Representing finite groups as Galois groups over \mathbb{Q}

Conventions, Terminology, Notation.

- Fields are assumed to have characteristic 0.
- If k is a field, $k(x_1, \ldots, x_m)$ denotes an extension of k by algebraically independent elements x_1, \ldots, x_m ; i.e., $k(x_1, \ldots, x_m)$ is the field of fractions of the polynomial ring $k[x_1, \ldots, x_m]$. If m = 1, we write k(x) instead of $k(x_1)$.
- For a ring R, a subring S, and a subset A of R, S[A] is the subring of R generated by $S \cup A$.
- G(L/k) denotes the Galois group of a Galois (i.e., finite, normal, separable) extension L/k. A group G is said to occur as a Galois group over k if $G \cong G(L/k)$ for a Galois extension L/k.
- If $f(x,y) \in k[x,y]$ is considered as a polynomial in y, we may write $f_x(y)$ for f(x,y).

Definition. A field k is hilbertian if for every irreducible polynomial $f_x(y) \in k[x, y]$, there exist infinitely many elements $b \in k$ such that the specialization $f_b(y) := f(b, y)$ is irreducible in k[y].

Main Theorem on Hilbertian Fields. If k is a hilbertian field and a finite group G occurs as a Galois group over $k(x_1, \ldots, x_m)$ for some $m \ge 1$, then G occurs as a Galois group over k.

Hilbert's Irreducibility Theorem. \mathbb{Q} is hilbertian.

Corollary. S_n is a Galois group over \mathbb{Q} for every integer $n \geq 1$.

Proof of the Main Theorem

Theorem 1. Let L/k(x) be a Galois extension of degree n > 1.

- (1) There exist $\alpha \in L$ and $f(x, y) \in k[x, y]$ such that (i) $k(x)(\alpha) = k(x)[\alpha] = L$ and $f(x, \alpha) = 0$,
 - (ii) $f_x(y)$ is monic and irreducible of degree n over k(x) (or equivalently, over k[x]).
- (2) If $b \in k$ is such that $f_b(y) := f(b, y) \in k[y]$ is irreducible, then the following hold for the evaluation homomorphism $\omega \colon k[x] \to k, \ h(x) \mapsto h(b)$:
 - (i) ω extends to a homomorphism $\widetilde{\omega}$ of the subring $k[x][\alpha]$ of L onto the field $L' := k[y]/(f_b)$ in such a way that $\alpha' := \widetilde{\omega}(\alpha)$ is a root of f_b ; namely,

$$\widetilde{\omega} \colon k[x][\alpha] \to k[y]/(f_b) =: L',$$

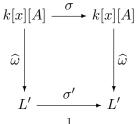
$$h(x, \alpha) \mapsto h(b, y) + (f_b) = h(b, \alpha').$$

- (ii) If A is a finite subset of L such that $\alpha \in A$ and A is invariant under G(L/k(x)), then
 - (a) there exists a nonzero polynomial $u(x) \in k[x]$ such that $u(x)a \in k[x][\alpha]$ for all $a \in A$;
 - (b) if $u(b) \neq 0$, then $\widetilde{\omega}$ extends further to a homomorphism

$$\widehat{\omega} \colon (k[x][A] \subseteq)k[x][\alpha][1/u(x)] \to L'$$

in such a way that $\widehat{\omega}(1/u(x)) = 1/\widetilde{\omega}(u(x)) = 1/u(b)$;

(c) L'/k is a Galois extension of degree |L':k| = n = |L:k(x)|, and there exists an isomorphism $G(L/k(x)) \to G(L'/k), \ \sigma \mapsto \sigma'$ such that the following diagram commutes for each $\sigma \in G(L/k(x))$:



Corollary 2. If k is a hilbertian field, then every finite group G that occurs as a Galois group over k(x), also occurs as a Galois group over k.

Theorem 3. Let L/k(x) be a Galois extension of degree n > 1, and let α and f satisfy conditions (i)-(ii) from Theorem 1 (1). If l/k is a finite extension with $l \subseteq L$, and $h_x(y) \in l[x, y]$ is irreducible over l(x) but splits over L, then for almost all (i.e., for all but finitely many) $b \in k$,

 $f_b(y) \in k[y]$ is irreducible $\implies h_b(y) \in l[y]$ is irreducible.

Corollary 4. The following conditions on a field k are equivalent:

- (a) k is hilbertian.
- (b) For every finite extension l/k and for arbitrary polynomials (h₁)_x(y),..., (h_m)_x(y) ∈ l[x, y] that are irreducible over l(x), there exist infinitely many b ∈ k such that the specialized polynomials (h₁)_b(y),..., (h_m)_b(y) are irreducible in l[y].

Corollary 5. Finite extensions of hilbertian fields are hilbertian.

Lemma 6. Let k be a hilbertian field, and let $f(x_1, \ldots, x_s) \in k[x_1, \ldots, x_s]$ have degree ≥ 1 in x_s $(s \geq 2)$. If $f(x_1, \ldots, x_s) \in k[x_1, \ldots, x_s]$ is irreducible, then there exist infinitely many $b \in k$ such that $f(b, x_2, \ldots, x_s) \in k[x_2, \ldots, s_s]$ is irreducible.

Theorem 7. Finitely generated extensions of hilbertian fields are hilbertian.

Proof of the Main Theorem. We have $k(x_1, \ldots, x_m) = k(x_1, \ldots, x_{m-1})(x_m)$, and $k(x_1, \ldots, x_{m-1})$ is hilbertian by Theorem 7. Therefore, by Corollary 2, if G is a Galois group over $k(x_1, \ldots, x_m)$, then it is also a Galois group over $k(x_1, \ldots, x_{m-1})$. Hence the claim follows by induction on m.