightarrow k \leq \frac{(B - B^\alpha)}{bB^{\alpha\beta}} \Leftrightarrow \\ \Leftrightarrow k \leq \frac{B^{1-\alpha\beta}}{b} - \frac{1}{bB^\beta} \Leftrightarrow \\ \Leftrightarrow k \leq \frac{B^{1-\alpha\beta}}{b} - \frac{1}{bB^\beta} \Rightarrow \\ \Leftrightarrow k \leq (1/b)B^\alpha. \end{aligned}$$

Now, for $B \geq B_1^{1/\alpha}$, we have that $N(B) \leq (1 + 1/b)B^\alpha$, and so

$$\frac{N(B)}{B^\alpha} \leq 1 + 1/b$$

for large enough B. □

That $N(B)/B^\alpha$ remains bounded when $B \to \infty$ is equivalent to saying that there exists a real numbers $M > 0$ and x_0 such that $N(B)/B^\alpha \leq M$ for all $x > x_0$. This is precisely the definition of $N(B) = O(B^\alpha)$, and we will use this notation.

Lemma 3.3.
Let $P \in \mathbb{Q}(T)[X]$ be a monic polynomial with degree n. There exists an integer $e \geq 1$ and Laurent series $x_1, \ldots, x_n$, with complex coefficients and nonzero radius of convergence, such that for any complex number t, with $|t|$ big enough, the set of the n complex roots of $P(t^e, X) \in \mathbb{Q}[X]$ is $\{x_j(1/t) \mid 1 \leq j \leq n\}$.

Proof. We first note that since $\mathbb{Q}(1/U) = \mathbb{Q}(U)$, we can make the variable change $T = 1/U$ and consider $P(T, X) \in \mathbb{Q}(T)[X]$ as a polynomial $P(1/U, X) \in \mathbb{Q}(U)[X]$.

Now, let R be a common denominator of the coefficients of $P(1/U, X)$. Then $R(U)P(1/U, X) \in \mathbb{Q}[U, X]$. By multiplying with $R(U)^{n-1}$ we get a polynomial $P(1/U, X)R(U)^n$, for which we can find $Q \in \mathbb{Q}[U, Y]$ such that $Q(U, R(U)X) = P(1/U, X)R(U)^n$ is monic and of degree n with respect to Y. Regarded as a polynomial in $\mathbb{Q}[Y]$, Q has coefficients $f_i \in \mathbb{Q}[U]$, so $f_i \in \mathscr{A}(r)$ for $r > 0$. By Puiseux's Theorem there exists an integer $e \geq 1$, a real number $\rho \in (0, r^{1/e})$ and functions $y_1, \ldots, y_n \in \mathscr{A}(\rho)$ such that $Q(u^e, Y) = \prod_{i=1}^{n} (Y - y_i(u))$. In particular, the roots of $Q(u^e, Y)$ are the $y_j(u)$, $1 \leq j \leq n$, for $0 \leq |u| < \rho$. Furthermore, since $R(u)$ is a polynomial in $\mathbb{Q}[u]$ we have that

$$R(u)^{-e} = \frac{1}{(a_n u^n + \ldots + a_0)^e}$$

is a Laurent series convergent for $|u| \neq 0$. Now, let $x_j(u) = R(u)^{-e} y_j(u)$. Changing back to the variable t gives us that the $x_j(1/t)$ are the roots of $P(t^e, X)$ when $|t|$ is large enough. □

We are now ready to prove the main theorem for this text, namely the Hilbert's Irreducibility Theorem.

Theorem 3.4 (Hilbert's Irreducibility Theorem)**.**
Let $P \in \mathbb{Q}(T)[X]$ be a monic irreducible polynomial. Denote by $N(B)$ the number of integers $t \in [0, B]$ such that $P(t, X)$ is well defined and that $P(t, X)$ is reducible in $\mathbb{Q}[X]$. Then there is a real number $\alpha < 1$ such that $N(B) = O(B^\alpha)$. In particular, the number of $t \in \mathbb{N}$ such that the specialization $P(t, X)$ of the polynomial $P(T, X)$ remains irreducible in $\mathbb{Q}[X]$ is unbounded.

Proof. Let $D \in \mathbb{Z}[T]$ be a common denominator of the coefficients of P, so that $P(T, X)D(T) \in \mathbb{Z}[T, X]$. Like in the preceding lemma, multiply with D^{n-1} to get $P(T, X)D(T)^n = Q(T, D(T)X)$, with $Q \in \mathbb{Z}[T, X]$ being a monic polynomial of degree n in X. If $D(t) \neq 0$ we have that $P(t, X) = \frac{Q(t,D(t)X)}{D(t)^n} \in \mathbb{Q}[X]$, which has a root $R(t) \in \mathbb{Q}$ if and only if $R(t)D(t) \in \mathbb{Q}$ is a root of $Q(t, Y)$. And since $P(T, X) = \frac{Q(T,D(T)X)}{D(T)^n}$ by assumption has no root in $\mathbb{Q}(T)$, neither Q has a root in $\mathbb{Q}(T)$. Therefore, it is enough to prove the theorem for Q, and so we may assume that $P \in \mathbb{Z}[T, X]$.

Now, let n be the degree of P and let $x_1, \ldots, x_n$ be the Laurent series given by the preceding lemma. These Laurent series converges for large enough $t \neq 0$, so we can say they converge for $t \geq B_0$. By letting $t = s^e$, we get that the $x_i(1/s) = x_i(t^{-1/e})$ are the roots of $P(s^e, X) = P(t, X)$. So, $P(t, X) = \prod_{i=1}^{n} (X - x_i(t^{-1/e}))$. Therefore, any monic factor of $P(t, X)$ can be written as the product of $X - x_i(t^{-1/e})$, with i ranging over a nonempty subset $I \subset \{1, \ldots, n\}$. We are interested in $t \in [0, B]$ such that $P(t, X)$ is reducible in $\mathbb{Z}[X]$. For such t, $P(t, X)$ has a monic factor in $\mathbb{Z}[X]$, i.e. we look at $t \in [0, B]$ for which there exists nonempty proper subsets $I \subset \{1, \ldots, n\}$ such that $\prod_{i \in I} (X - x_i(t^{-1/e})) = P_I(t) \in \mathbb{Z}[X]$. Now let K be the field of convergent Laurent series in the variable $T^{-1/e}$. Then we can consider P_I as a factor of $P \in K[X]$. If all coefficients of P_I where polynomials in T, then P_I would be in $\mathbb{Q}(T)[X]$. But this is a contradiction since P is irreducible in $\mathbb{Q}[T, X]$, so at least one of the coefficients of P_I is not a polynomial in T. Call this coefficient φ_I, and let $N'(B) = |\{t \in [B_0, B] : t, \varphi_I(t) \in \mathbb{Z}\}|$. By Proposition 5.9.1, there exists an $\alpha < 1$ such that $N'(B)/B^\alpha$ remains bounded when $B \to \infty$, and since $N(B) \leq N'(B)$ we can chose the same α to conclude that $N(B)/B^\alpha$ remains bounded when $B \to \infty$. Now, suppose that there is a real number M such that the cardinality of the set $\{t \in \mathbb{N} \mid P(t, X) \text{ is reducible in } \mathbb{Q}[X]\}$ is less than M. For a large enough B_0, $N(B) \geq B - M - 1$ for all $B > B_0$. But then,

$$\frac{N(B)}{B^\alpha} \geq \frac{B - M - 1}{B^\alpha} = B^{1-\alpha} - \frac{M + 1}{B^\alpha} \to \infty \text{ as } B \to \infty,$$

which is a contradiction. Therefore, there is no such bound M. □

This theorem is widely used in different areas of Number Theory. Later, we will look more closely to a particular application to an unsolved question regarding Galois theory. In Number Theory we often encounter problem that are easy to formulate and comprehend, but very complex to prove. One of the most famous examples of this perhaps Andrew Wiles' proof of Fermat's Last Theorem, in which he actually uses Hilbert's Irreducibility Problem. That work is of course far beyond the scope of this paper, so instead this little example will serve as an illustration of how one can take long, tedious and hopefully enlightening paths to solve seemingly simple problems:

Example 3.5.
Let $g(X) \in \mathbb{Z}[X]$. If there is an $M \in \mathbb{Z}$ such that $g(a)$ is a perfect square for all $a > M$, then $g(X) = (h(X))^2$ for some $h(X) \in \mathbb{Z}$.

Proof. Let $f(X,Y) = Y^2 - g(X)$. If $f(X,Y)$ is irreducible then, by Hilbert's Irreducibility Theorem, $f(t,Y)$ is also irreducible for infinitely many $t \in \mathbb{N}$. But $f(t,Y)$ is reducible for all $t > m$, so $f(X,Y)$ must be irreducible. We can therefore write $f(X,Y) = f_1(X,Y)f_2(X,Y)$. Since $g(X)$ is not dependent on Y, Y^2 cannot be a factor of f. In the variable Y, f_1 and f_2 must therefore both be monic polynomials of degree 1. If $f_1 = (Y + a_0 + a_1X + \cdots + a_nX^n)$ and $f_2 = (Y + b_0 + b_1X + \cdots + b_mX^m)$ we see that the coefficient in front of YX^i in f_1f_2 is equal to $a_i + b_1$. Since f does not have any terms with both X and Y, we get that $a_i = -b_i$ and $f = (Y + h(X))(Y - h(X)) = Y^2 - (h(X))^2$. □

4. Symmetric Polynomials

In the study of Galois groups we will see that polynomials that stay the same under all permutations of the indices of the variables are very important. These polynomials are called symmetric polynomials and we will see that they are in a sense all constructed from the same fundamental symmetric polynomials.

Definition 4.1.
*The **elementary symmetric polynomials** in variables $X_1, \ldots, X_n$, denoted $S_1, \ldots, S_n$, are defined as*

$$S_p(X_1, \ldots, X_n) = \sum_{1 \le i_1 < \cdots < i_p \le n} X_{i_1} \cdots X_{i_p}$$

If necessary to specify the number of variables, we will write $S_p(X_1, \ldots, X_n)$ as $S_p^{(n)}(X_1, \ldots, X_n)$

Theorem 4.2 (Fundamental Theorem of Symmetric Polynomials)**.**
Let A be a commutative ring and P any symmetric polynomial in $A[X_1, \ldots X_n]$. Then, there exists a unique polynomial $Q \in A[Y_1, \ldots Y_n]$ such that

$$P(X_1, \ldots, X_n) = Q(S_1(X_1, \ldots, X_n), \ldots, S_n(X_1, \ldots, X_n))$$

Proof. We will prove this by induction , first on the number of variables n and then on the degree of P. Our base case for n is that $n = 1$, which gives us $S_1 = X_1$ and $Q = P$. The base case for the degree of P is that $\deg(P) = 0$, i.e. $P = C$ is a constant. Simply letting $Q = C$ shows the theorem holds for any n if $\deg(P) = 0$.

Our induction hypothesis is now that the theorem holds in $n-1$ variables and that it also holds in n variables for polynomials of degree less than m. Let P be any symmetric polynomial of degree m in variables $X_1, \ldots, X_n$. Then, the polynomial $P_0(X_1, \ldots X_{n-1}) = P(X_1, \ldots X_{n-1}, 0)$ is a symmetric polynomial in $n-1$ variables. By the induction hypothesis, there is a polynomial $Q \in A[Y_1, \ldots, Y_{n.1}]$ such that

$$P_0(\boldsymbol{X}) = Q_0(S_1^{(n-1)}(\boldsymbol{X}), \ldots, S_{n-1}^{(n-1)}(\boldsymbol{X})),$$

with $\boldsymbol{X}$ denoting $X_1, \ldots, X_{n-1}$. By the definition of S_p, we have

$$S_p^{(n)}(X_1, \ldots, X_n) = S_p^{(n-1)}(X_1, \ldots, X_{n-1}) + X_n S_{p-1}^{(n-1)}(X_1, \ldots, X_{n-1}). \tag{3}$$

Now, let

$$P_1(\boldsymbol{X}, X_n) = P(\boldsymbol{X}, X_n) - Q_0(S_1^{(n)}(\boldsymbol{X}, X_n), \ldots, S_{n-1}^{(n)}(\boldsymbol{X}, X_n)).$$

This is a symmetric polynomial, and by (7), we get that $P_1(\boldsymbol{X}, 0) = 0$. Any monomial $X_1^{i_1} \cdots X_n^{i_n}$ in a term in P_1 can be written as $X_1^{i_1} \cdots X_{n-1}^{i_{n-1}}$, if $i_n = 0$. But since this monomial will stay the same if $X_n = 0$, we have that the coefficient of any such monomial must be zero, since $P_1(\boldsymbol{X}, 0) = 0$. By symmetry, the coefficient of $X_1^{i_1} \cdots X_n^{i_n}$ is then zero if any of the i_j is zero. From this we can conclude that $S_n^{(n)} = X_1 \cdots X_n$ is a factor of all nonzero terms in P_1. This motivates writing $P_1 = S_n^{(n)} P_2$ for some $P_2 \in A[X_1, \ldots, X_n]$. The polynomial P_2 must also be symmetric and since $\deg(P_2) < \deg(P_1) \leq \deg(P) = m$, the induction hypothesis lets us write

$$P_2 = Q_2(S_1^{(n)}, \ldots, S_n^{(n)})$$

We no have that

$$\begin{aligned} P(X) &= Q_0(S_1^{(n)}, \ldots, S_{n-1}^{(n)}) + P_1(X_1, \ldots, X_n) = \\ &= Q_0(S_1^{(n)}, \ldots, S_{n-1}^{(n)}) + S_n^{(n)} Q_2(S_1, \ldots, S_n). \end{aligned}$$

Letting $Q = Q_0 + Y^n Q_2$ proves the existence of Q. To show uniqueness, we will consider the polynomial $Q - Q' = H \in A[Y_1, \ldots, Y_n]$. If $Q(S_1, \ldots, S_n) = Q'(S_1, \ldots, S_n)$, then $H(S_1, \ldots, S_n) = 0$. So, it is enough to show that for any polynomial $H \in A[Y_1, \ldots, Y_n]$ such that $H(S_1, \ldots, S_n) = 0$, we have that $H = 0$. Again we show this by induction. The base case $n = 1$ follows directly from the fact that $H(S_1) = H(X_1)$. The second base case is on the degree of H. If H has degree zero, it is a constant and the statement holds, independently of n.

The induction hypothesis is that the statement is true for all polynomials in $n - 1$ variables, and also that it holds for polynomials in n variables if they have degree less than m. Now, if H is a polynomial in n variables of degree m, and that $H(S_1, \ldots, S_n) = 0$. Then for $X_n = 0$ we have

$$\begin{aligned} 0 &= H(S_1^{(n)}(X_1, \ldots, X_{n-1}, 0), \ldots, S_n^{(n)}(X_1, \ldots, X_{n-1}, 0)) = \\ &= H(S_1^{(n-1)}(X_1, \ldots, X_{n-1}), \ldots, S_{n-1}^{(n-1)}(X_1, \ldots, X_{n-1}), 0). \end{aligned}$$

By the induction hypothesis, $H(Y_1, \ldots, Y_{n-1}, 0) = 0$. From this we conclude that $H = Y^n \tilde{H}$, for some polynomial $\tilde{H} \in A[Y_1, \ldots, Y_{n-1}]$ with degree less than m. By the induction hypothesis, $\tilde{H} = 0$ which shows that $H = 0$. □

Theorem 4.3 (Vieta's Formulas)**.**
Let A be an integral domain and let $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ a monic polynomial of degree n $A[X]$. Let $x_1, \ldots, x_n$ be the roots of P in some splitting extension of P. Then, for each coefficient a_j of P, we have

$$a_{n-k} = (-1)^k S_k(x_1, \ldots, x_n).$$

where the S_k are the elementary symmetric polynomials.

