

Two Computations of Galois Groups

Muye

August 26, 2026

We compute two nontrivial Galois groups that appear among the exercises in Nathan Jacobson's *Basic Algebra*. Let F_0 be a field of characteristic $p > 0$, let s, t be algebraically independent over F_0 , and put $F = F_0(s, t)$. The results are due to Kôji Uchida [1].

1 The affine linear group

Problem 1.1 (Uchida). The Galois group over F of

$$x^p - sx - t \tag{1}$$

is isomorphic to the group of transformations

$$x \mapsto ax + b, \quad a, b \in \mathbb{F}_p, \text{quad } a \neq 0.$$

Equivalently, it is $\mathbb{F}_p \rtimes \mathbb{F}_p^\times$, where $\mathbb{F}_p^\times$ acts on the additive group of $\mathbb{F}_p$ by scalar multiplication.

Proof. We begin by computing the degree of the splitting field L of (1). By Gauss's lemma, it is enough to prove irreducibility in $F_0[s, t][x]$. Since

$$F_0[s, t][x] = F_0[s, x][t],$$

the polynomial is linear and primitive as a polynomial in t , hence has no nontrivial factorization.

If α is a root, therefore,

$$[F(\alpha) : F] = p. \tag{2}$$

Let β be another root and set $\zeta = \beta - \alpha$. Subtracting the two equations gives

$$\zeta^{p-1} = s. \quad (3)$$

The same linear-in- s argument shows that $X^{p-1} - s$ is irreducible over $F(\alpha)$, so

$$[F(\alpha, \zeta) : F(\alpha)] = p - 1. \quad (4)$$

Because F_0 contains its prime field $\mathbb{F}_p$, the elements $k\zeta, k \in \mathbb{F}_p^\times$, are all the nonzero roots of $X^{p-1} - s$. Moreover,

$$(\alpha + k\zeta)^p - s(\alpha + k\zeta) - t = 0 \quad (k \in \mathbb{F}_p).$$

Thus the roots of (1) are precisely $\alpha + k\zeta$, and

$$L = F(\alpha, \zeta), \quad [L : F] = p(p - 1). \quad (5)$$

Let $G = \text{Gal}(L/F)$. Identify the root $\alpha + k\zeta$ with $k \in \mathbb{F}_p$. If $\tau \in G$, write

$$\tau(\alpha) = \alpha + b\zeta, \quad \tau(\zeta) = a\zeta,$$

where $b \in \mathbb{F}_p$ and $a \in \mathbb{F}_p^\times$. Then

$$\tau(\alpha + k\zeta) = \alpha + (ak + b)\zeta. \quad (6)$$

The induced action on the roots is therefore the affine map $k \mapsto ak + b$. The action of a Galois group on all roots of a separable polynomial is faithful, so this gives an injection

$$G \hookrightarrow \text{AGL}_1(\mathbb{F}_p) \cong \mathbb{F}_p \rtimes \mathbb{F}_p^\times.$$

Both groups have order $p(p - 1)$ by (5); the injection is an isomorphism. □

2 The projective linear group

Problem 2.1 (Uchida). The Galois group over F of

$$x^{p+1} - sx - t \quad (7)$$

is isomorphic to the group of fractional linear transformations

$$x \mapsto \frac{ax + b}{cx + d}, \quad a, b, c, d \in \mathbb{F}_p, \text{quad} ad - bc \neq 0;$$

that is, it is isomorphic to $\text{PGL}_2(\mathbb{F}_p)$.

Proof. We again begin with the splitting-field degree. The same Gauss-lemma argument used above shows that (7) is irreducible. Hence, for any root α ,

$$[F(\alpha) : F] = p + 1. \quad (8)$$

Let $\beta \neq \alpha$ be a second root. Dividing the difference of the two equations by $\beta - \alpha$ gives

$$\frac{\beta^{p+1} - \alpha^{p+1}}{\beta - \alpha} - s = 0. \quad (9)$$

As a polynomial in β , the left-hand side has degree p . The same primitive, linear-in- s argument proves its irreducibility over $F(\alpha)$, and therefore

$$[F(\alpha, \beta) : F(\alpha)] = p. \quad (10)$$

Let γ be a third root. From

$$s = \frac{\alpha^{p+1} - t}{\alpha} = \frac{\gamma^{p+1} - t}{\gamma}$$

we obtain, in characteristic p ,

$$\alpha\gamma(\gamma - \alpha)^{p-1} + t = 0. \quad (11)$$

The same relation holds with α replaced by any root different from γ . In particular,

$$\alpha\gamma(\gamma - \alpha)^{p-1} = \beta\gamma(\gamma - \beta)^{p-1},$$

and hence

$$\left(\frac{\gamma - \beta}{\gamma - \alpha}\right)^{p-1} = \frac{\alpha}{\beta}. \quad (12)$$

