THE INVERSE GALOIS PROBLEM, HILBERTIAN FIELDS, AND HILBERT'S IRREDUCIBILITY THEOREM

LOGAN CHARIKER

Contents

1. Introduction

In the study of Galois theory, after computing a few Galois groups of a given field, it is very natural to ask the question of whether or not every finite group can appear as a Galois group for that particular field. This question was first studied in depth by David Hilbert, and since then it has become known as the Inverse Galois Problem. It is usually posed as which groups appear as Galois extensions over $\mathbb{Q}$ specifically, and there have been a number of celebrated results over the years pertaining to this question, perhaps most notably being Shafarevich's theorem that every solvable group has such a realization over $\mathbb{Q}$. This paper, however, will focus around the classical result known today as Hilbert's Irreducibility Theorem, which is a useful tool in Inverse Galois Theory.

A large number of realizations of groups as Galois groups over $\mathbb{Q}$ can easily be found using basic types of extensions. For instance, using cyclotomic field extensions and the theorem of finitely generated abelian groups, one finds that every finite abelian group can be realized. We also have that if K and K' are two Galois extensions of a field F, where $K \cap K' = F$, then KK' is also a Galois extension, with Galois group $Gal(K/F) \times Gal(K'/F)$, so we can often realize the direct product of two realizable groups. Given a Galois extension K with Galois group G and normal subgroup H, we have by the fundamental theorem of Galois that G/H can be realized over the same field as well.

A very important group we may be curious about realizing as a Galois group over $\mathbb{Q}$ is S_n. By looking at the general polynomial $f(x) = (x - x_1) \cdots (x - x_n)$, where $x_1, \ldots, x_n$ are indeterminate and $s_1, \ldots, s_n$ are the elementary symmetric functions of $x_1, \ldots, x_n$, we can find that the function field $\mathbb{Q}(x_1, \ldots, x_n)$ is Galois over $\mathbb{Q}(s_1, \ldots, s_n)$, with Galois group S_n. We would like, however, to find S_n realized as a Galois extension over $\mathbb{Q}$ instead. In general, when we have a Galois group realized as an extension of a field of rational functions over a field F, we

would also like to "descend" and have the group be realized over F. Hilbert's Irreducibility Theorem tells us that we can do this for $\mathbb{Q}$, and the aim of this paper will be to show that we can do the same for a general type of field called a hilbertian field. The reason this may be interesting to someone working on the Inverse Galois Problem is because it is often easier to find Galois groups realized over the field of rational functions of F.

Before we begin, we will set up some conventions for the paper. Every field will be of characteristic 0, and every Galois extension will be finite. For F a field, $F(x_1, \ldots, x_n)$ will, unless stated otherwise, denote the field of rational functions in n variables over F, and $F[x_1, \ldots, x_n]$ will denote the ring of polynomials of n variables. For R a subring of a ring S, and A a set, $R[A]$ will denote the smallest ring containing both R and A, and if A is a singleton, we will just write the element in place of A. $D(f)$ will denote the determinant of a polynomial f.

2. Some Machinery

To begin, we want to build up our machinery by proving a general lemma, which when given a Galois extension of a field of fractions, will allow us to find, for other fields, extensions with the same Galois group. This will be our main tool in finding the Galois extensions mentioned above.

Before immediately jumping in, however, we will prove some basic propositions:

Proposition 1. *Let R be an integral domain, and S a subring. Given $f, h \in S[x]$, and $g \in R[x]$ such that $fg = h$, we have that $g \in S[x]$ as well if f is monic.*

Proof. If f is monic, we have that there are unique polynomials $q, r \in S[x]$ such that $h = fq + r$ and $deg(r) < deg(f)$. Then $fq + r = fg$, so $r = f(g - q)$. Now since R is an integral domain, the sum of the degrees of f and $g - q$ is the degree of r, in the case $g - q \neq 0$. But this would contradict that $deg(r) < deg(f)$, so we must have that $g = q$ and $r = 0$. Hence g is a polynomial in $S[x]$. □

