CONSTRUCTING GENERIC POLYNOMIALS

ARNE LEDET

ABSTRACT. We construct a generic polynomial for A_4 over $\mathbb{Q}$.

INTRODUCTION

One problem in Inverse Galois Theory is that of describing Galois extensions with a given Galois group: If K is a field and G a finite group, what does a G-extension of K look like?

If we approach this problem analytically, by assuming we have a G-extension and trying to determine its structure, we are likely to end up with a description in terms of generating elements bearing some given algebraic relations to each other, ultimately expressed in terms of parameters from K. A convenient way of expressing this is by means of a *generic polynomial*:

Definition. A monic separable polynomial $P(\mathbf{s}, X) \in K(\mathbf{s})[X]$, where $\mathbf{s} = (t_1, \ldots, t_r)$ and X are indeterminates, is called *generic* for G over K, if it satisfies the following conditions:

(i) $\mathrm{Gal}(P/K(\mathbf{s})) \simeq G$, and
(ii) if M/L is a G-extension with $L \supseteq K$, M is the splitting field over K of a specialisation $P(\mathbf{a}, X)$ of $P(\mathbf{s}, X)$ at some point $\mathbf{a} = (a_1, \ldots, a_r) \in K^r$.

For instance, $X^2 - X - s \in K(s)[X]$ is generic for the cyclic group C_2 over any field K.

In this paper, we will produce a generic polynomial for the alternating group A_4 over the field $\mathbb{Q}$ of rational numbers. This polynomial is given in the Theorem in section 2. Prior to that, in section 1, we give various results, with or without proof, that are needed in our treatment of A_4.

1. NECESSARY PREREQUISITES

Let K be a field and V a finite-dimensional K-vector space. Then we denote by $K[V]$ the commutative tensor algebra for V, i.e., $K[V]$ is a polynomial ring over K in $n = \dim_K V$ indeterminates and we identify V with the space of homogeneous linear polynomials. The quotient

field of $K[V]$ is denotes $K(V)$. Thus, any K-basis for V is a generating transcendency basis (*rational generators*) for $K(V)/K$.

It is clear that if U is a subspace of V, we have $K(U)$ as a subfield of $K(V)$, and that $K(V)/K(U)$ is then a rational extension with any basis for a complement of U in V as rational generators. Also, any vector space automorphism on V extends to a field automorphism of $K(V)$. In particular, if the finite group G acts faithfully on V by linear transformations, we get a G-action on $K(V)$ and a G-extension $K(V)/K(V)^G$.

Our first important result is the following, from [K&Mt, Thm. 3]:

Proposition. *Let K be an infinite field and G a finite group. Consider a faithful linear action of G on the finite-dimensional K-vector space V, and assume that M/K is a subextension of $K(V)/K$ on which G acts faithfully. If the fixed field M^G is rational over K with generating transcendency basis $s_1, \ldots, s_r$, there is a generic G-polynomial over K with parameters $s_1, \ldots, s_r$. In fact, any monic polynomial in $M^G[X]$ with splitting field M is generic.*

We will not prove this Proposition, but refer to [K&Mt] for proof.

Using Kemper & Mattig's result, we can find generic polynomial by studying extensions of the form $K(V)/K(V)^G$. The most obvious question is of course whether $K(V)^G$ itself is a rational extension of K, the so-called *Noether Problem*. Here, a first step is the reduction to subrepresentations, by means of the *No-Name Lemma*:

The No-Name Lemma. *Let the finite group G act faithfully on the finite-dimensional K-vector space V, and let U be a G-closed subspace on which the restricted G-action is also faithful. Then the extension $K(V)^G/K(U)^G$ is rational.*

In other words: There is a set of G-invariant rational generators for $K(V)/K(U)$.

Proof. The $K(U)$-vector space $W = K(U) \cdot V$ generated by V inside $K(V)$ has a semi-linear G-action, i.e., $\sigma(aw) = \sigma a \, \sigma w$ for $a \in K(U)$ and $w \in W$. By the Invariant Basis Lemma (cf. e.g. [K&M]), any basis for the $K(U)^G$-vector space W^G of G-invariant elements is therefore also a $K(U)$-basis for W. If we pick such a basis $1, w_1, \ldots, w_s$, it is easy to see that $w_1, \ldots, w_s$ are rational generators for $K(V)/K(U)$, and hence also for $K(V)^G K(U)^G$. □