Proof. The special case of this formula for a_{n-1} has already been shown in the proof of Theorem 2.4. To show the general case, we start by writing P as the product of its linear factors:

$$P = (X - x_1) \cdots (X - x_n).$$

Expanding the right hand side gives a number of terms, where every term can be defined by n binary choices, one for each product $X - x_j$. The choice is to either include X or $-x_i$ in the multiplication. We get that each $a_{n-k}X^k$ in P is the sum of the terms obtained by these choices where X has degree k. In every term where X has degree k, there must be $n - k$ number of x_i. This gives the formula

$$(-1)^k a_{n-k} = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k}$$

which proves the theorem. □

A particularly important symmetric polynomial is the discriminant.

Definition 4.4.
*The **discriminant** $\Delta(P)$ of a polynomial $P = a_n X^n + \cdots + a_0$ with roots $x_1, \ldots, x_n$ is defined as*

$$\Delta(P) = a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2 = (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i \neq j} (x_i - x_j)$$

It is clear that a polynomial is separable if and only if its discriminant is nonzero. A useful formula for the discriminant of a polynomial on the form $P = X^n + aX + b$ is

$$\Delta(P) = (-1)^{n(n-1)/2}((1-n)^{n-1}a^n + n^n b^{n-1} \quad \text{[13, p. 26]}$$

This form will be greatly useful in the last section of this paper, but we will not go into details on how to deduce it.

5. Some Fundaments of Galois Theory

For the more interesting results we will soon explore, Galois Theory is really the fundament. However, since this topic is so well covered in so many algebra text-books, we won't go too deep into all proofs. Most results in this section will just be stated as a reference, and the interested reader can find find in depth proofs and reasoning by following the references.

Theorem 5.1 (Eisenstein's criterion)**.**
Suppose that R is an integral domain and let $P = a_0 + a_1 X + \cdots + a_n X^n$ be a polynomial with coefficients in R such that $a_0, \ldots, a_n$ are coprime. If there is a prime element $p \in R$ for which the following holds

- *p divides all a_i for $0 \leq i < n$;*
- *p does not divide a_n;*
- *p^2 does not divide a_0;*

then P is irreducible in $R[X]$.

Proof. Suppose that $P = P_1P_2$ and that

$$P_1 = b_0 + b_1X + \cdots + b_rX^r \quad \text{and} \quad P_2 = c_0 + c_1X + \cdots + c_sX^s$$

are not units in R. If $r = 0$, then $P_1 = b_0$ is a constant and we have that b_0 divides all coefficients of P. But this is a contradiction since the coefficients of P are assumed to be coprime. This gives us that $r \geq 1$, and by the same reasoning we get that $s \geq 1$. By assumption, p^2 does not divide $a_0 = b_0c_0$ so p cannot divide both b_0 and c_0. Assume p does not divide c_0. Again by assumption, p does not divide $a_n = b_rc_s$, so p does not divide b_r. Let i be the least integer such that p does not divide b_i. We get that $0 \leq i \leq r < n$ and since p divides f_i we can write

$$p \mid (b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i)$$

with $c_j = 0$ for $j > s$. Since p divides all b_k with $k < i$ we get that p divides b_ic_0. But as p is prime, this means that $p \mid b_i$ or $p \mid c_0$, which is a contradiction. So P is irreducible. □

Definition 5.2.
*If K is a field and $P \in K[X]$ is a polynomial with $P = a_0 + a_1X + \cdots + a_nX^n$, then the **reciprocal polynomial** P^* of P is defined as*

$$P^* = a_n + a_{n-1}X + \cdots + a_0X^n$$

This can also be written as $X^nP(1/X)$ which shows the following proposition.

Proposition 5.3. [6, p. 39]
Let K be a field and let $P \in K[X]$ be a polynomial with nonzero constant term. Then α is a root of P if and only if α^{-1} is a root of the reciprocal polynomial P^*. Furthermore, if P is irreducible then P^* is irreducible.

Proof. If $\alpha \neq 0$, then $(\alpha^{-1})^nP(\alpha) = 0$ if and only if $P(\alpha) = 0$. This gives the first part of the proposition. To prove the second part, we assume that P is irreducible and that P^* is reducible. Say P has degree n and write $P^* = QR$, where Q and R are nonconstant polynomials of degree k and m respectively. By definition, the polynomial P is the reciprocal of P^* so we get

$$P(X) = X^nP^*(1/X) = X^kQ(1/X)X^mR(1/X).$$

But this means that $P(X)$ is reducible which is a contradiction, so P^* must be irreducible. □

Proposition 5.4. [1, pp. 41–42.]
Let $K \subset L$ be a field extension and let P and Q be two polynomials with coefficients in K. Then, the greatest common divisor of P and Q as polynomials in $L[X]$ is equal to the greatest common divisor of P and Q as polynomials in $K[X]$.

Lemma 5.5 (Gauss' Lemma)**.** [1, p. 42.]
Let P be a polynomial in $F[X]$. If A and B are two polynomials in $F[X]$ such that P divides AB, then P divides A or P divides B. Furthermore, if K is the quotient field over F and P is irreducible in $F[X]$, we have that P is also irreducible in $K[X]$.

Definition 5.6.
Any field homomorphism $j : K \to L$ is called a ***field extension****.*

A field homomorphism is always injective [1, p. 9] and in most cases it makes sense to identify K with its image in L. In this text, we will consider field extensions where K is a subfield of L and write the field extension as $K \subset L$ (this corresponds to the field homomorphism where j is the inclusion mapping). Looking at L as an K-vector space with scalar multiplication $K \times L \to L$ defined by $k \cdot \ell = j(k)\ell$ justifies the following definition.

Definition 5.7.
The ***degree*** *of a field extension $j : K \to L$ is the degree of L as an K-vector space. We write this as $[L : K]$ and say that $K \subset L$ is a finite extension if $[L : K]$ is finite.*

Definition 5.8.
If P is a nonconstant polynomial with coefficients in K and $K \subset L$ is a field extension, then L is called a ***splitting extension*** *of P it there exist $x_1, \ldots, x_n \in L$ such that*

(1) *The polynomial P can be factored into linear factors over L, i.e.*

$$P = c\prod_{i=1}^{n}(X - x_i),$$

where n is the degree of P and c is the leading coefficient of P.

(2) *The field L is the smallest field in which (1) applies, i.e. $L = K(x_1, \ldots, x_n)$.*

Definition 5.9.
If $K \subset L$ is a field extension, then an element $\alpha \in L$ is ***algebraic*** *over K if there exists a polynomial $P \in K[X]$ such that $P(\alpha) = 0$. The monic polynomial of least degree with coefficients in K that has α as a root is called* ***the minimal polynomial*** *of α. A field extension $K \subset L$ is said to be algebraic if any element in L is algebraic over K.*

Definition 5.10.
A field K is said to be ***algebraically closed*** *if any nonconstant polynomial of $K[X]$ has a root in K. Furthermore, an* ***algebraic closure*** *of K is an algebraic extension $K \subset \Omega$ where Ω is an algebraically closed field.*

Definition 5.11.
Let $K \subset L$ be an algebraic extension and Ω be an algebraic closure on K. A polynomial P with coefficients in a field K is ***separable*** *if its roots in Ω are distinct. We say that an element $\alpha \in L$ is separable over K if its minimal polynomial is separable. If the minimal polynomial of every element $\alpha \in L$ is separable, then $K \subset L$ is called a separable extension.*

Lemma 5.12. [1, p. 56]
Let K be a field and let P be a polynomial in $K[X]$. Then the following holds:

(1) *P is separable if and only if it P and its formal derivative P' are coprime.*

(2) *A root α of P is multiple if and only if $P'(\alpha) = 0$.*

Proposition 5.13. [2, p. 273]
If $K \subset L$ is a field extension and $\alpha \in L$ is algebraic over K with minimal polynomial $P \in K[X]$, then $K(\alpha)$ is isomorphic to $K[X]/\langle P \rangle$, where $\langle P \rangle$ is the ideal generated by P.

Corollary 5.13.1.
If an element α is algebraic over K, then $K(\alpha) = K[\alpha]$. In particular, if $P \in K[X]$ is a polynomial with roots $x_1, \ldots, x_n$, then the splitting field $K(x_1, \ldots, x_n)$ over P is equal to $K[x_1, \ldots, x_n]$

We won't prove this corollary in detail, but the idea is simply to note that the mapping from $K[X]/\langle P \rangle$ to $K[\alpha]$ defined by

$$Q(X) + \langle P(X) \rangle \mapsto Q(\alpha) + \langle P(\alpha) \rangle = Q(\alpha)$$

is a bijection.

Theorem 5.14 (Primitive Element Theorem)**.** [1, p. 66]
Let $K \subset L$ be a finite separable extension. Then, there exists an element $x \in L$ such that $L = K[x]$.

Definition 5.15.
*An **automorphism** on L is a bijective mapping $\phi : L \to L$. The group of all automorphisms on L is denoted $Aut(L)$.*

Definition 5.16.
*A finite field extension $K \subset L$ is called a **Galois extension** if the group*

$$Aut(L/K) = \{\phi \in Aut(L) \mid \phi(a) = a \ \text{ for all } \ a \in K\}$$

*has cardinality $[L : K]$. The group $Aut(L/K)$ is then called its **Galois group**.*

Definition 5.17.
*If G is a group that acts on a set X, we say that G acts **transitively** on X if for all $x, y \in X$ there is a $g \in G$ such that $g(x) = y$. If G acts transitively on the set X, then G is said to be **doubly transitive** if for every $x_i \in X$, the stabilizer G_{x_i} acts transitively on the remaining elements of X.*

Proposition 5.18. [1, pp. 65–66]
Let K be a field and let $P \in K[X]$ be a separable polynomial. Let $K \subset L$ be a splitting extension of P and $G = Gal(L/K)$. Then, the action of G on the roots of P is transitive if and only if P is irreducible in $K[X]$.

Proposition 5.19. [1, p. 60]
Let $K \subset L$ be a finite extension. The following conditions are equivalent:

(1) *The extension $K \subset L$ is Galois.*

(2) *The extension $K \subset L$ is separable and any irreducible polynomial in $K[X]$ with a root in L is split in L.*

(3) *There exists a separable polynomial $P \in K[X]$ for which the extension $K \subset L$ is a splitting extension.*

Lemma 5.20 (Artin's Lemma)**.** [1, p. 61]
Let L be a field and let G be a finite group of automorphisms on L. The set

$$K = L^G = \{x \in L \mid \sigma(x) = x \ \text{ for all } \ \sigma \in G\}$$

is a subfield of L and the extension $K \subset L$ is Galois with Galois group G.

Theorem 5.21 (Galois correspondence)**.** [1, p. 60]
Let $K \subset L$ be a finite Galois extension with $G = Gal(L/K)$. Then the following holds:

(1) *For any subgroup $H \subset G$, the set*

$$L^H = \{x \in L \mid \sigma(x) = x \ \text{ for all } \ \sigma \in H\}$$

is a subfield of L containing K.

(2) *For any field E such that $K \subset E \subset L$, the extension $E \subset L$ is Galois and*

$$Gal(L/E) = \{\sigma \in G \mid \sigma(x) = x \ \text{ for all } \ x \in E\}$$

(3) *There is a bijection between the set of subgroups of G and the set of subfields of L that contain K. This bijection is defined by the map $H \mapsto L^H$, which has the inverse $E \mapsto Gal(L/E)$. Furthermore, if $H \subset H'$ then $L^H \subset L^{H'}$, and if $E \subset E'$, then $Gal(L/E') \subset Gal(L/E)$.*

We end this section with an example related to the previous section on symmetric polynomials as well as coming sections about the Inverse Galois Problem.

Example 5.22.
If $S_1, \ldots, S_n$ are the elementary symmetric functions over variables $X_1, \ldots, X_n$, then the function field $\mathbb{Q}(X_1, \ldots, X_n)$ is a Galois extension of $\mathbb{Q}(S_1, \ldots, S_n)$ with the symmetric group $\mathfrak{S}_n$ as Galois group.

Proof. Let $P = (Y - X_1) \cdots (Y - X_n)$. As showed in the proof of Theorem 4.3, the coefficients of this polynomial are $S_1(X_1, \ldots, X_n), \ldots, S_n(X_1, \ldots, X_n)$, so P is in $\mathbb{Q}(S_1, \ldots, S_n)[Y]$. Furthermore, $\mathbb{Q}(X_1, \ldots, X_n) = \mathbb{Q}(\boldsymbol{X})$ is a splitting field for P over $\mathbb{Q}(S_1, \ldots, S_n) = \mathbb{Q}(\boldsymbol{S})$, so it is a Galois extension. We can look at the Galois group $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{X})/\mathbb{Q}(\boldsymbol{S}))$ as a subgroup of $\mathfrak{S}_n$, permuting the roots of P. Since all elements of $\mathbb{Q}(\boldsymbol{S})$ stays invariant under all permutation in $\mathfrak{S}_n$, we have that $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{X})/\mathbb{Q}(\boldsymbol{S}))$ is in fact equal to $\mathfrak{S}_n$. □

6. Numbering of Roots

Galois Theory is named after the French mathematician Évariste Galois (1811–1832) who did groundbreaking work in this topic. However, the approach described in the previous section was not the one originally used by Galois. Instead it was developed through the study of permutations of the roots of a polynomial. We will use this approach to reach some initial connections between Hilbert's Irreducibility Theorem and Galois Theory.

Definition 6.1.
Let $P \in K[X]$ be a separable polynomial of degree n, and let L be a splitting extension of K. Denote by $R \subset L$ the set of roots of P. A ***numbering*** *of R is a bijection $\nu : \{1, \dots, n\} \to R$.*

Proposition 6.2.
Let P, K, L, R and ν be as in Definition 6.1. Furthermore let $\lambda_\nu : Gal(L/K) \to \mathfrak{S}_n$ be a mapping defined by ν, such that $\nu(\lambda_\nu(g)(i)) = g(\nu(i))$ for all $g \in Gal(L/K)$, $i \in \{1, \dots, n\}$. Then, λ_ν is an injective group homomorphism. In particular, for any $g \in Gal(L/K)$ its image $\lambda_\nu(g)$ permutes the elements of R.