Proposition 2. *Let F be the field of fractions of one of its subrings R, and let K/F be a Galois extension of degree n. Then we can find a generator α for K/F such that its minimal polynomial f is in $R[x]$.*

Proof. We assume it is known that all Galois extensions are simple extensions, so take β a generator of K/F. Since F is the field of fractions of R, we can multiply the minimal polynomial of β, which we'll call m_β, by a nonzero constant $d \in R$ such that all of the coefficients of dm_β lie in R. Defining $\alpha := d\beta$, we see that $F(\alpha) = F(\beta)$, i.e., α is also a generator for K/F. For $b_{n-1}, \ldots, b_0$ the coefficients of m_β, define f as follows:

$$f(x) = x^n + db_{n-1}x^{n-1} + d^2b_{n-2}x^{n-2} + \cdots + d^{n-1}a_1x + d^na_0. \tag{1}$$

We see that f is a monic, degree n polynomial in $R[x]$, and that it has α as a root: $f(\alpha) = f(d\beta) = d^n m_\beta(\beta) = 0$. Since the degree of $K/F(=F(\alpha)/F)$ is the degree of the minimal polynomial of α, we see that f must be the minimal polynomial. □

We will be working with polynomial rings and rational function fields, so when we apply the previous proposition and the following lemma, our field of fractions will be some rational function field, and the underlying ring will be a polynomial ring. The following lemma is at the core of our end result, since it will be what we use to construct our Galois extensions. So here it is:

Lemma 1. *Take K, F, R, f, and α from the previous proposition. Let A be a finite subset of K closed under the automorphisms of $G := Gal(K/F)$, and let α be in A. Then $\exists u \in R$ such that for any field F' and ring homomorphism $\omega : R \to F'$ satisfying $\omega(u) \neq 0$, we can extend ω to a ring homomorphism $\tilde{\omega}$ from $R[A]$ to a Galois extension K'/F' with the following properties:*

(1) $\alpha' := \tilde{\omega}(\alpha)$ is a generator for K'/F'.

(2) Let $f' \in F'[x]$ be the polynomial obtained by applying ω to the coefficients of f. Then if f' is irreducible, we have that $G' := Gal(K'/F')$ is isomorphic to G, and furthermore, for $\sigma' \in K'$ the image of $\sigma \in K$ under this isomorphism, we have that $\widetilde{\omega}(\sigma'(s)) = \sigma'(\widetilde{\omega}(s))$.

Proof. Let $u = D(f)$ be the discriminant of f. Since f is a minimal polynomial, it is irreducible, and since we are working in a characteristic 0 field, f is separable, and hence $u \neq 0$. Consider some field F' and ring homomorphism $\omega : R \to F'$ satisfying $\omega(u) \neq 0$. We see that $D(f') = \omega(u)$, so f' is separable.

Since α is a generator for K/F, we know that for every $s \in A$ there is a polynomial $g_s \in F[x]$ such that $s = g_s(\alpha)$. Recall that F is the field of fractions of R, so there is a $d_s \in R$ such that $d_s g_s$ is a polynomial with coefficients in R. Because there are only finitely many $s \in A$, we can find a common d such that $dg_s \in R[x]$ regardless of which s we choose, namely by setting

$$d = \prod_{s \in A} d_s. \tag{2}$$

Given d, we now define $\tilde{R} := R[d^{-1}]$. Note that $\tilde{R}[A] = \tilde{R}[\alpha]$, since for every $s \in A$ we have by choice of d that $ds \in \tilde{R}[\alpha]$, and $d^{-1} \in \tilde{R}[\alpha]$, so that $s = d^{-1}ds \in \tilde{R}[\alpha]$. Now extend ω to a homomorphism from $\tilde{R}$ to F' by setting $\omega(d^{-1}) = \omega(d)^{-1}$. In the course of this proof, we will end up finding an extension from $\tilde{R}[A]$ to some K' with the above properties, but we will be able to take the restriction over $R[A]$ afterwards and still retain these desired properties.