To take the reduction of the problem one step further, we make the following observations, cf. [Ke, Prop. 1.1(a)]: Let $G \hookrightarrow \mathrm{GL}_K(V)$

for a finite-dimensional K-vector space V. Then G acts on the subfield $K(V)_0$ of homogeneous elements of degree 0 through $\mathrm{PGL}_K(V)$. (A *homogeneous element* in $K(V)$ is an element of the form f/g, where $f, g \in K[V]$ are homogeneous. The *degree* is then $\deg f - \deg g$. It follows that the homogeneous elements of degree 0 constitute a subfield, and in fact that $K(V)_0 = K(v_2/v_1, \ldots, v_n/v_1)$, when $v_1, \ldots, v_n$ is a K-basis for V. The action of $\mathrm{GL}_K(V)$ on $K(V)$ becomes an action of $\mathrm{PGL}_K(V)$ on $K(V)_0$.) Clearly, $K(V)/K(V)_0$ is rational, but in fact the extension $K(V)^G/K(V)_0^G$ of fixed field is rational, generated by any homogeneous element in $K(V)^G$ of minimal positive degree. This is easily seen, once we note that $K(V)^G$ is generated by homogeneous elements.

For instance, if we start with a two-dimensional representation, this 'homogenisation' brings us down to transcendency degree 1, where everything is rational by Lüroth's Theorem (see e.g. [Ja, 8.14]). For convenience, we cite this result in the form we need:

Lüroth's Theorem. *Let K and L be fields with $K \subsetneq L \subseteq K(t)$, t and indeterminate. Then $K(t)/L$ is finite, and if r_i is a non-constant coefficient in the minimal polynomial $X^n + r_{n-1}X^{n-1} + \cdots + r_1X + r_0$ for t over L, then $L = K(r_i)$.*

Example. Let $C_3 = \langle\sigma\rangle$ act on $\mathbb{Q}(x, y, z)$ by $\sigma\colon x \mapsto y$, $y \mapsto z$, $z \mapsto x$.

With $s = x - y$ and $t = y - z$ we then get $\sigma\colon s \mapsto t$, $t \mapsto -s - t$, and using the above result we easily get that $\mathbb{Q}(s, t)^{C_3} = \mathbb{Q}(u, v)$ for

$$u = \frac{s^2 + t^2 + st}{st(s + t)} \quad \text{and} \quad v = \frac{s^3 - 3st^2 - t^3}{st(s + t)},$$

and also that

$$\mathbb{Q}(x, y, z)^{C_3} = \mathbb{Q}\Big(\frac{(x-y)^2 + (y-z)^2 + (x-y)(y-z)}{(x-y)(y-z)(x-z)}, \frac{(x-y)^3 - 3(x-y)(y-z)^2 - (y-z)^3}{(x-y)(y-z)(x-z)}, x + y + z\Big).$$

Thus, these two Noether Problems have affirmative answers.

For use below, we record the following consequence of the above example: Notice that the generators for $\mathbb{Q}(x, y, z)^{C_3}$ are homogeneous of degrees -1, 0 and 1. If we call them X, Y and Z for convenience, we thus have $\mathbb{Q}(x, y, z)^{C_3} = \mathbb{Q}(X, Y, Z) = \mathbb{Q}(XZ, Y)(Z)$, from which it follows that $\mathbb{Q}(x, y, z)_0^{C_3} = \mathbb{Q}(XZ, Y)$: '$\supseteq$' is obvious, and since $\mathbb{Q}(x, y, z)^{C_3}$ is rational over both fields of transcendency degree 1, we get equality. (Cf. also [Ke, Prop. 1.1(b) + proof].)

Now, $\mathbb{Q}(x,y,z)_0 = \mathbb{Q}(s,t)$, where $s = x/y$ and $t = y/z$, and on this field σ acts by $s \mapsto t$, $t \mapsto 1/st$.

Thus, we can conclude the following: Let σ be the automorphism on the rational function field $\mathbb{Q}(s,t)$ given by $\sigma\colon s \mapsto t$, $t \mapsto 1/st$. Then σ has order 3, and the fixed field $\mathbb{Q}(s,t)^{C_3}$ is rational over $\mathbb{Q}$. More precisely,

$$\mathbb{Q}(s,t)^{C_3} = \mathbb{Q}\Bigg(\frac{s^3t^3 - 3st^2 + t^3 + 1}{t(s-1)(t-1)(st-1)}, \frac{s^3t^3 - 3s^2t^3 + 6st^2 - 3st + t^3 - 3t^2 + 1}{t(s-1)(t-1)(st-1)}\Bigg).$$