Proof. Since $g \in \mathrm{Gal}(L/K)$ is a field automorphism, $g(0) = 0$. Furthermore, g acts on P coefficient-wise. So if $r \in R$, then $g(P(r)) = P(g(r)) = 0$, and $g(r) \in R$. An automorphism is bijective, so in particular the restriction of g to R is injective, and since R is finite it is in fact a bijection. Hence, $\nu^{-1} \circ g \circ \nu$ is a composition of bijections on R, so it is itself a bijection on R. In other words, it is a permutation of R. So , since $\lambda_\nu(g)(i) = \nu^{-1}(g(\nu(i)))$, $\lambda_\nu(g)$ is that same permutation of R and $\lambda_\nu(g) \in \mathfrak{S}_n$. For $g, g' \in \mathrm{Gal}(L/K)$ we get

$$\begin{aligned}\lambda_\nu(gg')(i) &= \nu^{-1} \circ g \circ g' \circ \nu(i) = \nu^{-1} \circ g \circ g' \circ \nu(i) = \\ &= \nu^{-1} \circ g \circ \nu \circ \nu^{-1} \circ g' \circ \nu(i) = \lambda_\nu(g) \circ \lambda_\nu(g')(i),\end{aligned}$$

so λ_ν is a group homomorphism. Now, to see that λ_ν is injective suppose $\lambda_\nu(g) = \lambda_\nu(g')$. Then for all $i \in \{1, \dots, n\}$ we have that

$$\nu^{-1} \circ g \circ \nu(i) = \nu^{-1} \circ g' \circ \nu(i) \Leftrightarrow g(i) = g'(i)$$

and so λ_ν is injective. □

This proposition lets us look at a Galois group as a subgroup of $\mathfrak{S}_n$. It is clear that it as such depends on the numbering of the roots. For now, we will just make use of the fact that the Galois group can be regarded as a permutation group. In the next section however, we will make use of the differences depending of numberings more explicitly.

Throughout the rest of this section, let P be a polynomial over a field K and let Ω be an algebraic closure of K. Furthermore, let L be the splitting extension of K generated by the roots $x_1, \dots, x_n$ of P in Ω and let $G = \mathrm{Gal}(L/K)$ be the Galois group of this splitting extension. When possible, we will denote variables $Y_1, \dots, Y_n$ with $\boldsymbol{Y}$.

Lemma 6.3.
For any $\sigma \in \mathfrak{S}_n$, let $\xi_\sigma = x_1 Y_{\sigma(1)} + \cdots + x_n Y_{\sigma(n)} \in L[\boldsymbol{Y}]$. Then the following holds:

(1) *For any element $\tau \in G$, $\tau(\xi_\sigma) = \xi_{\sigma\tau^{-1}}$*

(2) *The extension $K(\boldsymbol{Y}) \subset L(\boldsymbol{Y})$ is Galois, with Galois group G.*

(3) *The polynomial $\xi = \xi_{id} = x_1 Y_1 + \cdots + x_n Y_n$ is a primitive element.*

Proof. a) We define the action of G on $L[\boldsymbol{Y}]$ by letting elements of G act on the coefficients of a polynomial in $L[\boldsymbol{Y}]$. In particular, by Proposition 6.2 it acts on the x_i by permuting i. Hence, for any $\tau \in G$, we get

$$\tau(\xi_\sigma) = \sum_{i=1}^{n} \tau(x_i) Y_{\sigma(i)} = \sum_{i=1}^{n} x_{\tau(i)} Y_{\sigma(i)}.$$

By letting $j = \tau(i)$, we get that $\sigma(i) = \sigma(\tau^{-1}(j))$ and so

$$\sum_{i=1}^{n} x_{\tau(i)} Y_{\sigma(i)} = \sum_{j=1}^{n} x_j Y_{\sigma(\tau^{-1}(j))} = \xi_{\sigma\tau^{-1}},$$

and a) is proved.

b) Let $R = P/Q \in L(Y)$. Like in a), we define an action of G on $L(\boldsymbol{Y})$ by letting G act on the coefficients of P and Q respectively. Denote by $\mathrm{id} \in G$ the identity mapping of L. Then we have

$$R = \frac{P}{Q} \prod_{\tau \in G \setminus \{\mathrm{id}\}} \frac{\tau(Q)}{\tau(Q)} = \frac{P \prod_{\tau \neq \mathrm{id}} \tau(Q)}{\prod_{\tau} \tau(Q)}.$$

The denominator D of this expression is invariant under G, since $\tau'\left(\prod_{\tau} \tau(Q)\right) = \prod_{\tau} \tau(Q)$ for any $\tau' \in G$. Therefore the denominator belongs to $K[\boldsymbol{Y}]$. Now, let $N = RD$ be the numerator of the fraction. Since D is invariant under G, R is invariant under G if and only if N is. Since $N \in L[\boldsymbol{Y}]$, it is invariant under G if and only if it belongs to $K[X]$. From this we can conclude that $L(\boldsymbol{Y})^G = K(\boldsymbol{Y})$, and so b) follows directly from Artin's lemma.

c) Since $K(\boldsymbol{Y}, \xi)$ is the smallest field that contains $K(\boldsymbol{L})$ and ξ, we have that $K(\boldsymbol{L}) \subset K(\boldsymbol{L}, \xi) \subset L(\boldsymbol{Y})$. Furthermore, by a), we have that $\tau(\xi_{\mathrm{id}}) = \xi_{\tau^{-1}}$. Therefore, $\tau = \mathrm{id}$ is the only element of G such that $\tau(\xi) = \tau$. By Galois correspondance, we can now conclude that the extension $K(\boldsymbol{Y}, \xi) \subset L(\boldsymbol{Y})$ is Galois with the Galois group

$$\mathrm{Gal}(L(\boldsymbol{Y})/K(\boldsymbol{Y}, \xi)) = \{\tau \in G \mid \forall x \in K(\boldsymbol{Y}, \xi) : \tau(x) = x\} = \{\mathrm{id} \in G\}.$$

Therefore, $K(\boldsymbol{Y}, \xi) = L(\boldsymbol{Y})$ and ξ is a primitive element. □ □

Corollary 6.3.1.
The polynomial

$$M_\xi(T) = \prod_{\tau \in G} (T - \tau(\xi))$$

is the minimal polynomial of ξ over $K(\boldsymbol{Y})$.

Proof. By the previous lemma, we have that

$$\prod_{\tau\in G}(T-\tau(\xi))=\prod_{\tau\in G}(T-\xi_\tau),$$

so ξ is a root of M_ξ. Since all its roots are on the for ξ Since it is invariant under G, its coefficients belong to $K(\boldsymbol{Y})$. Furthermore, it is irreducible in $K(\boldsymbol{Y})[T]$ since G acts transitively on its roots and by construction it is monic, so it is minimal. □

We will now define another polynomial in $L(\boldsymbol{Y})[T]$:

$$\mathscr{R}_P(T)=\prod_{\sigma\in\mathfrak{S}_n}(T-\xi_\sigma)=\prod_{\sigma\in\mathfrak{S}_n}(T-(x_1Y_{\sigma(1)}+\cdots+x_nY_{\sigma(n)}))$$

It turns out that this polynomial gives us a tool to explicitly compute the Galois group $\mathrm{Gal}(L/K)$. However, to do this we need to know the roots of P, and the computations will be very impractical (and even impossible for large Galois groups). Instead we will use this result theoretically further on.

Proposition 6.4.
The polynomial $\mathscr{R}_P(T)$ is separable with coefficients in K.

Proof. The coefficients of $\mathscr{R}_P(T)$ is determined by the roots ξ_σ. By letting $\tau\in G$ act on ξ_σ, we get $\tau(\xi_\sigma)=\xi_{\sigma\tau^{-1}}$ (by the previous lemma). Since $\sigma\tau^{-1}\in\mathfrak{S}_n$, $\mathscr{R}_P(T)$ in invariant under all elements of G, and so the coefficients of $\mathscr{R}_P(T)$ belongs to K. That it is separable follows from the assumption that P is separable, hence all $x_1,\dots,x_n$ are unique and so all ξ_σ are unique. □

From this proposition and the fact that $K(\boldsymbol{Y})[T]$ is an integral domain, we can conclude that there is a unique factorization of $\mathscr{R}_P(T)$ in $K(\boldsymbol{Y})[T]$. Since $\mathscr{R}_P(T)$ might actually already be split in $K[T]$, this factorization could be the same as in $K[T]$, as we will see in Example 6.6. In the general case however, we will consider a factorization $\mathscr{R}_P(T)=M(T)Q(T)\in K(\boldsymbol{Y})[T]$. Since $T-\xi$ is a root of $\mathscr{R}_P(T)$ in $L(\boldsymbol{Y})[T]$, we can assume that M is divisible by $T-\xi$ in $L(\boldsymbol{Y})[T]$. Furthermore, if M is irreducible, we get that it is unique up to units, since $K(\boldsymbol{Y})[T]$ is a unique factorization domain. Finally, if M is monic, it is a unique. Thus letting M be the unique monic irreducible factor of $\mathscr{R}_P(T)$ divisible by $T-\xi$ is well defined, which leads us to the following theorem.

Theorem 6.5.
Let $M\in K(\boldsymbol{Y})[T]$ be the factor of $\mathscr{R}_P(T)$ as defined above. Then $M=M_\xi$ and furthermore, $\sigma\in\mathfrak{S}_n$ belongs to G if and only if

$$M(Y_1,\dots,Y_n,T)=M(Y_{\sigma(1)},\dots,Y_{\sigma(n)},T)$$

Proof. Since M and M_ξ have $T-\xi$ as a common factor in $L(\boldsymbol{Y})[T]$ they have nontrivial g.c.d. in $L(\boldsymbol{Y})[T]$. Then, by Proposition 5.4 this is also their g.c.d. in $K(\boldsymbol{Y})[T]$. But as they are both irreducible and monic in $K(\boldsymbol{Y})[T]$, they must be equal. Therefore, we have that

$$M(Y_1,\dots,Y_n,T)=\prod_{\tau\in G}(T-(x_1Y_{\tau(1)}+\cdots+x_nY_{\tau(n)}))$$

and for $\sigma \in \mathfrak{S}_n$ we get

$$M(Y_{\sigma(1)}, \dots, Y_{\sigma(n)}, T) = \prod_{\tau \in G} (T - (x_1 Y_{\tau(\sigma(1))} + \cdots + x_n Y_{\tau(\sigma(n))})) = \\ = \prod_{\tau \in G\sigma} (T - (x_1 Y_{\tau(1)} + \cdots + x_n Y_{\tau(n)})).$$

We see that the last part of this expression is equal to $M(Y_1, \dots, Y_n, T)$ if and only if $G\sigma = G$, which is the same as saying that $\sigma \in G$. □

Example 6.6.
To see how inconvenient this theorem is for actually computing Galois groups, consider the polynomial $P = x^2 + 1$ over $\mathbb{R}$. In the algebraic closure $\mathbb{C}$ of $\mathbb{R}$, P has the roots i and $-i$. So we get that

$$\begin{aligned}\mathscr{R}_P(T) = &\prod_{\sigma \in \mathfrak{S}_2} (T - (x_1 Y_{\sigma(1)} + x_2 Y_{\sigma(2)}) = \\ =&(T - (iY_1 - iY_2))(T - (iY_2 - iY_1)) = \\ =&(T + i(Y_2 - Y_1)(T - i(Y_2 - Y_1)) = \\ =&T^2 + (Y_2 - Y_1)^2.\end{aligned}$$

This polynomial is irreducible in $\mathbb{R}(\boldsymbol{Y})[T]$, and so $M = \mathscr{R}_P$ and $M(Y_1, Y_2, T) = M(Y_{\sigma(1)}, Y_{\sigma(2)}, T)$ for all $\sigma \in \mathfrak{S}_2$. Therefore the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathfrak{S}_2$. This example is doable, even though there are easier ways of determining this Galois group. However, we can see that for polynomials P of higher degree, the degree of $\mathscr{R}_P$ will be too big to handle.

Note that the definition of $\xi_{\mathrm{id}} = x_1 Y_1 + \cdots + x_n Y_n$ is dependant on the numbering of the roots of P. More explicitly, we can let $\xi_{\nu,\sigma} = \nu(1) Y_{\sigma(1)} + \cdots + \nu(n) Y_{\sigma(1)}$ for some numbering ν. Now recall the mapping λ_ν from Proposition 6.2. Denote by G_ν its image $\lambda_\nu(G) = \{\sigma \in \mathfrak{S}_n \mid \exists g \in G : \lambda_\nu(g) = \sigma\}$. Then we can write the minimal polynomial of ξ_ν as

$$\begin{aligned}\mathscr{R}_{P,\nu}(T) &= \prod_{\tau \in G} (T - (\tau(\nu(1))Y_1 + \cdots + \tau(\nu(n))Y_n)) \\ &= \prod_{\sigma \in G_\nu} (T - (\nu(\sigma(1))Y_1 + \cdots + \nu(\sigma(n))Y_n)) .\end{aligned}$$

The notation $\mathscr{R}_{P,\nu}$ is motivated by the following proposition.

Proposition 6.7. *Let ν be a numbering of the roots of P and let C be a set containing one representative from each left coset of G_ν. Then we have that*

$$\mathscr{R}_P = \prod_{\tau \in C} \mathscr{R}_{P,\nu\circ\tau}$$

Proof. The polynomial $\mathscr{R}_P$ is independent of the numbering ν, since $\mathscr{R}_P$ might as well be defined by permutations of the roots $x_1, \dots, x_n$ as of the variables $Y_1, \dots, Y_n$. More specifically, with $\mathscr{N}$ being the set of all numberings of the roots of P, we can write

$$\mathscr{R}_P(T) = \prod_{\mu \in \mathscr{N}} (T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n))$$

If ν is a specific numbering, we have that every numbering in $\mathscr{N}$ can be described as $\nu \circ \delta$ for some $\delta \in \mathfrak{S}_n$. Since G_ν is a subgroup of $\mathfrak{S}_n$, the left cosets of G_ν form a partition of $\mathfrak{S}_n$. Hence, every permutation in $\mathfrak{S}_n$ is uniquely defined by $\tau \circ \sigma$ for some $\tau \in C$ and some $\sigma \in G_\nu$. This gives us

$$\begin{aligned}\prod_{\tau \in C} \mathscr{R}_{P,\nu\circ\tau} &= \prod_{\tau \in C} \prod_{\sigma \in G_\nu} (T - (\nu(\tau \circ \sigma(1))Y_1 + \cdots + \nu(\tau \circ \sigma(n))Y_n)) = \\ &= \prod_{\mu \in \mathscr{N}} (T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n)) = \mathscr{R}_P\end{aligned}$$

which proves the proposition. □

7. Specialization of Polynoials and Galois Groups

Now we will look at special mappings of a field, and in particular those mappings applied on polynomials over a field. We will define it in general terms, but for this text we will mostly be interested in one particular such mapping, namely the evaluation mapping of the coefficients of a polynomial over a field of rational functions.

Definition 7.1.
*Let K and k be fields and let $\varphi : K \to k \cup \{\infty\}$ be a mapping such that $\varphi(1) = 1$. Then φ is a **place** of K if it satisfies the following properties:*

1. *if $\varphi(x)$ and $\varphi(y)$ are not both ∞, then $\varphi(x+y) = \varphi(x)+\varphi(y)$, with $a+\infty = \infty$ for all $a \in k$;*
2. *if $\{\varphi(x), \varphi(y)\} \neq \{0, \infty\}$, then $\varphi(xy) = \varphi(x)\varphi(y)$, with $a\infty = \infty$ for nonzero $a \in k \cup \{\infty\}$.*

In the case of applying a place to a polynomial, we call this a **specialization** of that polynomial. A specialization that will be of particular interest for us comes from the following, rather obvious but still important proposition.