Let $\varphi : \tilde{R}[x] \to \tilde{R}[\alpha]$ denote the evaluation homomorphism defined $\varphi(g) = g(\alpha)$. We claim that the kernel of φ is the ideal generated by f in $\tilde{R}[x]$. To see this, first take $h \in ker(\varphi)$, i.e., a polynomial with α as a root. Then $fg = h$ for some g in $F[x]$ since f is the minimal polynomial of α. Now, our first proposition tells us that $g \in \tilde{R}[x]$, and hence h is in the ideal of f. Thus $ker(\varphi) \subset (f)$. The other inclusion is clear since every multiple of f must also have α as a root, and hence must be in the kernel.

We see from the definition of $\tilde{R}[\alpha]$ that φ is surjective, so if we factor this homomorphism through the kernel, we get an isomorphism $\phi : \tilde{R}[x]/(f) \to \tilde{R}[\alpha]$. Note that $\tilde{R}[x]/(f)$ is an extension of $\tilde{R}$, and that ϕ restricted to $\tilde{R}$ is the identity.

Now, we construct K' and $\tilde{\omega}$. First, let g' be an irreducible factor of f', and then take the natural projection homomorphism $\rho : F'[x] \to F'[x]/(g')$. If $\hat{\omega} : \tilde{R}[x] \to F'[x]$ is the homomorphism applying ω to the coefficients of polynomials in $\tilde{R}[x]$, then we can then factor the homomorphism $\rho \circ \hat{\omega}$ through the ideal generated by f in $\tilde{R}[x]$, giving us a homomorphism $\gamma : \tilde{R}[x]/(f) \to F'[x]/(g')$. Note here that $\rho \circ \hat{\omega}$ restricts to ω on $\tilde{R}$, and factoring through (f) does not affect this, so γ is an extension of ω. Then let $K' := F'[x]/(g')$ and $\tilde{\omega} := \gamma \circ \phi^{-1}$. K' is a field extension

of F', and by what we noted before about ϕ and γ, $\tilde{\omega}$ must restrict to ω on $\tilde{R}$. The following diagram depicts the construction of $\tilde{\omega}$ and K':

$$\tilde{R}[A] = \tilde{R}[\alpha] \xrightarrow{\phi^{-1}} \tilde{R}[x]/(f) \xrightarrow{\gamma} F'[x]/(g') = K' \tag{3}$$

We wish to see that K' is generated by α'. First note that, by following the homomorphisms constructing it, $\tilde{\omega}$ takes α to $x \pmod{g'}$, which is trivially the root of g', and that adjoining any root of g' to F' gives us an extension isomorphic to K'. So K' is generated by α'.

Next we show that K'/F' is Galois. take $\hat{\tilde{\omega}} : \tilde{R}[A][y] \to F'[y]$ the homomorphism applying $\tilde{\omega}$ to the coefficients of polynomials in $\tilde{R}[A][y]$. Then we see that for $\alpha_1, \ldots, \alpha_n$ the conjugates of α, and $\alpha'_1, \ldots, \alpha'_n$ their images under $\tilde{\omega}$,

$$f' := \hat{\tilde{\omega}}(f) = \hat{\tilde{\omega}}((y-\alpha_1)\cdots(y-\alpha_n)) = (y-\alpha'_1)\cdots(y-\alpha'_n). \tag{4}$$

We showed before that f' is separable, and we know that adjoining $\alpha'_1, \ldots, \alpha'_n$ to F' gives us K', since all of these roots are trivially in K' and one of them is α', a generator of K'. Hence K' is the splitting field of f', and so it is Galois.