Put

$$u = \frac{\gamma - \beta}{\gamma - \alpha}. \quad (13)$$

For every root $\delta \neq \alpha, \beta$, the analogous cross ratio

$$K_\delta = \frac{\delta - \beta}{\delta - \alpha}$$

also satisfies (12). Consequently the values K_δ/u run through $\mathbb{F}_p^\times$, while $K_\beta = 0$ and we interpret $K_\alpha = \infty$. Solving for δ gives

$$\delta = \frac{K_\delta \alpha - \beta}{K_\delta - 1}. \quad (14)$$

It follows that

$$L = F(\alpha, \beta, u). \quad (15)$$

The polynomial $\beta X^{p-1} - \alpha$ is irreducible over $F(\alpha, \beta)$ by the same generic-parameter argument, so (8), (10), and (15) yield

$$[L : F] = (p+1)p(p-1). \quad (16)$$

We now identify the action. Fix the three roots α, β, γ and define

$$f(\delta) = \frac{K_\delta}{K_\gamma} = \frac{(\delta - \beta)(\gamma - \alpha)}{(\delta - \alpha)(\gamma - \beta)}. \quad (17)$$

Then

$$f(\alpha) = \infty, \quad f(\beta) = 0, \quad f(\gamma) = 1,$$

and Equation (12) identifies the $p+1$ roots bijectively with $\mathbb{P}^1(\mathbb{F}_p)$.

For $\tau \in G$, the induced permutation

$$\sigma = f \circ \tau \circ f^{-1}$$

is determined by the three distinct values

$$x_1 = \sigma(\infty), \quad x_2 = \sigma(0), \quad x_3 = \sigma(1).$$

The unique fractional linear transformation with these values is

$$\Sigma(k) = \frac{x_1(x_2 - x_3)k - x_2(x_1 - x_3)}{(x_2 - x_3)k - (x_1 - x_3)}. \quad (18)$$

Indeed, substitution gives $\Sigma(\infty) = x_1$, $\Sigma(0) = x_2$, and $\Sigma(1) = x_3$. Its determinant is

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \neq 0,$$

so $\Sigma \in \mathrm{PGL}_2(\mathbb{F}_p)$. Cross ratios are preserved by fractional linear transformations, and the definition (17) therefore gives $\sigma = \Sigma$ on all roots.

We have obtained an injective homomorphism

$$G \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_p).$$

Finally,

$$|\mathrm{PGL}_2(\mathbb{F}_p)| = (p+1)p(p-1) = [L : F]$$

by (16), so this homomorphism is an isomorphism. □

3 Remarks on Uchida's general result

Rmk. 3.1. Uchida studied the Galois group of the general trinomial $X^n - aX + b$ in [1]. In characteristic zero the generic group is $\mathfrak{S}_n$; the same conclusion holds in characteristic p when $p \nmid n(n-1)$. The exceptional cases $n = p^m$ and $n = p^m + 1$ generalize ?? 1.1?? 2.1: the coefficients a, b in the affine or projective transformations range over $\mathbb{F}_{p^m}$, together with the field automorphisms of $\mathbb{F}_{p^m}$ that fix its intersection with the ground field. When $m = 1$, the latter automorphism is necessarily the identity.

Uchida's paper states the relevant extension degrees very tersely and writes down a projective matrix for the second action directly. The calculation above instead uses the normalized cross-ratio coordinate (17); this makes both the occurrence of $\mathbb{P}^1(\mathbb{F}_p)$ and the formula (18) transparent.

References

- [1] K. Uchida, Galois group of an equation $X^n - aX + b = 0$, *Tohoku Math. J. (2)* **22** (1970), no. 4, 670–678, doi:10.2748/tmj/1178242731.