Proposition 7.2.
Let $K(T)$ be the field of rational functions over a field K and let $P \in K(T)$ be a rational function. Furthermore, let t be an element in K such that $P(t) \in K$ or t is a pole of P. Then the map

$$\varphi_t : K(T)[X] \to K[X] \cup \infty \ ;$$
$$\begin{cases} P \mapsto P(t, X) & \text{if } t \text{ is not a pole of } P \\ P \mapsto \infty & \text{if } t \text{ is a pole of } P \end{cases}$$

is a place of $K(T)$.

Proof. Let P and Q be rational functions in $K(T)$ and suppose $\varphi_t(P)$ and $\varphi_t(Q)$ are not both ∞. Then t is not a pole of both P and Q. If t is not a pole of neither P nor Q, then $(P + Q)(t) = P(t) + Q(t)$. Assume now that $\varphi_t(P) = \infty$ and $\varphi_t(Q) \neq \infty$. We can write $P(T) = \frac{R_1(T)}{D_1(T)(T-t)}$ for some $R_1, D_1 \in K[T]$ with

$T - t$ not being a factor of R_1. Since $\varphi_t(Q) \neq \infty$, t is not a pole of Q. So with $Q(T) = \frac{R_2(T)}{D_2(T)}$ we have that $T - t$ is not a factor of D_2. Then we can write

$$P + Q = \frac{R_1(T)}{D_1(T)(T-t)} + \frac{R_2(T)}{D_2(T)} = \frac{R_1(T)D_2(T)}{D_1(T)(T-t)} + \frac{R_2(T)D_1(T)}{D_2(T)}$$

and since $T - t$ doesn't factor neither R_1 nor D_2 we have that $(P+Q)(t) = \infty$. So, in both cases we have

$$\varphi_t(P + Q) = \varphi_t(P) + \varphi_t(Q),$$

which varifies (1) in the definition of a place.

Now let $\{\varphi_t(P), \varphi_t(Q)\} \neq \{0, \infty\}$. Suppose t is a pole of one of the functions, P say. Then $P(T) = \frac{R_1(T)}{D_1(T)(T-t)}$ as above. We also have that $Q(t) \neq 0$, so $T - t$ is not a factor of Q. But then the factor $1/(T - t)$ cannot be canceled in PQ, and so t is a pole of PQ and $\varphi_t(PQ) = \infty = \varphi_t(P)\varphi_t(Q)$. And as above, if t is not a pole of neither P nor Q, then $(PQ)(t) = P(t)Q(t)$. So

$$\varphi_t(PQ) = \varphi_t(P)\varphi_t(Q)$$

holds in both cases, which varifies (2) in the definition of a place. The condition $\varphi_t(1) = 1$ is trivial, so φ_t is a place. □

Definition 7.3.
If $\varphi : K \to k \cup \{\infty\}$ is a place, then the set

$$\varphi^{-1}(k) = \{x \in K : \varphi(x) \neq \infty\}$$

*is called the **valuation ring** of φ.*

Proposition 7.4.
Let A be a valuation ring of a place $\varphi : K \to k \cup \{\infty\}$. Then A is an integrally closed subring of K.

Proof. First we show that A is a subring. We already know that $1 \in A$, so A is not empty. If $x, y \in A$ we have that $\varphi(x + y) = \varphi(x) + \varphi(y) \in k$. So A is closed under addition. Similarly, $\varphi(xy) = \varphi(x)\varphi(y) \in k$ so A is also closed under multiplication.

If $\varphi(x) \neq \infty$, then $\varphi(x + 0) = \varphi(x) + \varphi(0) \neq \infty$. So $\varphi(0) \neq \infty$ and $0 \in A$. For all $x \in A$, we have that $\varphi(0) = \varphi(x - x) = \varphi(x) + \varphi(-x)$. Since $\varphi(x) \neq \infty$ and $\varphi(0) \neq \infty$ we have that $\varphi(-x) \neq \infty$ and $-x \in A$.

That A is integrally closed is to say that for any x in an algebraic closure Ω of K, the statement that there exists a monic polynomial $P \in A[X]$ such that $P(x) = 0$ is equivalent to saying that $x \in A$. If $x \in A$ the implication is trivial, since $P = X - x \in A[X]$. For the other direction, we will actually show an even stronger result. Our claim is that if there is a monic polynomial $P \in A[X]$ such that $P(x) \in A$, then $x \in A$. Since $0 \in A$, proving this claim finishes the whole proof. We will do this by induction on the degree $n \geq 1$ of P. If $\deg(P) = 1$, then $P = X - a_0$ for some $a_0 \in A$. If $P(x) \in A$, then $\varphi(P(x)) = \varphi(x + a_0) = \varphi(x) + \varphi(a_0) \neq \infty$. So $\varphi(x) \neq \infty$ and $x \in A$. This shows the claim holds for the base case $n = 1$. The induction hypothesis is now that the claim holds for polynomials of degree less than

n. Let $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ be a monic polynomial in $A[X]$ of degree n such that $P(x) \in A$. Then,

$$\varphi(P(x)) = \varphi(x^n + a_{n-1}x^{n-1} + \cdots + a_1x) + \varphi(a_0) \neq \infty.$$

Since $\varphi(a_0) \neq \infty$, we have that

$$\varphi(x^n + a_{n-1}x^{n-1} + \cdots + a_1x) = \varphi(x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)) \neq \infty.$$

Assume now that $\varphi(x) = \infty$. Then by the last inequality,

$$\varphi(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = 0.$$

But this means that $x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 \in A$, so letting $Q = X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_1$ we have that Q is a monic polynomial in $A[X]$ of degree $n-1$ for which $Q(x) \in A$. By the induction hypothesis $x \in A$, which contradicts the assumption that $\varphi(x) = \infty$, so x is in fact in A. This shows that the claim holds for P, and so A is integrally closed. □

Lemma 7.5 (Gauss' lemma for valuation rings)**.**
Let A be a valuation ring of a place $\varphi : K \to k \cup \{\infty\}$ and let P and Q be two monic polynomials in $K[X]$. If $P \in A[X]$ and Q divides P in $K[X]$, then $Q \in A[X]$

Proof. If $\deg(Q) = \deg(P)$, then $Q = P$ and the statement is trivial. Assume that $\deg(Q) < \deg(P)$.

Since A is integrally closed, all roots $x_1, \ldots, x_n$ of P are in A. We can write

$$P = \prod_{i=1}^{n}(X - x_i),$$

and since Q divides P, we have that

$$Q = \prod_{I}(X - x_i)$$

for some $I \subset \{1, \ldots, n\}$. The coefficients of Q are therefore products of elements in A, so $Q \in A[X]$. □

For the rest of this section, let $\varphi : K \to k \cup \{\infty\}$ be a place with valuation ring A. Let $P \in A[X]$ be a monic polynomial of degree n such that $\varphi(P) \in k[X]$ is separable (as a consequence of Lemma 5.12 P is then also separable). Let L be a splitting extension of P over K and ℓ be a splitting extension of $\varphi(P)$ over k, with Galois groups $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(\ell/k)$.

Lemma 7.6.
The polynomial $\mathscr{R}_P$ belongs to $A[T, \boldsymbol{Y}]$, and $\mathscr{R}_{\varphi(P)} = \varphi(\mathscr{R}_P)$.

Proof. Consider the polynomial

$$R = \prod_{\sigma \in \mathfrak{S}_n} (T - (\sum_{i=1}^{n} X_{\sigma(i)}Y_i)).$$

It is symmetric in $X_1, \ldots, X_n$, and by writing

$$R = \sum_{I=(i_0,\ldots,i_n)} R_I(\boldsymbol{X})T^{i_0}Y_1^{i_1}\cdots Y_n^{i_n},$$

with $\sum_{j=0}^{n} i_j = n$, we can regard it as a polynomial in $T, \boldsymbol{Y}$. Since its coefficients $R_I(\boldsymbol{X}) \in \mathbb{Z}[\boldsymbol{X}]$ only depend on $X_1, \ldots, X_n$, we get that $R_I(\boldsymbol{X})$ is also symmetric. By Fundamental Theorem of Symmetric Polynomials, there is a polynomial $\tilde{R}_I \in \mathbb{Z}[S_1, \ldots, S_n]$ for every I, such that $R(\boldsymbol{X}) = \tilde{R}(S_1(\boldsymbol{X}), \ldots, S_n(\boldsymbol{X}))$. With $P = X^n + a_1 X^{n-1} + \cdots + a_n$ and $x_1, \ldots, x_n$ being the roots of P in L, we get by Vieta's Formulas that

$$a_j = (-1)^j S_j(x_1, \ldots, x_n).$$

Since

$$\mathscr{R}_P = \sum_{I=(i_0,\ldots,i_n)} R_I(x_1, \ldots, x_n) T^{i_0} Y_1^{i_1} \cdots Y_n^{i_n},$$

we get that

$$\begin{aligned} \mathscr{R}_P &= \sum_{I=(i_0,\ldots,i_n)} \tilde{R}_I(S_1(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n)) T^{i_0} Y_1^{i_1} \cdots Y_n^{i_n} = \\ &= \sum_{I=(i_0,\ldots,i_n)} \tilde{R}_I(-a_1, \ldots, (-1)^n a_n) T^{i_0} Y_1^{i_1} \cdots Y_n^{i_n}. \end{aligned} \tag{1}$$

Then, since the coefficients a_j of P belongs to A, $\mathscr{R}_P \in A[T, \boldsymbol{Y}]$.

Letting φ act on the coefficients of P, we get

$$\varphi(P) = X^n + \varphi(a_1) X^{n-1} + \cdots + \varphi(a_n).$$

It is a polynomial of degree n with coefficients $\varphi(a_j)$. By assumption, it is also separable with roots $\tilde{x}_1, \ldots, \tilde{x}_n$ in ℓ. Relation (1) we can write

$$\mathscr{R}_{\varphi(P)} = \sum_{I=(i_0,\ldots,i_n)} \tilde{R}_I(-\varphi(a_1), \ldots, (-1)^n \varphi(a_n)) T^{i_0} Y_1^{i_1} \cdots Y_n^{i_n}.$$

Furthermore, since $\tilde{R}_I \in \mathbb{Z}[\boldsymbol{S}]$, we have that $\tilde{R}_I(-a_1, \ldots, (-1)^n a_n)$ can be written only with addition and multiplication of powers of the elements $a_1, \ldots, a_n$ (i.e. without coefficients). By the definition of a place, this means that

$$\varphi(\tilde{R}_I(-a_1, \ldots, (-1)^n a_n) = \tilde{R}_I(-\varphi(a_1), \ldots, (-1)^n \varphi(a_n)).$$

This gives us

$$\begin{aligned} \varphi(\mathscr{R}_P) &= \sum_{I=(i_0,\ldots,i_n)} \varphi(\tilde{R}_I(-a_1, \ldots, (-1)^n a_n)) T^{i_0} Y_1^{i_1} \cdots Y_n^{i_n} = \\ &= \sum_{I=(i_0,\ldots,i_n)} \tilde{R}_I(-\varphi(a_1), \ldots, (-1)^n \varphi(a_n)) T^{i_0} Y_1^{i_1} \cdots Y_n^{i_n} = \mathscr{R}_{\varphi(P)}, \end{aligned}$$

and the lemma is proved. □

Lemma 7.7.
Let ν be a numbering of the roots of P in L. Then, the polynomial $\mathscr{R}_{P,\nu}$ belongs to $A[T, \boldsymbol{Y}]$.

Proof. First, we note that we in fact have extended φ to be a map from $K[T, \boldsymbol{Y}]$ to $k[T, \boldsymbol{Y}] \cup \{\infty\}$ by letting φ act on coefficients of polynomials. As such, $A[\boldsymbol{Y}]$ is the valuation ring of φ. Since $\mathscr{R}_{P,\nu}$ divides $\mathscr{R}_P$ and since $\mathscr{R}_P \in A[T, \boldsymbol{Y}]$, we have by Lemma 7.5 that $\mathscr{R}_{P,\nu} \in A[T, \boldsymbol{Y}]$ □

Definition 7.8.
A numbering ν of the roots of P and a numbering μ of the roots of $\varphi(P)$ are said to be ***compatible*** *if $\mathscr{R}_{\varphi(P),\mu}$ divides $\mathscr{R}_{\varphi(P),\nu}$.*

Theorem 7.9. *Let ν be a numbering of the roots of P, and let $\lambda_\nu : Gal(L/K) \to \mathfrak{S}_n$ be its corresponding embedding with image G_ν. Then, there exists a numbering μ of the roots of $\varphi(P)$ which is compatible with ν. The image H_μ of its corresponding embedding $\lambda_\mu : H \to \mathfrak{S}_n$ is a subgroup of G_ν.*

Proof. By Proposition 6.7 we can write $\mathscr{R}_P = \mathscr{R}_{P,\nu}Q$ for some polynomial Q. By applying φ to both sides we get $\varphi(\mathscr{R}_P) = \varphi(\mathscr{R}_{P,\nu}Q)$ and by the previous lemmas we can write $\mathscr{R}_{\varphi(P)} = \varphi(\mathscr{R}_{P,\nu})\,\varphi(Q)$, with $\varphi(Q) \in A[T, \boldsymbol{Y}]$. Hence, irreducible factors of $\mathscr{R}_{P,\nu}$ divide $\mathscr{R}_{\varphi(P)}$. Again by Proposition 6.7, this means that they are on the form $\mathscr{R}_{\varphi(P),\mu}$ for some numberings μ of the roots of $\varphi(P)$ in ℓ. By construction, this means that they the numberings compatible with ν. Let N be the set of these numberings and we get

$$\varphi(\mathscr{R}_{P,\nu}) = \prod_{\mu\in N}(T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n)).$$

If $\sigma \in G_\nu$, then

$$\mathscr{R}_{P,\nu}(T, Y_{\sigma(1)}, \ldots, Y_{\sigma(n)}) = \mathscr{R}_{P,\nu}(T, Y_1, \ldots, Y_n\}.$$

By applying φ to both sides we get

$$\prod_{\mu\in N}(T - (\mu(1)Y_{\sigma(1)} + \cdots + \mu(n)Y_{\sigma(n)})) = \prod_{\mu\in N}(T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n)).$$

Furthermore, since

$$\begin{aligned}
&\prod_{\mu\in N}(T - (\mu(1)Y_{\sigma(1)} + \cdots + \mu(n)Y_{\sigma(n)})) = \\
&= \prod_{\mu\in N}(T - (\mu(1)Y_{\sigma(1)} + \cdots + \mu(n)Y_{\sigma(n)})) = \\
&= \prod_{\mu\in N}(T - (\mu(\sigma^{-1}(1))Y_{\sigma(\sigma^{-1}(1))} + \cdots + \mu(n)Y_{\sigma(\sigma^{-1}(n))})) = \\
&= \prod_{\mu\in N\sigma^{-1}}(T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n)),
\end{aligned}$$

we get that $N = N\sigma^{-1}$. In other words, for every $\mu \in N$ and every $\sigma \in G_\nu$, there is a $\mu' \in N$ such that $\mu' = \mu\sigma$. But since $\mu\sigma$ is distinct for every $\sigma \in G_\nu$, there must be exactly $|N|$ elements in G_ν and $N = \mu G_\nu$ for any $\mu \in N$. For such a μ, the polynomial $\mathscr{R}_{\varphi(P),\mu}$ divides $\varphi(\mathscr{R}_{P,\nu})$, as concluded above. Therefore it must be on the form

$$\prod_{\mu\in N'}(T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n)),$$

with $N' \subset N$. On the other hand,

$$\begin{aligned}
\mathscr{R}_{\varphi(P),\mu} &= \prod_{\sigma\in H_\mu}(T - (\mu(\sigma(1))Y_1 + \cdots + \mu(\sigma(n))Y_n)) = \\
&= \prod_{\tau\in\mu H_\mu}(T - (\tau(1)Y_1 + \cdots + \tau(n)Y_n)),
\end{aligned}$$

so $\mu H_\mu \subset N = \mu G_\nu$, which implies that $H_\mu \subset G_\nu$. □ □

8. Some Basic Results Regarding the Inverse Galois Problem

As we saw in Theorem 7.9, a Galois group over $\mathbb{Q}$ of a specialized polynomial $\varphi(P)$ can be regarded as a subgroup of the Galois group over $\mathbb{Q}(T)$ of the polynomial P. This approach to use Galois groups of some Galois extension of $\mathbb{Q}(T)$ to say something about what we might call the specialized Galois group can be taken a few steps further. The reason we are interested in this method is because we want to find out which groups that appear as Galois groups of some Galois extension $K/\mathbb{Q}$. This problem is called the Inverse Galois Problem, and it is still unsolved. However, Hilbert's Irreducibility Theorem can reduce the problem to finding an extension over $\mathbb{Q}(T_1, \dots, T_n)$ for which a group G is the Galois group. We start by proving an immediate consequence from the irreducibility theorem, which we will then generalize.