Next, we want to show that when f' is irreducible(i.e., when $g' = f'$), we have that $\tilde{\omega}$ induces an isomorphism between the Galois groups G and G'. To define the isomorphism, note first that there is a unique automorphism $\sigma_i \in G$ taking α to one of its conjugates α_i. We know there is such an automorphism by definition of conjugates, and we know it is unique because the size of the Galois group G is n, the number of distinct roots of f. Likewise, since f' is now irreducible, we have that the degree of K'/F' is the degree of f', and since $\alpha'_1, \ldots, \alpha'_n$ are the distinct roots of f'(which we see by (4) and the fact that f' is separable), there are also unique automorphisms σ'_i taking α' to α'_i. Then we define our isomorphism as the map taking σ_i to σ'_i.

So now we wish to prove that this actually is an isomorphism. In order to do so, we must first show the identity $\tilde{\omega}(\sigma(s)) = \sigma'(\tilde{\omega}(s))$ where s is some element of $\tilde{R}[A]$. Since $\tilde{R}[A]$ is generated by $\tilde{R}$ and α, and $\tilde{\omega}\sigma$ and $\sigma'\tilde{\omega}$ are homomorphisms, we only need to show that the identity holds for α and elements of $\tilde{R}$. We have that σ and σ' are the identities on $\tilde{R}$ and F', respectively, and $\tilde{\omega}$ takes elements of $\tilde{R}$ to elements of F', so both sides of the identity reduce to $\tilde{\omega}(s)$ when $s \in \tilde{R}$. For $s = \alpha$, we see that if we replace σ and σ' with σ_i and σ'_i, respectively, then both sides evaluate to α'_i.

Given this identity, we see

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

so our map is a homomorphism. It is clearly a bijection since the map goes from a set of n distinct elements onto another set of n distinct elements.

□

3. A preliminary version of the theorem

Now that we have the basic tool we need to create the Galois extensions we want, we will apply it in part (1) of the following theorem to get a preliminary version of our final theorem. The rest of the paper will work toward defining hilbertian fields, determining some of their properties, and then generalizing part (1) of the following theorem for hilbertian fields.

Theorem 1. *Let K be a Galois extension of $F(x)$. $F(x)$ is the field of fractions of its subring $F[x]$, so take $f \in F[x][y]$ and $\alpha \in K$ given by proposition 1. Then we have the following facts:*

(1) For almost all $b \in F$, if $f_b(y) := f(b, y)$ is irreducible in $F[y]$, then for $K' := F[x]/(f_b)$, K'/F is Galois, and we have that $G := Gal(K/F(x))$ is isomorphic to $G' := Gal(K'/F)$.

(2) Let L/F be a finite extension, with $L \subset K$, and take $h \in L[x, y]$ an irreducible polynomial with all of its roots in K. Then for almost all $b \in F$, if $f_b(y)$ is irreducible in F[x], then $h_b(y) := h(b, y)$ is irreducible in L[x].

Proof. Part (1) is an application of the previous lemma. K is a Galois extension of $F(x)$, which is the field of fractions of the ring $F[x]$, so by the previous theorem, $\exists u \in F[x]$ such that if we look at the evaluation homomorphisms $\omega_b : F[x] \to F$, defined $\omega_b(g) = g(b)$, we get an isomorphism between the Galois groups $Gal(K/F(x))$ and $Gal(K'/F)$, where $K' := F[y]/(f_b)$, as long as $\omega_b(u) \neq 0$. Now $\omega_b(u) \neq 0$ for almost all b, since u is a single-variable polynomial, so part (1) follows.

Part (2) also employs the previous lemma, however it does so less directly. Once again, take $F[x]$, $F(x)$, and K to be the ring, it's field of fractions, and the Galois extension mentioned in the previous lemma, and again consider evaluation homomorphisms ω_b where b is not a root of $u(x) \in F[x]$. This time, however, we include in our set A two finite collections: the generators (and their conjugates) of L/F, and the roots $\beta_1, \ldots, \beta_m$ of h_x. Then by the previous lemma, for each b we consider, we can extend ω_b to $\tilde{\omega}_b$ from $F[x][A]$ to some K' Galois over F, and since we included the generators of L into A, our extension maps L isomorphically into K'(isomorphically, since any ring homomorphism from a field is either trivial or 1-1, and $\tilde{\omega}_b$ is not the trivial map on L since it is the identity on F). From now on, identify L with its isomorphic copy, so that $\tilde{\omega}_b$ is the identity on L and thus the evaluation homomorphism on $L(x)$(remember $\tilde{\omega}_b$ sends x to b).