2. The alternating group A_4

We find a generic polynomial for A_4 over $\mathbb{Q}$ by proceeding in several steps:

(1) There is a linear action of A_4 on $\mathbb{Q}^3$, obtained by considering S_4 as the rotation group of the cube. If we write

$$A_4 = \left\langle \sigma, \rho_1, \rho_2 \mid \sigma^3 = \rho_1^2 = 1,\ \sigma\rho_1\sigma^{-1} = \rho_2,\ \sigma\rho_2\sigma^{-1} = \rho_1\rho_2 = \rho_2\rho_1 \right\rangle,$$

this gives us an A_4-action on $\mathbb{Q}(x,y,z)$ given by

$$\begin{aligned} \sigma\colon x \mapsto y, &\quad y \mapsto z, &\quad z \mapsto x, \\ \rho_1\colon x \mapsto -x, &\quad y \mapsto -y, &\quad z \mapsto z. \end{aligned}$$

(2) Stepping down to the homogeneous degree-0 part $\mathbb{Q}(x,y,z)_0 = \mathbb{Q}(s,t)$, $s = x/y$, $t = y/z$, we have

$$\sigma\colon s \mapsto t, \quad t \mapsto 1/st, \quad \text{and} \quad \rho_1\colon s \mapsto s, \quad t \mapsto -t.$$

(Also, $\mathbb{Q}(x,y,z)^{A_4}/\mathbb{Q}(s,t)^{A_4}$ is rational of transcendency degree 1, generated by $xyz/(x^2+y^2+z^2)$.) Clearly, $\mathbb{Q}(s,t)^{V_4} = \mathbb{Q}(s^2,t^2)$, and so we are left with the extension $\mathbb{Q}(s^2,t^2)/\mathbb{Q}(s^2,t^2)^{C_3}$ for $C_3 = \langle\sigma\rangle$.

(3) Letting $u = s^2$ and $v = t^2$, we now ask: If $C_3 = \langle\sigma\rangle$ acts on $\mathbb{Q}(u,v)$ by $\sigma\colon u \mapsto v$, $v \mapsto 1/uv$, is $\mathbb{Q}(u,v)^{C_3}/\mathbb{Q}$ rational? From the Example in section 1, we know that the answer is 'yes', and that in fact

$$\mathbb{Q}(u,v)^{C_3} = \mathbb{Q}\Bigg(\frac{u^3v^3 - 3uv^2 + v^3 + 1}{v(u-1)(v-1)(uv-1)}, \frac{u^3v^3 - 3u^2v^3 + 6uv^2 - 3uv + v^3 - 3v^2 + 1}{v(u-1)(v-1)(uv-1)}\Bigg).$$

(4) All in all: $\mathbb{Q}(s,t)/\mathbb{Q}(s,t)^{A_4}$ is an extension of rational function fields, sitting inside our 'Noether Extension'. Thus, this Noether Problem has a positive answer for A_4, and there is a generic A_4-polynomial with two parameters over $\mathbb{Q}$.

(5) By theProposition in section 1, we can now find a generic polynomial for A_4 over $\mathbb{Q}$ by expressing the minimal polynomial for, say, $s+t+1/st$ over $\mathbb{Q}(s,t)^{A_4}$ in terms of the generators found above. Denoting these generators by α and β, resp., we thus get

Theorem. *The polynomial*

$$F(\alpha,\beta,X) = X^4 - \frac{6A}{B}X^2 - 8X + \frac{9A^2 - 12(\alpha^3-\beta^3+27)B}{B^2}$$

in $\mathbb{Q}(\alpha,\beta)[X]$, *where*

$$A = \alpha^3 - \beta^3 - 9\beta^2 - 27\beta - 54,$$
$$B = \alpha^3 - 3\alpha\beta^2 + 2\beta^3 - 9\alpha\beta + 9\beta^2 - 27\alpha + 27\beta + 27,$$

is generic for A_4 *over* $\mathbb{Q}$.

Remark. Finding the polynomial in the Theorem is basically linear algebra, and was done using MAPLE V.

References

[Ja] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, New York, 1989.

[Ke] G. Kemper, *A constructive approach to Noether's Problem*, Manuscripta Math. **90** (1996), 343–363.

[K&M] G. Kemper & G. Malle, *Invariant fields of finite irreducible reflection groups*, Math. Ann. **315** (1999), 569–586.

[K&Mt] G. Kemper & E. Mattig, *Generic polynomials with few parameters*, J. Symbolic Computation **30** (2000), 843–857.