Theorem 8.1.
Let $P \in \mathbb{Q}(T)[X]$ be a monic polynomial. Let K be a splitting extension of P over $\mathbb{Q}(T)$, with $G = Gal(K/\mathbb{Q}(T))$. Denote by $N(B)$ the number of integers $t \in [0, B]$ such that t is either a pole of $P(T, X)$ or the Galois group of $P(t, X)$ over $\mathbb{Q}$ is not isomorphic to G. Then there is a real number $\alpha < 1$ such that $N(B) = O(B^\alpha)$.

Proof. Like in Theorem 3.4, we can assume that $P \in \mathbb{Z}[T, X]$. Let n be the degree of P as a polynomial in X and let γ be a primitive element for K with minimal polynomial $Q \in \mathbb{Q}(T)[X]$. Denote by N the degree of Q, so that $N = [K : \mathbb{Q}(T)]$. Let $D \in \mathbb{Q}(T)$ be a common denominator of the coefficients of Q. Since $\mathbb{Q}(T)(\gamma) = \mathbb{Q}(T)(\gamma D)$, γD is a primitive element and its minimal polynomial has degree N. The polynomial $Q(T, D(T)^{-1}X)$ is indeed an irreducible polynomial with γD as a root. However, its leading coefficient is $D(T)^{-N}$ so to get a monic polynomial we multiply by $D(T)^N$ and get $D(T)^N Q(T, D(T)^{-1}X)$ as the minimal polynomial of γD. This polynomial is in $\mathbb{Q}[T, X]$, as the factor $D(T)^N$ cancels out all denominators in $Q(T, D(T)^{-1}X)$. Since γ was chosen arbitrarily, we can assume that $Q \in \mathbb{Q}[T, X]$. From Proposition 5.19 we know that Q also is split in K. So by the next lemma, there is a finite subset $\Sigma \subset \mathbb{Q}$ such that for any $t \notin \Sigma$, the polynomials $Q(t, X)$ and $P(t, X)$ are separable and have a common splitting extension over $\mathbb{Q}$. Call this splitting extension K_t. From Proposition 7.2, we know that the valuation mapping $P(T, X) \mapsto P(t, X)$ is a place so by Theorem 7.9, the Galois group $\mathrm{Gal}(K_t/\mathbb{Q}) = H$ can be considered as a subgroup of G. This gives us

$$[K_t : \mathbb{Q}] \leq [K : \mathbb{Q}(T)] = N.$$

Now, for $t \in [0, B]$ such that $t \notin \Sigma$ and $Q(t, X)$ is irreducible in $\mathbb{Q}[X]$, we have that $Q(t, X)$ has N distinct roots not in $\mathbb{Q}$. For all such t we get that $[K_t : \mathbb{Q}] \geq N$, and so H is isomorphic to G. By Theorem 3.4, there exists an $\alpha < 1$ such that the number $\tilde{N}(B)$ of integers $t \in [0, B]$ such that $Q(t, X)$ is reducible in $\mathbb{Q}[X]$ satisfies $\tilde{N}(B) = O(B^\alpha)$ (note that t is not a pole of Q as it belongs to $\mathbb{Q}[T, X]$). Since Σ is finite, the number of $t \in \Sigma$ is obviously bounded. If $N(B)$ is the number of $t \in [0, B]$ for which G not isomorphic to H we have that $N(B) \leq \tilde{N}(B) + |\Sigma|$ and

$$N(B)/B^\alpha \leq \tilde{N}(B)/B^\alpha + |\Sigma|/B^\alpha$$

which remains bounded as $B \to \infty$. □

Lemma 8.2.
Let $P \in \mathbb{Q}(T)[X]$ be a monic irreducible polynomial and let $\mathbb{Q}(T) \subset K$ be a splitting extension of P. Let $y \in K$ be a primitive element with minimal polynomial $Q \in \mathbb{Q}(T)[X]$. Then, there exists a finite subset $\Sigma \subset \mathbb{Q}$ such that for any $t \notin \Sigma$, the polynomials $Q(t, X)$ and $P(t, X)$ are separable and have a common splitting extension.

Proof. Let $x_1, \dots, x_n$ be the roots of P in K. Take polynomials $A_i \in \mathbb{Q}(T)[Y]$ such that $x_i = A_i(y)$, for any $i \in \{1, \dots, n\}$. These polynomials are well defined since all elements of K can be written as linear combinations of powers of y. This lets us write

$$P(T, X) = \prod_{i=1}^{n} (X - A_i(T, y)).$$

Consider now the following polynomial with coefficients in $\mathbb{Q}(T)[Y]$:

$$P(T, X) - \prod_{i=1}^{n} (X - A_i(T, Y)).$$

All coefficients of this polynomial vanish at $Y = y$, and so Q must be a factor of these coefficients. Therefore, there is a polynomial $R \in \mathbb{Q}(T)[X, Y]$ such that

$$P(T, X) = \prod_{i=1}^{n} (X - A_i(T, Y)) + R(T, X, Y)Q(T, Y). \tag{1}$$

Now, let $B \in \mathbb{Q}(T)[X_1, \dots, X_n]$ be such that $B(T, x_1, \dots, x_n) = y$. This is well defined since K is generated by the roots of P. The polynomial

$$Y - B(T, A_1(Y), \dots, A_n(Y))$$

vanishes at y. So Q divides its terms and we get

$$Y = B(T, A_i(T, Y), \dots, A_n(T, Y)) + S(T, Y)Q(T, Y) \tag{2}$$

for some $S \in \mathbb{Q}(T)[Y]$. Since Q is split in K there are polynomials $C_i \in \mathbb{Q}(T)[Y]$ such that

$$Q(T, X) = \prod_{i=1}^{m} (X - C_i(T, y)).$$

As above, we use this to write

$$Q(T, X) = \prod_{i=1}^{m} (X - C_i(T, Y)) + U(T, X, Y)Q(T, Y) \tag{3}$$

for som $U \in \mathbb{Q}(T)[X, Y]$.

The coefficients of the polynomials $P, Q, A_1, \dots, A_n, B, C_1, \dots, C_m, R, S$ all belong to $\mathbb{Q}(T)$. Let Σ be the set of all $t \in \mathbb{Q}$ such that either t is a pole of one of these coefficients, or such that the discriminant of P or Q vanishes at t. Each coefficient has finitely many poles, and the discriminant is a single variable polynomial depending on t, so it has finitely many roots. Hence Σ is a finite set. For any $t \notin \Sigma$, the polynomials $P(t, X)$ and $Q(t, X)$ are separable, since their discriminant is nonzero. And since $t \notin \Sigma$ is not a pole of any of said coefficients, relation (1), (2) and (3) hold for $T = t$.

Now we only have to show that for any $t \in \mathbb{Q} \setminus \Sigma$, the polynomials $P(t, X)$ and $Q(t, X)$ are split in exactly the same extensions. Let L be an extension of $\mathbb{Q}$ in

which $Q(t, X)$ has a root α. For any $i \in \{1, \ldots, n\}$, let $\xi_i = A_i(t, \alpha)$. From relation (1) we have that

$$P(t, X) = \prod_{i=1}^{n} (X - \xi_i),$$

so P is split in L.

Conversely, let L be an extension of $\mathbb{Q}$ in which $P(t, X)$ is split with roots $\xi_1, \ldots, \xi_n$. Let α be a root of $Q(t, X)$ in some extension L' of L. Again by (1), we have that the roots of P in L' the $A_i(t, \alpha)$ for $1 \leq i \leq n$. Hence, there is a permutation $\sigma \in \mathfrak{S}_n$ such that $A_i(t, \alpha) = \xi_{\sigma(i)}$ for all i. From relation (2) we then have that

$$\alpha = B(t, \xi_{\sigma(1)}, \ldots, \xi_{\sigma(n)}) \in \mathbb{Q}[\xi_1, \ldots, \xi_n].$$

So, $\alpha \in L$ and so we get from (3) that

$$Q(t, X) = \prod_{i=1}^{m} (X - C_i(t, \alpha))$$

and $Q(t, X)$ is split in L. □

The results from Theorem 8.1 are interesting in itself, as we see that any group G that is a Galois group of a finite extension over $\mathbb{Q}(T)$ can also be realized as a Galois group of a finite extension over $\mathbb{Q}$. However, we also want to say things about a group that is a Galois group of a finite extension of $\mathbb{Q}(T_1, \ldots, T_n)$. For this we need some more work. We will approach the problem more generally than just looking at $\mathbb{Q}$ and fields of rational functions over $\mathbb{Q}$. Instead we will consider any fields of characteristic zero and then apply our results to $\mathbb{Q}$. This general approach is justified by the fact that the results are applicable to many fields, even though we will actually only use it to extensions of $\mathbb{Q}$. As we now will be working with general fields, we will mostly reserve capital letter for fields (and rings) and write polynomials in small letters to avoid confusion.

First, we will basically go through the proof of Theorem 8.1 again in general terms. This will eventually allow us to apply the result on extensions of $\mathbb{Q}$. We begin with some basic algebra from which we will see that the assumption that the minimal polynomial in the previous theorem had coefficients in $\mathbb{Q}[T]$ was not a unique situation. It follows from the fact that the polynomial ring over a field forms an integral domain.

Proposition 8.3.
Let R be an integral domain with subring S. Furthermore, let $f, h \in S[X]$ and $g \in R[X]$ be polynomials such that $fg = h$. Then, if f is monic, $g \in S[X]$.

Proof. If f is monic, there are unique polynomials $q, r \in S[X]$ such that $h = fq + r$, with the degree of r being less than the degree of f. So,

$$fq + r = fg \Rightarrow r = f(g - q).$$

By assumption, R is an integral domain, so $R[X]$ is also an integral domain. Therefore, if $g - q \neq 0$ we can write

$$\begin{aligned} f(g - q) &= (a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n)(b_0 + b_1 X + \cdots + b_m X^m) = \\ &= c(X) + b_m X^{m+n}, \end{aligned}$$

with $c(x)$ being a polynomial with degree less than $m+n$. So, r has degree $m+n$. This is a contradiction, since $\deg(r) < \deg(f)$, so $g - q = 0$ and $g = q \in S[X]$. □

Proposition 8.4.
Let K be the field of fractions over one of its subrings R. Furthermore, let L/K be a Galois extension of degree n. Then, there is a primitive element α for L/K, such that its minimal polynomial f is in $R[X]$.

Proof. A Galois extension is separable so by the Primitive Element Theorem, there is an element $\beta \in L$ such that $L = K[\beta]$. Let m_β be the minimal polynomial of β. Since K is the field of fractions over R, we have that the coefficients of m_β are on the form $\frac{a_i}{b_i}$, with $a_i, b_i \in R$ and $b \neq 0$. Now, let d be the least common multiple of all b_i. Then we have that $dm_\beta \in R[X]$. Let $\alpha = d\beta$. Then $K[\alpha] = K[\beta]$, so α generates L. Since $[L : K] = n$, we have that $\deg(m_\beta) = n$. Now define

$$f(X) = X^n + d\frac{a_{n-1}}{b_{n-1}}X^{n-1} + \cdots + d\frac{a_0}{b_0},$$

with $\frac{a_i}{b_i}$ being the coefficients of m_β. Obviously, this polynomial is monic and has degree n. Furthermore, since $f(\alpha) = f(d\beta) = d^n m_\beta(\beta) = 0$, it has α as a root. Finally, since $[K[\alpha] : K] = [L : K] = n$ is the degree of the minimal polynomial of α, the polynomial f must be this minimal polynomial. □

Now we are ready to go to the actual result. We begin with a lemma that is the key result for generalizing Theorem 8.1. We will show that for a Galois group defined by a minimal polynomial over a field, it is possible to find a ring homomorphism such that the Galois group of the mapped polynomial stays the same under certain circumstances. As we have seen, the evaluation homomorphism is a place and this is what we will make use of to connect this result with the Irreducibility Theorem.

Lemma 8.5.
Let L, K, R, f and α be as in Proposition 8.4 and let G be the Galois group $Gal(L/K)$. Furthermore, let A be a finite subset of L such that A is closed under the automorphisms of G and such that $\alpha \in A$. Then, there exists an element $u \in R$ such that for any field K' and any ring homomorphism $\omega : R \to K'$ with $\omega(u) \neq 0$, we can extend ω to a ring homomorphism $\tilde{\omega} : R[A] \to L'/K'$, for being some Galois extensions L'/K' of K', with $\tilde{\omega}$ having the following properties:

(1) *$\tilde{\omega}(\alpha)$ is a generator for L'/K'.*

(2) *If the polynomial obtained by applying $\tilde{\omega}$ to the coefficients of f is irreducible, we have that $Gal(L'/K') = G'$ is isomorphic to G. Furthermore, for $\sigma \in G$ and its image $\sigma' \in G'$ under this isomorphism, we have that $\tilde{\omega}(\sigma'(s)) = \sigma'(\tilde{\omega}(s))$.*

Proof. Let $u = \Delta(f)$ be the discriminant of f. Since f is minimal, it is irreducible and as we are working in perfect fields, it is separable. Therefore, we have that $u \neq 0$. Consider any field K' and a ring homomorphism $\omega : R \to K'$ with $\omega(u) \neq 0$. With $r_1, \ldots, r_n$ being the roots we have that

$$\Delta(f') = \Delta(\omega(f)) = \omega(\Delta(f)) = \omega(u) \neq 0,$$

so f' is separable. From Proposition 8.4, we know that $L = K[\alpha]$. So for every $s \in A \subset L$, there is a polynomial $g_s \in K[X]$ for which $s = g_s(\alpha)$. Since K is the field of fractions of R, the coefficients of g_s are on the form $\frac{a_i}{b_i}$, with $a_i, b_i \in R$ and $b_i \neq 0$. Let d_s be the least common multiple of all b_i. Then $d_s g_s$ is in $R[X]$. Now, let d be the least common multiple of all d_s (this exists since A is finite). This lets us conclude that $dg_s \in R[X]$ for all $s \in A$. Given d, we now define a subset of K as $\tilde{R} := R[d^{-1}]$. For any $s \in A$ we have that $ds = dg_s(\alpha) \in R[d^{-1}\alpha] = \tilde{R}[\alpha]$. And by definition, we also have that $d-1 \in \tilde{R}$. So, $s = d^{-1}ds \in R[\alpha]$, which means that $R[A] = R[\alpha]$ (since $\alpha \in A$). Now we can extend ω to a homomorphism from $\tilde{R}$ to K' by setting $\omega(d^{-1}) = \omega(d)^{-1}$.