Now, extend $\tilde{\omega}_b$ to $\hat{\tilde{\omega}}_b$ the homomorphism on $F[x][A][y]$ applying $\tilde{\omega}_b$ to coefficients, and apply this to h_x. We claim see that $\hat{\tilde{\omega}}_b(h_x)(y) = h_b(y)$, since as we just noted, $\tilde{\omega}_b$ is the evaluation homomorphism on the coefficients of h_x.

Now view h_x as a product of its linear factors:

$$h_x(y) = g_m(x)(y - \beta_1) \cdots (y - \beta_m).$$

Then for β_i' the images of the β_i under $\hat{\tilde{\omega}}_b$, we see from the fact stated in the previous paragraph that

$$h_b(y) = g_m(b)(y - \beta_1') \cdots (y - \beta_m').$$

Because $h_x(y)$ is irreducible (and therefore separable) in $L(x)[y]$ by Gauss's Lemma, $Gal(K/L(x))$ permutes the β_i transitively. Now assume that f_b is irreducible. Then we get by the previous lemma an isomorphism from $Gal(K/F(x))$ to $Gal(K'/F)$, which when restricted to $Gal(K/L(x))$ takes us to a subgroup of $Gal(K/L)$(since

for $z \in L$, $\sigma \in Gal(K/L(x))$, and σ' the corresponding automorphism, we see $\sigma'(z) = \sigma'(\tilde{\omega}_b(z)) = \tilde{\omega}_b(\sigma(z)) = \tilde{\omega}_b(z) = z$, i.e., σ' fixes L). If $\sigma \in Gal(K/L(x))$ takes β_i to β_j, and σ' is the corresponding automorphism in $Gal(K/L)$, then we see that

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

We know there is such a σ for any β_i and β_j since $Gal(K/L(x))$ permutes the roots of h_x transitively. Hence $Gal(K'/L)$ permutes the roots of h_b transitively. We exclude from our consideration the finitely many $b \in F$ such that h_b is not separable (i.e., the roots of $D(h) \in F(x)$, since $D(h_b) = D(h)(b)$), so that h_b is therefore irreducible.

□

4. The hilbertian property

Now we define a specific property for fields to have so that they will work well with part (1) of theorem 1, and have other nice properties as well:

Definition 1. A field F is called hilbertian, or is said to have the hilbertian property, if for any irreducible polynomial $f \in F[x, y]$, we have that for infinitely many $b \in F$, $f_b(y) := f(b, y)$ is irreducible in $F[y]$.

We see that if F is hilbertian, then we can apply part (1) of theorem 1, without having to worry about satisfying the antecedent of part (1), since it is already satisfied for infinitely many b by the hilbertian property.

Hilbert's Irreducibility Theorem is the statement that the specific field $\mathbb{Q}$ is hilbertian. We will not prove this theorem, but instead derive properties of hilbertian fields in general, so that we can see some of the consequences of the Irreducibility Theorem in the context of the Inverse Galois Problem.

First, we supply a powerful equivalent definition of the hilbertian property, which is where part (2) of theorem 1 comes in:

Proposition 3. *F is hilbertian iff for any finite extension L/F and irreducible polynomials $h_1, \ldots, h_k \in L[x, y]$, there are infinitely many $b \in F$ such that each $h_i(b, y)$ is irreducible as a polynomial in $L[y]$.*

