Artin's Theorem

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

In this file:

Notation-Lemma. For any field L and any subgroup H of $\mathrm{Aut}(L)$,

$$L^H \stackrel{\mathrm{def}}{=} \{a \in L : \sigma(a) = a, \ \forall\, \sigma \in H\}$$

is a sub-field of L, called the fixed field of H.

H-fixed subfield of L

Proof: Direct check:

Artin's Theorem: For any field L and any finite ~~group~~ sub-group H of $\mathrm{Aut}(L)$,

1. L is a Galois extension of L^H; : $|\mathrm{Aut}_{L^H}(L)| = |L : L^H|$
2. $\mathrm{Aut}_{L^H}(L) \overset{\supset}{=} H$.

Proof.

- Let $\alpha \in L$ be arbitrary, let $H\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, and define
$$f(x) = \prod_{i=1}^{n} (x - \alpha_i) \in L[x].$$
- The coefficients of $f(x)$, expressed as symmetric polynomials of $\alpha_1, \ldots, \alpha_n$, are in L^H. Thus $f(x) \in L^H[x]$.
- $f(\alpha) = 0$, so $\alpha \in L$ is algebraic over L^H.

Proof of Artin's Theorem continued:

- Let $p \in L^H[x]$ be the minimal polynomial of α in $L^H[x]$. Thus $p|f$.
- Since f has no repeated roots in L, p completely splits over L and has no repeated roots in L. Moreover,

$$|L^H(\alpha) : L^H| = \deg(p) \leq \deg f = n = |H\alpha| \leq |H|.$$

- Since $\alpha \in L$ is arbitrary, L is a normal and separable algebraic extension of L^H (but we do not yet know that $|L : L^H| < \infty$).
- Choose $\alpha \in L$ such that $|L^H(\alpha) : L^H|$ is the largest.

Proof of Artin's Theorem continued:

- Suppose that $L^H(\alpha) \neq L$. Choose $\beta \in L \backslash L^H(\alpha)$. Then $L^H(\alpha, \beta)$ is a finite separable extension of L^H. By the Primitive Element Theorem, $L^H(\alpha, \beta) = L^H(\gamma)$ for some $\gamma \in L$, contradicting the assumption on α. Thus $L^H(\alpha) = L$.

- By the basic lemma on automorphism groups of finite simple extensions, $L = L^H(\alpha)$ is Galois over L^H, and

$$|\mathrm{Aut}_{L^H}(L)| = |L : L^H| \leq |H|.$$

- As $H \subset \mathrm{Aut}_{L^H}(L)$ by definition, one thus has $\mathrm{Aut}_{L^H}(L) = H$.

Q.E.D.

Example: Let K be any field. For any integer $n \geq 1$, let

$$L = K(x_1, \ldots, x_n),$$

the fraction field of the polynomial ring $K[x_1, \ldots, x_n]$. The symmetric group S_n embeds into $\mathrm{Aut}(L)$ as a subgroup via action on L

$$(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}), \qquad \sigma \in S_n.$$

Applying Artin's Theorem, we conclude

- L is a (finite) Galois extension of L^{S_n} with Galois group S_n.
- For any subgroup $G \subset S_n$, L is a (finite) Galois extension of L^G with Galois group G.

Every finite group is the Galois group of some finite Galois extension!