Now, let

$$\varphi : \tilde{R}[X] \to \tilde{R}[\alpha];\ \varphi(g) = g(\alpha),$$

and let

$$h \in \ker(\varphi) = \{h \in \tilde{R}[X] \mid h(\alpha) = 0\}.$$

Since f is the minimal polynomial of α, we have that $h = fg$ for some $g \in K[X]$. By Proposition 8.3, $g \in \tilde{R}[X]$, so h is in the ideal generated by f in $\tilde{R}[X]$ and $\ker(\varphi) \subset \langle f \rangle$. On the other hand, every multiple of f have α as a root, so $\langle f \rangle \subset \ker(\varphi)$ and therefore $\ker(\varphi) = \langle f \rangle$.

Any element $r \in \tilde{R}[\alpha]$ is of the form $r = r_0 + r_1\alpha + \cdots + r_n\alpha^n$ with $r_i \in \tilde{R}$. Therefore, $\varphi(r_0 + r_1X + \cdots + r_nX^n) = r$ and φ is surjective. So by the Fundamental Homomorphism Theorem for Rings, there is an isomorphism

$$\phi : \tilde{R}[X]/\langle f \rangle \to \tilde{R}[\alpha];\ \phi(g + \langle f \rangle) = g(\alpha).$$

Looking at $\tilde{R}[X]/\langle f \rangle$ as an extension of $\tilde{R}$ we see that for $r \in \tilde{R}$, $\phi(r) = r$. In other words, ϕ restricted to $\tilde{R}$ is the identity (1).

Now we are getting ready to construct L' and $\tilde{\omega}$. Let g' be the minimal polynomial of α' over K' and let

$$\rho : K'[X] \to K'[X]/\langle g' \rangle;\ \rho(h + kg') = h + \langle g' \rangle,$$

where $h + kg'$ is any polynomial in $K'[X]$ written on the form obtained from the division algorithm (with $\deg(h) < \deg(g')$). Since

$$f(\alpha') = f(\omega(\alpha)) = \omega(f(\alpha)) = \omega(0) = 0$$

the polynomial g' must be an irreducible factor of f'. If $\hat{\omega} : \tilde{R}[X] \to K'[X]$ is the homomorphism obtained by applying ω to the coefficients of polynomials over $\tilde{R}$, then we can use $\rho \circ \hat{\omega} : \tilde{R}[X] \to K'[X]/\langle g' \rangle$ to define a new homomorphism:

$$\gamma : \begin{cases} \tilde{R}[X]/\langle f \rangle \to K'[X]/\langle g' \rangle \\ h + \langle f \rangle \mapsto \rho \circ \hat{\omega}(h) \end{cases}$$

Looking at $K'[X]/\langle g' \rangle$ as an extension of K', we have that ρ restricted to K' is the identity mapping. This means that $\rho \circ \hat{\omega}$ restricts to ω on $\tilde{R}$, and since $\gamma(r + \langle f \rangle) = \rho \circ \hat{\omega}(r)$ for all $r \in \tilde{R}$, we have that γ is an extension of ω (2). Let $L' = K'[x]/\langle g' \rangle$ and let $\tilde{\omega} := \gamma \circ \phi^{-1}$. Obviously, L' is a field extension of K' and from (1) and (2), we have that $\tilde{\omega}$ restricted to $\tilde{R}$ is equal to $\omega \circ \mathrm{id}$, so $\tilde{\omega}$ is an extension of ω. That $L' = K'(\alpha')$ follows directly from Proposition 5.13, since g' is the minimal polynomial of α'.

To show that L'/K' is Galois, let $\hat{\tilde{\omega}} : \tilde{R}[A][Y] \to L'[Y]$ be the homomorphism defined by applying $\tilde{\omega}$ to coefficients of polynomials over $\tilde{R}[A]$. Also, let $\alpha_1, \ldots, \alpha_n$

be the conjugates of α (i.e. the elements α_i such that $f(\alpha_i) = 0$) and $\alpha'_1 \dots \alpha'_n$ be their images under $\tilde{\omega}$. Now, we see that

$$f' = \hat{\tilde{\omega}}(f) = \hat{\tilde{\omega}}((Y - \alpha_1) \cdots (Y - \alpha_n)) = (Y - \alpha'_1) \cdots (Y - \alpha'_n).$$

As showed, f' is separable. Since all these α_i are images of $\tilde{\omega}$, they are in L', and since one of them generates L' we have that $K'(\alpha'_1, \dots, \alpha'_n) = L'$. So L' is a splitting field of f', and by 5.19 we have that L'/K' is Galois. This concludes the proof of the first part of the lemma.

Assume now that f' is irreducible. By Proposition 5.18, the Galois group G acts transitively on the roots of f. Furthermore, the size of G is n, the number of distinct roots of f. From this, it is justified to define σ_i as the unique automorphism in G taking α to one of its conjugates α_i. Likewise, by the assumption that f' is irreducible we can define σ'_i as the unique automorphism in $G' = \mathrm{Gal}(L'/K')$, taking α' to α'_i. We will now show that

$$\psi : \begin{cases} G \to G \\ \sigma_i \mapsto \sigma'_i \end{cases}$$

is an isomorphism.

Since $\tilde{\omega}$, σ_i and σ'_i are homomorphisms, $\tilde{\omega}\sigma_i$ and $\sigma_i\tilde{\omega}$ are also homomorphisms. Furthermore, $\sigma'_i(\tilde{\omega}(r)) = \tilde{\omega}(r)$ for all $r \in \tilde{R}$, since $\tilde{\omega}$ is an extension of ω and σ'_i restricted to K' is the identity. Thus, for any $s \in \tilde{R}[A] = \tilde{R}[\alpha]$ we get

$$\begin{aligned} \tilde{\omega}(\sigma_i(s)) &= \tilde{\omega}(\sigma_i(r_0)) + \tilde{\omega}(\sigma_i(r_1))\tilde{\omega}(\sigma_i(\alpha)) + \cdots + \tilde{\omega}(\sigma_i(r_n))\tilde{\omega}(\sigma_i(\alpha))^n = \\ &= \tilde{\omega}(r_0) + \tilde{\omega}(r_1)\tilde{\omega}(\alpha_i) + \cdots + \tilde{\omega}(r_n)\tilde{\omega}(\alpha_i)^n = \\ &= \tilde{\omega}(r_0) + \tilde{\omega}(r_1)\alpha'_i + \cdots + \tilde{\omega}(r_n)(\alpha'_i)^n \end{aligned}$$

and

$$\begin{aligned} \sigma'_i(\tilde{\omega}(s)) &= \sigma'_i(\tilde{\omega}(r_0)) + \sigma'_i(\tilde{\omega}(r_1))\sigma'_i(\tilde{\omega}(\alpha)) + \cdots + \sigma'_i(\tilde{\omega}(r_n))\sigma'_i(\tilde{\omega}(\alpha))^n = \\ &= \tilde{\omega}(r_0) + \tilde{\omega}(r_1)\sigma'_i(\alpha') + \cdots + \tilde{\omega}(r_n)\sigma'_i(\alpha')^n = \\ &= \tilde{\omega}(r_0) + \tilde{\omega}(r_1)\alpha'_i + \cdots + \tilde{\omega}(r_n)(\alpha'_i)^n. \end{aligned}$$

So $\tilde{\omega}(\sigma_i(s)) = \sigma'_i(\tilde{\omega}(s))$, which gives us that

$$\begin{aligned} (\sigma_i\sigma_j)'(\alpha') &= (\sigma_i\sigma_j)'(\tilde{\omega}(\alpha)) = \\ &= \tilde{\omega}((\sigma_i\sigma_j)(\alpha))) = \\ &= \tilde{\omega}(\sigma_i(\sigma_j(\alpha))) = \\ &= \sigma'_i(\tilde{\omega}(\sigma_j(\alpha))) = \\ &= \sigma'_i\sigma'_j(\alpha'). \end{aligned}$$

To see that ψ is a homomorphism, we want to show that $(\sigma_i\sigma_j)'(x') = \sigma'_i\sigma'_j(x')$ for all $x' \in K'$. Since α' generates L' over K', we can write all elements of L' on the form

$$\frac{p(\alpha')}{q(\alpha')} = \frac{a_0 + a_1\alpha' + \cdots + a_\ell(\alpha')^\ell}{b_0 + b_1\alpha' + \cdots + b_m(\alpha')^m} =$$

where $p, q \in K'[\alpha']$ and $q \neq 0$. Automorphisms of G' map all elements of K' to themselves, so we have that

$$\begin{aligned}(\sigma_i\sigma_j)'(x') &= (\sigma_i\sigma_j)'\left(\frac{a_0 + a_1\alpha' + \cdots + a_\ell(\alpha')^\ell}{b_0 + b_1\alpha' + \cdots + b_m(\alpha')^m}\right) = \\ &= \left(\frac{(\sigma_i\sigma_j)'(a_0) + (\sigma_i\sigma_j)'(a_1)(\sigma_i\sigma_j)'(\alpha') + \cdots + (\sigma_i\sigma_j)'(a_\ell)(\sigma_i\sigma_j)'(\alpha')^\ell}{(\sigma_i\sigma_j)'(b_0) + (\sigma_i\sigma_j)'(b_1)(\sigma_i\sigma_j)'(\alpha') + \cdots + (\sigma_i\sigma_j)'(b_m)(\sigma_i\sigma_j)'(\alpha')^m}\right) = \\ &= \left(\frac{a_0 + a_1(\sigma_i'\sigma_j'(\alpha')) + \cdots + a_\ell(\sigma_i'\sigma_j'(\alpha'))^\ell}{b_0 + b_1(\sigma_i'\sigma_j'(\alpha')) + \cdots + b_m(\sigma_i'\sigma_j'(\alpha'))^m}\right) = \sigma_i'\sigma_j'(x').\end{aligned}$$

So ψ is a homomorphism and by construction it is also onto. Since $|G| = |G'|$ it is therefore a bijection. □

The the next theorem will give us the tool to connect the previous lemma to the Irreducibility Theorem. The first part is more or less a restatement of Theorem 8.1 in general terms, but it also explicitly gives us the specialized Galois extension. For this theorem we will use the fact that if K is a field, then $K(X)$ is the field of fraction over $K[X]$. So if $L/K(X)$ is a Galois extension, Proposition 8.4 allows us to let $\alpha \in L$ be a generator of L, with minimal polynomial $f \in K[X][Y]$.

Theorem 8.6.
Let K be a field and let $L/K(X)$ be a Galois extension. Let α be a generator of L with minimal polynomial $f \in K[X][Y]$. Then the following holds:

(1) *For all but a finite number of $t \in K$, if $f_t(Y) = f(t, Y)$ is irreducible in $K[Y]$, then for $L' = K[X]/\langle f_t\rangle$, L'/K is Galois, and $G = Gal(L/K(X))$ is isomorphic to $G' = Gal(L'/K)$.*

(2) *Let E/K be a finite extension, with $E \subset L$ and let $h \in E[X, Y]$ be an irreducible polynomial with all of its roots in L. Then, for all but a finite number of $t \in K$, if $f_t(Y)$ is irreducible in $K[X]$, then $h_t(Y) = h(t, Y)$ is irreducible in $E[Y]$.*

Proof. Looking at the evaluation homomorphism

$$\omega_t : \begin{cases} K[X] \to K \\ g \mapsto g(t) \end{cases}$$

we see that for any given polynomial $u \in K[X]$ and all but finitely many $t \in K$, $\omega_t(u) \neq 0$, since u is a polynomial in one variable. By Lemma 8.5, for all such $t \in K$ we have an isomorphism between the Galois groups $\mathrm{Gal}(L/K(X))$ and $\mathrm{Gal}(L'/K)$, with $L' = K[Y]/\langle f_t\rangle$. This proves part (1).

For part (2), let ω_t be the same homomorphism as above. Let A be a set as defined in Lemma 8.5 and assume that A contains the generators (and their conjugates) of E/K and the roots $\beta_1, \ldots, \beta_m$ of $h_X = h(X, Y)$. Again by Lemma 8.5, we can then extend ω_t to a homomorphism $\tilde{\omega}_t : K[X][A] \to L'$, where L' is a Galois extension over K. Since all the generators of E is in A, we have that $E \subset K[X][A]$. The homomorphism $\tilde{\omega}_t$ is not trivial and since a homomorphism from a field is either trivial or injective we have that $\tilde{\omega}_t$ maps E isomorphically into L'. For simplicity, we will say that E is in fact equal to its isomorphic copy in L' and by that regard $\tilde{\omega}_t$

restricted to E as the identity. By doing this, we get that $\tilde{\omega}_t$ is also the evaluation homomorphism on $E[X]$. As before, we denote by $\hat{\tilde{\omega}}_t$ the homomorphism we get by letting $\tilde{\omega}_t$ act on coefficients of polynomials in $K[X][A][Y]$. The polynomial h_X has coefficients in $E[X]$, so by letting $\hat{\tilde{\omega}}_t$ act on h_X we get that $\hat{\tilde{\omega}}_t(h_X)(Y) = h_t(Y)$, since this is simply an evaluation of the coefficients. We can now factor $h_X(Y)$ as

$$h_X(Y) = g(X)(Y - \beta_1) \cdots (Y - \beta_m)$$

By letting $\hat{\tilde{\omega}}_t(\beta_i) = \beta_i'$, we then have that

$$h_t(Y) = \hat{\tilde{\omega}}_t(h_X(Y)) = g(t)(Y - \beta_1') \cdots (Y - \beta_m')$$

Since $h_X(Y)$ is irreducible it is also irreducible in $E(X)[Y]$, by Gauss lemma. And since we are working in perfect fields, $h_X(Y)$ is also separable in $E(X)[Y]$ and therefore, by Proposition 5.18 $\mathrm{Gal}(K/L(X))$ permutes the roots β_i transitively.