Proof. Suppose F is hilbertian. Take irreducible polynomials $h_1, \ldots, h_k \in L[x][y]$. Then by Gauss's Lemma, these polynomials are also irreducible in $L(x)[y]$. Adjoining the roots of these polynomials gives us a finite extension M of $L(x)$, and hence also of $F(x)$. Then let K be the Galois closure of M over $F(x)$. We can find $f \in F[x, y]$ and $\alpha \in K$ given by proposition 3, and then we can apply part (2) of the previous theorem to any of the polynomials h_i to see that for almost all $b \in F$, if $f(b, y)$ is irreducible, then so is $h_i(b, y)$. Since these statements hold for almost all $b \in F$, we see that it is also the case that for almost all $b \in F$, if $f(b, y)$ is irreducible, then so is $h_i(b, y)$ for any i. Now, by the hilbertian property of F, there are infinitely many $b \in F$ such that $f(b, y)$ is irreducible, and hence there are infinitely many $b \in F$ such that $h_i(b, y)$ is irreducible for any i.

For the reverse direction, we set $L := F$, choose a single irreducible polynomial $f \in F[x, y]$, and then the hilbertian property comes immediately.

□

We want to start generalizing what we've found to polynomials in many variables, and in order to do so, a useful tool to have will be the Kronecker Specialization:

Definition 2. The Kronecker Specialization is a map $S_d : F[x_1, \ldots, x_k] \to F[x, y]$ defined as follows:

$$S_d(f)(x, y) = f(x, y, y^d, y^{d^2}, y^{d^3}, \ldots, y^{d^{k-2}})$$

This may appear at first to be somewhat arbitrary, but the following proposition shows why it is useful:

Proposition 4. *Let F be a field and define V_d to be the set of polynomials in $F[x_1, \ldots, x_k]$ of degree less than d in each variable $x_2, \ldots, x_k$. Also define W_d to be the set of polynomials in $F[x, y]$ to be the polynomials of degree less than d^{k-1} in y. Then S_d is a bijection between V_d and W_d. Furthermore, S_d is a ring homomorphism.*

Proof. That S_d is also a ring homomorphism is clear from the fact that it is a composition of evaluation homomorphisms.

Take $f \in V_d$ a monomial of the form $ax_1^{\alpha_1} \cdots x_k^{\alpha_k}$. Then S_d takes f to the monomial $ax^{\alpha_1} y^{\alpha_2 + \alpha_3 d + \alpha_4 d^2 + \cdots + \alpha_k d^{k-2}}$ in $F[x, y]$. Now by the uniqueness of base d integer representations, we see that S_d is a bijection between the monomials of V_d and W_d. From this bijection, it is easy to see that S_d is a bijection from V_d to W_d.

□

So we see that in the context of hilbertian fields, the Kronecker Specialization will give us information about polynomials of many variables, since we already have a nice property for polynomials in two variables, and the Kronecker Specialization provides a bridge between the two types of polynomials. We will use this in the following theorem, which shows that the hilbertian property extends in a sense to polynomials in many variables.

Theorem 2. *If F is hilbertian and $f \in F[x_1, \ldots, x_k]$ an irreducible polynomial, we have that there are infinitely many $b \in F$ such that $f(b, x_2, \ldots, x_k)$ is irreducible as a polynomial in $F[x_2, \ldots, x_k]$.*

Proof. To begin, take d greater than the degree of any variable $x_2, \ldots, x_k$ in f. We want to take the prime factorization of $S_d(f)$, and after taking this factorization, we will group all irreducible polynomials of degree 0 in the variable y into a polynomial $g(x)$. Then we get the following factorization of $S_d(f)$:

$$S_d(f)(x, y) = g(x) \prod_{i \in C} g_i(x, y) \tag{5}$$

where each g_i is an irreducible polynomial with positive degree in y. Then, by the hilbertian property of F, we see that for almost all $b \in F$, $g_i(b, y)$ is irreducible in $F[y]$. So consider only $b \in F$ such that this holds and such that $g(b) \neq 0$. Note that we are still considering all but finitely many possible $b \in F$ here, since g is a single-variable polynomial.