Assume now that f_t is irreducible. As f_t can be identified with f' in the previous lemma there is an isomorphism between $\mathrm{Gal}(L/K(X))$ and $\mathrm{Gal}(L'/K)$, φ say. Consider the restirction of φ to $\mathrm{Gal}(L/E(X))$. For $z \in E$, $\sigma \in \mathrm{Gal}(L/K(X))$ and $\sigma' = \varphi(\sigma)$ we have $\sigma'(z) = \sigma'(\tilde{\omega}_t(z)) = \tilde{\omega}_t(\sigma(z)) = \tilde{\omega}_t(z) = z$, i.e. E is invariant under σ', and $\varphi(\mathrm{Gal}(L/E(X)) \subset \mathrm{Gal}(L'/E)$. If $\sigma \in \mathrm{Gal}(L/E(X))$ takes β_i to β_j we see that

$$\begin{aligned}\sigma'(\beta_i') &= \sigma'(\tilde{\omega}_t(\beta_i)) \\ &= \tilde{\omega}_t(\sigma(\beta_i)) \\ &= \tilde{\omega}_t(\beta_j) \\ &= \beta_j.\end{aligned}$$

As noted, there is such a σ for any β_j and β_j, so $\mathrm{Gal}(L'/E)$ permutes the roots of h_t transitively. By Proposition 5.18 h_t is therefore irreducible if and only if it is separable.

With $\Delta(h_X) \in E[X]$ being the discriminant of h_X, we have the following:

$$\Delta(h_X) = g(X)^{2n-2} \prod_{i<j} (\beta_i - \beta_j)^2.$$

We can evaluate this polynomial by applying $\tilde{\omega}_t$ and get

$$\Delta(h_X)(t) = g(t)^{2n-2} \prod_{i<j} (\beta_i' - \beta_j')^2 = \Delta(h_t).$$

Since $\Delta(h_X)$ is a single variable polynomial in $E[X]$, there are finitely many $t \in K$ such that $\Delta(h_t) = 0$, and so there are finitely many $t \in K$ for which h_t is not separable. Hence, h_t is irreducible for all but finitely many $t \in K$. □

Definition 8.7.
*A field K is **Hilbertian** (or is said to have the **Hilbertian property**), if for any irreducible polynomial $f \in K[X, Y]$, there are infinitely many $t \in K$ for which $f_t(Y) = f(t, Y)$ is irreducible in $K[Y]$.*

As we have shown with Hilbert's Irreducibility Theorem, $\mathbb{Q}$ is Hilbertian. To see that there are fields that are not Hilbertian it is enough to consider $\mathbb{C}$. For example, the polynomial $f = Y^n + XY + X$ is irreducible in $\mathbb{C}[X, Y]$ but $f(z, Y) = Y^n + zY + z$ is split in $\mathbb{C}[Y]$ for any $z \in \mathbb{C}$. In the next proposition we use part (2) of Theorem 8.6 to give an equivalent definition to a field being Hilbertian.

Proposition 8.8.
A field K is Hilbertian if and only if, for any finite extension E/K and irreducible polynomials $h_1, \ldots, h_k \in E[X, Y]$, there are infinitely many $t \in K$ such that each $h_i(t, Y)$ is irreducible in $E[Y]$.

Proof. Suppose K is Hilbertian and let $h_1, \ldots, h_k \in E[X][Y]$ be irreducible polynomials. By Gauss' lemma, these polynomials are also irreducible in $E(X)[Y]$. Let M be the finite extension of $E(X)$ obtained by adjoining the roots of all said polynomials to $E(X)$. Define L to be the Galois closure of M over $K(X)$ (i.e. the smallest Galois extension over $K(X)$ containing M). By Proposition 8.4, there is an element $\alpha \in L$ such that $L = K(X)[\alpha]$ with $f \in K[X, Y]$ being the minimal polynomial of α. For any h_i, we have by part (2) of Theorem 8.6 that for all but finitely many $t \in K$, if $f(t, Y)$ is irreducible then $h_i(t, Y)$ is also irreducible. If C is the set of elements $t \in K$ for which any $h_i(t, Y)$ is reducible even if $f(t, Y)$ is irreducible, then C is a finite union of finite set, hence itself finite. If B is the set of elements $t \in K$ such that $f(t, Y)$ is irreducible, then B is obviously infinite since K is Hilbertian. Conclusively, the set $B \setminus C$ is infinite, and for all elements t in this set, $h_i(t, Y)$ is irreducible, for all i.

For the other direction, consider the trivial extension K/K. Let $f \in K[X, Y]$ be any irreducible polynomial. By assumption, $f(t, Y) \in K[Y]$ is irreducible for infinitely many $t \in K$, which means exactly that K is Hilbertian. □

We will use this proposition to generalize our results to polynomials in several variables, and to do this we need a very useful mapping called the Kronecker Specialization.

Definition 8.9.
*For any $d \in \mathbb{N}$, the **Kronecker Specialization** is a map defined as follows:*

$$S_d : K[X_1, \ldots, X_k] \to K[X, Y]$$
$$S_d(f)(X, Y) = f(X, Y, Y^d, Y^{d^2}, \ldots, Y^{d^{k-2}})$$

Since S_d is a composition of evaluation homomorphisms, it is itself a ring homomorphism, which we use in the following result.

Proposition 8.10.
Let K be a field. Also, let V_d be the set of polynomials in $K[X_1, \ldots, X_k]$ of degree less than d in each variable $X_i \neq X_1$, and let W_d be the set of polynomials in $K[X, Y]$ of degree less than d^{k-1} in Y. Then the Kronecker Specialization S_d is a bijection between V_d and W_d. In particular, S_d maps irreducible polynomials in V_d to irreducible polynomials in W_d.

Proof. Let $f \in V_d$ be a monomial of the form $aX_1^{\alpha_1} \cdots X_k^{\alpha_k}$. Applying S_d to f we get the monomial $aX^{\alpha_1}Y^{\alpha_2+\alpha_3 d+\alpha_4 d^2+\cdots+\alpha_k d^{k-2}}$ in $K[X, Y]$. Since each α_i is smaller than d the exponent of Y is the representation of an integer in base d. Hence it is unique, and every integer can be represented this way [3]. Therefore, S_d is a bijection between monomials in V_d and monomials in W_d. Since S_d is a ring homomorphism we can consider it to act on monomials in a polynomial separately,

and so we see that S_d is a bijection from V_d to W_d. Suppose f is an irreducible polynomial in V_d and that $S_d^{-1}(gh) = f$. Since $f = S_d^{-1}(gh) = S_d^{-1}(g)S_d^{-1}(h)$. Hence, $S_d^{-1}(g)$ or $S_d^{-1}(h)$ is a unit, and since S_d maps units to units we have that g or h is a unit. So gh is irreducible. □

We now have the proper tools to extend the Hilbertian Property to polynomials in several variables. First we will see that the property remains for specialization of one of these variables, but a very immediate result is that we in fact can specialize any number of variables and still keep irreducibility. This will be a key result to allow us to go from extensions of rational function fields over $\mathbb{Q}$ to extensions over $\mathbb{Q}$.

Theorem 8.11.
If K is Hilbertian and $f \in K[X_1, \ldots, X_k]$ is an irreducible polynomial, then there are infinitely many $t \in K$ such that $f(t, X_2, \ldots, X_k)$ is irreducible in $K[X_2, \ldots, X_k]$.

Proof. Take d to be an integer large enough so that $S_d(f)$ is in W_d. Now, consider the prime factorization of $S_d(f)$ and denote by $g(X)$ the product of all polynomials in this factorization that only depend on X. Then we have the factorization

$$S_d(f)(X, Y) = g(X) \prod_{i \in C} g_i(X, Y)$$

where C is the set such that $g_i(X, Y)$ is a prime factor of $S_d(f)$ with positive degree in the variable Y. All $g_i(X, Y)$ are irreducible so by the Hilbertian property, any $g_i(t, Y)$ is irreducible in $K[Y]$ for infinitely many $t \in F$. Let $\mathscr{B}$ be the set consisting of $t \in K$ such that all $g_i(t, Y)$ is irreducible in $K[Y]$ and $g(t) \neq 0$. Since $g(X)$ is a single variable polynomial, it has finitely many roots. Furthermore, the number of $t \in K$ such that any $g_i(t, Y)$ is reducible is a finite union of finite sets, hence finite. So $\mathscr{B}$ consists of all but finitely many $t \in K$. For any $t \in \mathscr{B}$, we have that $g(t) \prod_{i \in C} g_i(t, Y)$ is a prime factorization of $S_d(f)(t, Y)$ Suppose now that $f_t = f(t, X_2, \ldots, X_k)$ is reducible. Then $f_t = hh'$, and since S_d is a ring homomorphism we get

$$\begin{aligned} S_d(h)S_d(h') &= S_d(hh') = \\ &= S_d(f_t) = \\ &= S_d(f)(t, Y) = \\ &= g(t) \prod_{i \in C} g_i(t, Y). \end{aligned}$$

Therefore, if $A \coprod B = C$ is a partition of C and $uu' = g(t)$ we can write

$$S_d(h) = u \prod_{i \in A} g_i(t, Y) \text{ and } S_d(h') = u' \prod_{i \in B} g_i(t, Y)$$

Now define

$$H(X, Y) = \prod_{i \in A} g_i(X, Y) \text{ and } H'(X, Y) = \prod_{i \in B} g_i(X, Y).$$

Since $S_d(f) = gHH'$ and $S_d(f) \in W_d$, H and H' must also be in W_d. Therefore we can find unique polynomials $\tilde{h}, \tilde{h}' \in V_d$ such that $S_d(\tilde{h}) = H$ and $S_d(\tilde{h}') = H'$.

If $\tilde{h}_t = \tilde{h}(t, X_2, \ldots, X_k)$ and $\tilde{h}'_t = \tilde{h}'(t, X_2, \ldots, X_k)$ we see that

$$\begin{aligned} S_d(\tilde{h}_t) &= S_d(\tilde{h})(t, Y) = \\ &= H(t, Y) = \\ &= \prod_{i \in A} g_i(t, Y) = \\ &= u^{-1} S_d(h) = \\ &= S_d(u^{-1} h). \end{aligned}$$

As $\tilde{h} \in V_d$ the specialization $\tilde{h}_t$ must also be in V_d and since S_d is a bijection between V_d and W_d, we have that $\tilde{h}_t = u^{-1}h$. By the same reasoning we get that $\tilde{h}'_t = (u')^{-1}h'$. Thus

$$\tilde{h}_t \tilde{h}'_t = u^{-1}(u')^{-1} h h' = g(t)^{-1} f_t. \tag{1}$$

If $\tilde{h}\tilde{h}'$ is in V_d, then $S_d(g\tilde{h}\tilde{h}') = g S_d(\tilde{h}) S_d(\tilde{h}') = gHH' = S_d(f)$. But then $f = g\tilde{h}\tilde{h}'$, contradicting the irreducibility of f. Hence, $\tilde{h}\tilde{h}'$ is not in V_d. By (1) we have that $\tilde{h}_b \tilde{h}'_b \in V_d$, if we look at $\tilde{h}\tilde{h}'$ as a polynomial with coefficients in $K[X_1]$ we have that t must be a root of the coefficients of every term where the degree of any of the variable $X_2, \ldots, X_k$ is greater than $d-1$. But since there are finitely many ways to factor $S_d(f)$, there are finitely many possible polynomials to choose as H and H'. And therefore, there are also finitely many possibilities for their bijections $\tilde{h}$ and $\tilde{h}'$, and so the roots of said coefficients must be a finite set, $\mathscr{B}'$ say. So, for all t in the infinite set $\mathscr{B} \setminus \mathscr{B}'$ we get a contradiction, and so f_t is irreducible for all $t \in \mathscr{B} \setminus \mathscr{B}'$. □

Corollary 8.11.1.
If K is a Hilbertian field and $f \in K[X_1, \ldots, X_k]$ is irreducible, then for any $n < k$ and any nonzero polynomial $p \in K[X_1, \ldots, X_n]$ there are elements $t_1, \ldots, t_n$ in K such that $p(t_1, \ldots, t_n) \neq 0$ and $f(t_1, \ldots, t_n, X_{n+1}, \ldots, X_k)$ is irreducible in $K[X_{n+1}, \ldots, X_k]$.

Proof. We will prove this by induction on the number of specialized variables of f. The statement for $n = 1$ follows directly from the previous theorem, since p then is a single variable polynomial with finitely many roots. Our inductive hypothesis is that it holds true for $n < k-1$. Take p now to be a polynomial in $K[X_1, \ldots, X_{n+1}]$. We can consider p as a polynomial with coefficients in $K[X_{n+1}]$. Since each coefficient of p has finitely many roots, there is a $b \in K$ such that $p(X_1, \ldots, X_n, b)$ is a nonzero polynomial in n variables. By the inductive hypothesis, there are elements $t_1, \ldots, t_n \in K$ such that $f(t_1, \ldots, t_n, X_{n+1}, \ldots, X_k)$ is irreducible. By the previous theorem, for all but finitely many $t \in K$, we have that $f(t_1, \ldots, t_n, t, X_{n+2}, \ldots, X_k)$ is irreducible. Now, since $p(t_1, \ldots, t_n, X_{n+1})$ is a single variable polynomial, it has finitely many roots. Thus, there is a $t \in K$ satisfying both $p(t_1, \ldots, t_n, t) \neq 0$ and $f(t_1, \ldots, t_n, t, X_{n+2}, \ldots, X_k)$ being irreducible. This proves that the inductive hypothesis holds for $n+1$. □

Theorem 8.12.
Every finitely generated extension of a Hilbertian field is Hilbertian

Proof. Let K be a Hilbertian field and $L = K(\alpha_1, \ldots, \alpha_n)$ a finitely generated extension. Take L' to be the subfield of L generated over K by the elements of $\alpha_1, \ldots, \alpha_n$ that are algebraic over K, call these elements $\alpha'_1, \ldots, \alpha'_k$. Then $L' = K[\alpha'_1, \ldots, \alpha'_k]$, and $L'[X, Y] = K[\alpha'_1, \ldots, \alpha'_k, X, Y]$. By Theorem 8.11, for any irreducible polynomial $f \in L'[X, Y]$ there are infinitely many t in K (hence in L' such that $f(t, Y)$ is irreducible in $L'[Y]$, i.e. $L'[Y]$ is Hilbertian. Now, we can consider L as a purely transcendental extension of L', so $L[X, Y] = L'(\beta_1, \ldots, \beta_m)[X, Y]$ for $\beta_1, \ldots, \beta_m$ transcendental over L'. Let $f \in L'(\beta_1, \ldots, \beta_m)[X, Y]$ be irreducible and let $g \in L'(\beta_1, \ldots, \beta_m)$ be the least common multiple of the coefficients of f. Then, gf is an irreducible polynomial in $L'[\beta_1, \ldots, \beta_m, X, Y]$ (it is irreducible because any root of fg would also be a root of f). By Theorem 8.11, there are infinitely many t in L' (hence also in L) such that $gf(t, Y)$ is irreducible in $L'[\beta_1, \ldots, \beta_m, Y]$ and by Gauss' lemma, $gf(t, Y)$ is also irreducible in $L[Y]$. Finally, we can look at g as a constant polynomial in $L[X, Y]$ and get that $gf(t, Y) = g(t, Y)f(t, Y) = gf(t, Y)$. Since g is a unit, $f(t, Y)$ is irreducible. □

Now we have all we need to prove the main result of this section.

Theorem 8.13. *If K is Hilbertian and L is a Galois extension of $K(X_1, \ldots, X_k)$, then Gal$(L/K(X_1, \ldots, X_k))$ is isomorphic to the Galois group given by some Galois extension L'/K.*

Proof. We prove this by induction on k. The base case $k = 1$ follows from part (1) of Theorem 8.6 and the fact that K is Hilbertian. Our induction hypothesis is that the statement holds for $k \geq 1$. Let L be a Galois extension of $K(X_1, \ldots, X_k)$, By the previous theorem, $K(X_1, \ldots, X_k)$ is Hilbertian. Since $K(X_1, \ldots, X_{k+1}) = K(X_1, \ldots, X_k)(X_{k+1})$, the base case gives us that $\mathrm{Gal}(L/K(T_1, \ldots, T_{k+1}))$ is isomorphic to $\mathrm{Gal}(L'/K(T_1, \ldots, T_k))$, which by the inductive hypothesis is isomorphic to $\mathrm{Gal}(L''/F)$. □

This last theorem lets us conclude that all Groups that appear as Galois groups of some Galois extension over a rational function field over $\mathbb{Q}$ is also a Galois group of some extension over $\mathbb{Q}$. This greatly simplifies the task to find groups that appear as Galois groups over some extension of $\mathbb{Q}$. We have already shown in Example 5.22 $\mathfrak{S}_n$ has this property. There are many other examples, for example abelian groups [11, pp. 36–37]. We will dedicate the last section of this text to another motivating example. There are of course also a lot of groups for which it is still unknown if they have this property. The smallest simple group for which the Inverse Galois Problem is not known has cardinality 9828 [14].

9. The Alternating Group A_n as Galois Group

We will start this section by once again showing that $\mathfrak{S}_n$ appears as the Galois group of some Galois extension over $\mathbb{Q}$. This time we will do it in a much more complicated way, but it will have its reward as it will also give us a tool to show the same property holds for the alternating group A_n.

Theorem 9.1.
Let K be the splitting field of $f(t,X) = X^n + tX + t \in \mathbb{Q}(t)[X]$ over $Q(t)$. Then $Gal(K/\mathbb{Q}(t)) = \mathfrak{S}_n$.

Proof. By applying Eisenstein's criterion to $\mathbb{Q}[t]$, we get that $f(t,X)$ is irreducible in $\mathbb{Q}(t)[X]$. Consider now the following specialization to $\mathbb{Q}[X]$:

$$f\left(-\frac{1}{2}, X\right) = X^n - \frac{1}{2}X - \frac{1}{2} = \\ = (X-1)\frac{1}{2}\left(2X^{n-1} + 2X^{n-2} + \cdots + X + 1\right).$$

The reciprocal polynomial of the last factor is $X^{n-1}+2X^{n-1}+\cdots+2X+2$, which is irreducible due to Eisenstein's criterion. Therefore, this factor of $f\left(-\frac{1}{2}, X\right)$ is also irreducible. The Galois group $H_1 = \mathrm{Gal}\left(f\left(-\frac{1}{2}, X\right)/\mathbb{Q}\right)$ then acts transitively on $n-1$ roots of this irreducible polynomial. Furthermore, since $1 \in \mathbb{Q}$ we have that one root of $f\left(-\frac{1}{2}, X\right)$ is fixed by H_1. By Theorem 7.9, H_1 can be considered as a subgroup of $G = \mathrm{Gal}(f(t,X)/\mathbb{Q}(t))$. Since $f(t,X)$ is irreducible, G acts transitively on its roots. Denote the roots by $x_1, \ldots, x_n$ with x_q being the root fixed by $H_1 \subset G$. Let $g_r \in G$ be such that $g_r(x_1) = x_r$, with $1 < r \leq n$. Then the subgroup $g_r H_1 g_r^{-1}$ fixes the root x_r and acts transitively on the other roots. Hence, G is doubly transitive.

Before we continue, it might be worth noting that we are only interested in $n > 1$ (the group $\mathfrak{S}_1$ being trivial as the identity), which will justify coming variable changes. Now, let $s = t + n^n(1-n)^{n-1}$. By this change of variable we can write

$$g(s,X) = f(t,X) = X^n + \left(s - \frac{n^n}{(1-n)^{n-1}}\right)X + \left(s - \frac{n^n}{(1-n)^{n-1}}\right),$$

This does not affect the Galois group G since $\mathbb{Q}(s) = \mathbb{Q}(t)$. If $\mathbb{C}((s))$ is the quotient field of the ring of formal power series in the variable s over $\mathbb{C}$, then it is clear that $\mathbb{Q}(s) \subset \mathbb{C}((s))$ and by the Galois correspondence we have

$$H_2 = \mathrm{Gal}(g(s,X)/\mathbb{C}((s))) \subset \mathrm{Gal}(g(s,X)/\mathbb{Q}(s)) = G.$$

The discriminant

$$\Delta(g) = (-1)^{n(n-1)/2}(1-n)^{n-1}s\left(s - \frac{n^n}{(1-n)^{n-1}}\right)^{n-1}$$

is not a square in $\mathbb{C}((s))$ so the splitting extension of $g(s,X)$ over $\mathbb{C}((s))$ is not trivial. Now, we can in fact regard $g(s,X)$ as a polynomial in $\mathscr{A}(r)[X]$, since the coefficients of g as power series are obviously convergent for all s. Specializing in $s = 0$ gives us

$$g(0,X) = X^n - \frac{n^n}{(1-n)^{n-1}}X - \frac{n^n}{(1-n)^{n-1}}$$

Again we make a change in variable, by setting

$$X = \frac{nY}{1-n}$$

which gives us

$$g(0,Y) = \frac{n^n Y^n}{(1-n)^n} - \frac{n^{n+1}Y}{(1-n)^n} - \frac{n^n}{(1-n)^{n-1}}.$$

This polynomial can be multiplied by $\left(\frac{1-n}{n}\right)^n$ without changing it roots. We call this new scaled polynomial h and regard it as a polynomial i $\mathbb{C}[Y]$.

$$\begin{aligned} h(Y) &= Y^n - nY + (n-1) = \\ &= (x-1)^2(Y^{n-2} + 2Y^{n-3} + \cdots + (n-2)Y + (n-1)) \end{aligned}$$

It has a double root at 1. If we take its formal derivative, we get

$$h'(Y) = n(Y^{n-1} - 1).$$

A root y of h is a multiple root if and only if $h'(y) = 0$ and since a root y of h' is such that $y^{n-1} = 1$ we get

$$\begin{aligned} &h(y) = 0 \Leftrightarrow \\ \Leftrightarrow\ &y^n - ny + (n-1) = 0 \Leftrightarrow \\ \Leftrightarrow\ &y(1-n) + (n-1) = 0 \Leftrightarrow y = 1. \end{aligned}$$

So h has a double root at $Y = 1$ and $n-2$ simple roots. Set $\delta \in \mathbb{C}$ to be any of these simple roots. Then $h(Y) = (Y-\delta)\tilde{h}(Y)$ where $\tilde{h}(Y)$ is a monic polynomial of degree $n-1$. Obviously $Y - \delta$ and $\tilde{h}(Y)$ are coprime and so by Proposition 2.3, this means that $g(s, Y)$ as a polynomial in $\mathscr{A}(r)[Y]$ has a linear factor in $\mathscr{A}(\rho)[Y]$ that specializes to $Y - \delta$. In other words, it has a root in $\mathscr{A}(\rho)$ corresponding to the simple root δ. This can be done for each of the $n-2$ simple roots and since $\mathscr{A}(\rho) \subset \mathbb{C}((s))$ we have that the $n-2$ simple roots of $g(s, Y)$ are left invariant by the Galois group H_2. We have shown that H_2 is not trivial so it must act by permuting the two remaining roots.

So, G is a doubly transitive subgroup of $\mathfrak{S}_n$ that contains a transposition. To see that this means that $G = \mathfrak{S}_n$, let $(i\ j)$ be the transposition we know is in G and let $(k\ \ell)$ be any other transposition in $\mathfrak{S}_n$. Take σ_1 to be an element of G that fixes i and takes j to ℓ, and take σ_2 to be the element that fixes ℓ and takes i to k. Then

$$\sigma_2 \circ \sigma_1 \circ (i\ j) \circ \sigma_1^{-1} \circ \sigma_2^{-1} = (k\ \ell)$$

and since $\mathfrak{S}_n$ is generated by all transpositions, we have that $G = \mathfrak{S}_n$. □

Corollary 9.1.1.
For $n \in \mathbb{N}$ with $n > 1$, the Galois extension of the polynomial

$$p(\kappa, X) = \begin{cases} X^n + \frac{(-1)^{(n-1)/2}\kappa^2 - n^n}{(n-1)n-1}(X+1) & \text{if } n \text{ is odd} \\ X^n + \frac{n^n}{(-1)^{n/2}\kappa^2 + (n-1)^{n-1}}(X+1) & \text{if } n \text{ is even} \end{cases}$$

over $\mathbb{Q}(\kappa)$ has Galois group A_n.

Proof. Let K and f be as in the theorem above. The procedure is to find a quadratic subextension of K over $\mathbb{Q}(t)$. If F is such a subextension of K over $\mathbb{Q}(t)$ with degree two, we have that

$$[K : \mathbb{Q}(t)] = [K : F][F : \mathbb{Q}(t)] = 2[K : \mathbb{Q}(t)]$$

This means that the Galois group $\mathrm{Gal}(K/F)$ has cardinality $|\mathfrak{S}_n|/2$.

We have that the discriminant

$$\Delta(f(t, X) = (-1)^{n(n-1)/2} t^{n-1}((1-n)^{n-1}t + n^n). \tag{1}$$

First assume n is odd. Then if we define

$$u = \sqrt{(-1)^{n(n-1)/2}((1-n)^{n-1}t + n^n)}$$

we have that $u^2 \in \mathbb{Q}(t)$ and u is obviously algebraic over $\mathbb{Q}(t)$ with minimal polynomial $X^2 - u^2$. Hence, $\mathbb{Q}(t,u)$ has degree 2 over $\mathbb{Q}(t)$. We can express t in terms of u as

$$t = \frac{(-1)^{n(n-1)/2}u^2 - n^n}{(1-n)^{n-1}}$$

and get by (1) that

$$\begin{aligned}\Delta(f(t,X)) &= (-1)^{n(n-1)/2}t^{n-1}\left((1-n)^{n-1}\frac{(-1)^{n(n-1)/2}u^2 - n^n}{(1-n)^{n-1}} + n^n\right) = \\ &= (-1)^{n(n-1)/2}t^{n-1}\left((-1)^{n(n-1)/2}u^2 - n^n + n^n\right) = t^{n-1}u^2.\end{aligned}$$

As n is odd, this is a perfect square and since $\prod_{i<j}(x_i - x_j)$, i.e. the root of $\Delta(f)$, is in the splitting field K, we have that $t^{(n-1)/2}u \in K$. Then $u \in K$ and $\mathbb{Q}(t,u) \subset K$. The polynomial $p(u,X)$ is simply $f(t,X)$ with t expressed in terms of u.

Now assume n is even and let

$$v = \sqrt{(-1)^{n(n-1)/2}((1-n)^{n-1} + n^n/t)}.$$

By the same argument as above, $\mathbb{Q}(v)$ is an extension of $\mathbb{Q}(t)$ with degree 2. We can write

$$t = \frac{n^n}{(-1)^{n(n-1)/2}v^2 - (1-n)^{n-1}}$$

and we can proceed as above:

$$\begin{aligned}\Delta(f(t,X)) &= (-1)^{n(n-1)/2}t^{n-1}\left((1-n)^{n-1}\frac{n^n}{(-1)^{n(n-1)/2}v^2 - (1-n)^{n-1}} + n^n\right) = \\ &= (-1)^{n(n-1)/2}t^{n-1}\left(\frac{(-1)^{n(n-1)/2}n^n v^2}{(-1)^{n(n-1)/2}v^2 - (1-n)^{n-1}}\right) = \\ &= t^{n-1}\left(\frac{n^n v^2}{(-1)^{n(n-1)/2}v^2 - (1-n)^{n-1}}\right) = \\ &= t^{n-1}(tv^2) = t^n v^2.\end{aligned}$$

This is a perfect square as n is even, and by the same reasoning as above this means that $\mathbb{Q}(t,v) \subset K$. And the polynomial $p(v,X)$ is $f(t,X)$ with t expressed in terms of v.

Finally, we have seen that the discriminant of $p(\kappa,X)$ is a perfect square in $\mathbb{Q}(\kappa)$ for both odd and even n. Therefore, the root of the discriminant is invariant under $\mathrm{Gal}(K/\mathbb{Q}(\kappa))$. Now we simply just have to note that applying an odd number of transposition to $\prod_{i<j}(x_i - x_j)$ gives us $-\prod_{i<j}(x_i - x_j)$, so elements of $\mathrm{Gal}(K/\mathbb{Q}(\kappa))$ must be the product of an even number of transpositions. Hence $\mathrm{Gal}(p(\kappa,X)/\mathbb{Q}(\kappa))$ is the alternating group A_n. □

References

[1] A. Chambert-Loir, *A Field Guide to Algebra*, Springer, New York, 2005.

[2] J. A. Beachy and W. D. Blair, *Abstract Algebra*, Waveland Press, Illinois, 3rd edition, 2006.

[3] V. H. Moll, *Numbers and Functions: From a Classical-Experimental Mathematician's Point of View*, Student Mathematical Library, 2012, pp. 17–18.

[4] E. B. Saff and A. D. Snider, *Fundamentals of Complex Analysis with Applications to Engineering and Science*, Pearson Education, New Jersey, 3rd edition, 2003.

[5] M. Rosenzweig, *Banach Fixed Point Theorem and Some Applications*, http://www.math.uoc.gr/ pamfilos/Winter2013/Rosenzweig.pdf (as per 2015.06.10)

[6] S. Roman, *Field Theory*, Springer, 2nd edition, 2003, pp. 37–39.

[7] K. J. Nowak *Some Elementary Proofs of Puiseux's Theorem*, Universitatis Iagellonicae Acta Mathematica, 2000.

[8] S. S. Abhyankar *Algebraic Geometry for Scientists and Engineers*, Universitatis Iagellonicae Acta Mathematica, 2000, pp. 89-94.

[9] L. Chariker *The Inverse Galois Problem, Hilbertian Fields, and Hilbert's Irreducibility Problem*, http://www.math.uchicago.edu/ may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Chariker.pdf (as per 2015.06.10)

[10] H Völklein, *Groups as Galois Groups*, Cambridge University Press, 1996.

[11] J-P. Serre, *Topics in Galois Theory*, Course at Harvard University (written by H. Darmon), 1988.

[12] D. J. H. Garling *A course in Galois theory*, Cambridge University Press, 1986, p. 51.

[13] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials Constructive Aspects of the Inverse Galois Problem*, Cambridge University Press, 2002.

[14] D. Zywina, *Inverse Galois Problem For Small Simple Groups*, Department of Mathematics, Cornell University, http://www.math.cornell.edu/ zywina/papers/smallGalois.pdf (as per 2015.06.01)