Now, specializing b into the variable x in (5) gives us a prime factorization of $S_d(b, y)$. Supposing $f_b := f(b, x_2, \ldots, x_k)$ is reducible, i.e., $f_b = hh'$, we have that

$$\begin{aligned} S_d(h)S_d(h') &= S_d(hh') \\ &= S_d(f_b) \\ &= S_d(f)(b, y) \\ &= g(b) \prod_{i \in C} g_i(b, y). \end{aligned}$$

So the prime factorizations of $S_d(h)$ and $S_d(h')$ partition the factorization of $S_d(f)(b, y)$, i.e., for $\{A, B\}$ a partition of C, and $uu' = g(b)$, we have

$$S_d(h) = u \prod_{i \in A} g_i(b, y) \text{ and } S_d(h') = u' \prod_{i \in B} g_i(b, y).$$

Then define $H(x, y)$ and $H'(x, y)$ as the polynomials corresponding to the $S_d(h)$ and $S_d(h')$ as follows:

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

H and H' are both in W_d, so there are unique $\tilde{h}$, $\tilde{h'} \in V_d$ such that $S_d(\tilde{h}) = H$, and $S_d(\tilde{h'}) = H'$. Now we want to consider the specialization of these two polynomials, $\tilde{h}_b := h(b, x_2, \ldots, x_k)$ and $\tilde{h}'_b := h'(b, x_2, \ldots, x_k)$. We see that

$$\begin{aligned} S_d(\tilde{h}_b) &= S_d(\tilde{h})(b, y) \\ &= H(b, y) \\ &= \prod_{i \in A} g_i(b, y) \\ &= u^{-1} S_d(h) \\ &= S_d(u^{-1}h), \end{aligned}$$

and thus $\tilde{h}_b = u^{-1}h$. Likewise, we find that $\tilde{h'}_b = u'^{-1}h'$. Thus

$$\tilde{h}_b \tilde{h}'_b = u^{-1}u'^{-1}hh' = g(b)^{-1} f_b. \tag{6}$$

Note that $\tilde{h}\tilde{h'}$ is not in V_d, since otherwise we see that

$$S_d(g\tilde{h}\tilde{h'}) = gS_d(\tilde{h})S_d(\tilde{h'}) = gHH' = S_d(f), \tag{7}$$

and then by the previous proposition, $g\tilde{h}\tilde{h'} = f$, contradicting the irreducibility of f.

By (6), we see that if we look at $\tilde{h}\tilde{h'}$ as a polynomial over $F[x_1]$, then b must be a root of the coefficients of every monomial where any of $x_2, \ldots, x_n$ has degree greater than $d - 1$, since f is in V_d but $\tilde{h}\tilde{h'}$ is not. But there are only finitely many possible such coefficients, since there are only finitely many possible factorizations gHH' of $S_d(f)$. So if we choose b outside this finite set, we get a contradiction. Thus f_b is irreducible for almost all b.

□

The following corollary shows how we can go further and specialize any number of variables in an irreducible polynomial $f \in F[x_1, \ldots, x_k]$ over a hilbertian field and still have an irreducible polynomial.

Corollary 1. *For F and f as in the previous theorem, we have that for any polynomial $p \in F[x_1, \ldots, x_{k-1}]$ that there are elements $b_1, \ldots, b_{k-1}$ in F such that $p(b_1, \ldots, b_{k-1}) \neq 0$ and $f(b_1, \ldots, b_{k-1}, x_k)$ is irreducible in $F[x_k]$.*

Proof. Take $f \in F[x_1, \ldots, x_k]$ irreducible. The theorem will follow from induction on the number of specialized variables. Our inductive hypothesis goes as follows: for any polynomial $p \in F[x_1, \ldots, x_n]$, there are $b_1, \ldots, b_n \in F$ such that $p(b_1, \ldots, b_n) \neq 0$ and $f(b_1, \ldots, b_n, x_{n+1}, \ldots, x_k)$ irreducible. The previous theorem proves the base case $n = 1$, so assume the hypothesis holds true for $n < k - 1$. Then take $p \in F[x_1, \ldots, x_{n+1}]$. By looking at p as a polynomial with coefficients in $F[x_{n+1}]$, we see that since each coefficient has finitely many roots, we can easily find $c \in F$ to specialize x_{n+1} so that $p(x_1, \ldots, x_n, c)$ is a nonzero polynomial in n variables. Then by the inductive hypothesis, we can find $b_1, \ldots, b_n$ such that $f(b_1, \ldots, b_n, x_{n+1}, \ldots, x_k)$ is irreducible. By the previous theorem, for almost all $b \in F$, $f(b_1, \ldots, b_n, b, x_{n+2}, \ldots, x_k)$ is irreducible, and since $p(b_1, \ldots, b_n, x_{n+1})$ is a single-variable polynomial, we know that for almost all $b \in F$, $p(b_1, \ldots, b_n, b) \neq 0$. So we can find a $b \in F$ satisfying both, thus proving the inductive hypothesis for $n + 1$.

□

Now, armed with theorem 2, we can show the following nice fact about hilbertian fields, which will help us in our generalization of part (1) of theorem 1:

Theorem 3. *Every finitely generated extension of a hilbertian field is hilbertian.*

Proof. First, we show the hilbertian property is preserved under finite extensions. To see this, let F be hilbertian and L a finite extension of F. Then for $f \in F[x, y]$ an irreducible polynomial, we have by theorem(x) that there are infinitely many $b \in F$(and hence in L) such that $f(b, y)$ is irreducible in $L[y]$. Hence L is hilbertian.

Next, we show the hilbertian property is preserved under purely transcendental extensions. To see this, take an irreducible polynomial $f \in F(x_1, \ldots, x_n)[x, y]$, and let subscripts denote specialization of x. Then $\exists g \in F(x_1, \ldots, x_n)$ such that gf is in $F[x_1, \ldots, x_n, x, y]$, so by theorem 2, there are infinitely many $b \in F$ (and hence in $F(x_1, \ldots, x_n)$) such that $(gf)_b$ is irreducible in $F[x_1, \ldots, x_n, y]$. By Gauss's Lemma, this must also be irreducible in $F(x_1, \ldots, x_n)[y]$. Now $(gf)_b = g_b f_b = g f_b$, and g is a unit in $F(x_1, \ldots, x_n)$, so f_b is irreducible in $F(x_1, \ldots, x_n)[y]$.

Every finitely generated extension can be made from a purely transcendental extension followed by a finite extension, so we have shown that every finitely generated extension of a hilbertian field is hilbertian.

□

5. The end result

Here, we can finally generalize the result of part (1) of theorem 1 for hilbertian fields:

Theorem 4. *If F is hilbertian, and K is a Galois extension of $F(x_1, \ldots, x_k)$, we have that $Gal(K/F(x_1, \ldots, x_k))$ is isomorphic to the Galois group given by some Galois extension K'/F*

Proof. We show this by induction on k. For $k = 1$, this follows from part (1) of theorem 1, and the fact that F is hilbertian. So suppose this is true for $k \geq 1$. Then let

K be a Galois extension of $F(x_1, \ldots, x_{k+1})$. By the previous theorem, $F(x_1, \ldots, x_k)$ is hilbertian, so by the base case we just proved, $Gal(K/F(x_1, \ldots, x_{k+1}))$ is isomorphic to some $Gal(K'/F(x_1, \ldots, x_k))$, and by the inductive hypothesis, this is isomorphic to some $Gal(K''/F)$.

□

So now, given Hilbert's Irreducibility Theorem that $\mathbb{Q}$ is hilbertian, we know that we can realize over $\mathbb{Q}$ any group realizable over one of its rational function fields.

References

[1] Helmut Völklein. Groups as Galois Groups. Cambridge University Press. 1996.
[2] David S. Dummit and Richard M. Foote. Abstract Algebra. John Wiley and Sons, Inc. 2004.