GALOIS GROUPS OVER Q AND FACTORIZATIONS MOD p

KEITH CONRAD

For a monic irreducible polynomial $f(T)$ in $\mathbf{Z}[T]$ of degree n, let K be its splitting field over $\mathbf{Q}$. Writing the roots of $f(T)$ as $\alpha_1, \ldots, \alpha_n$, each element of $\mathrm{Gal}(K/\mathbf{Q})$ is determined by how it permutes the n roots of $f(T)$, and this embeds $\mathrm{Gal}(K/\mathbf{Q})$ into S_n.[1]

The following striking theorem of Dedekind tells us cycle types of elements of $\mathrm{Gal}(K/\mathbf{Q})$ as a permutation of the roots of $f(T)$ by how $f(T)$ factors modulo primes.

Theorem 1 (Dedekind)**.** *Let f and K be as above. For each prime p where $p \nmid \operatorname{disc} f$, let*

$$f(T) \equiv \pi_1(T) \cdots \pi_k(T) \bmod p, \tag{1}$$

where the $\pi_j(T)$'s are distinct monic irreducibles in $\mathbf{F}_p[T]$. There is a σ in $\mathrm{Gal}(K/\mathbf{Q})$ that permutes the roots of $f(T)$ in K with cycle type $(d_1, d_2, \ldots, d_k)$, where $d_j = \deg \pi_j$ for all j.

This is easier to use than to prove. For some uses, see both https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf or https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisSnAn.pdf. To prove the theorem, we'll use algebraic number theory (Frobenius elements of prime ideals).

Proof. Let $\mathfrak{p}$ be a prime ideal over p in K. We'll show p is unramified in K and the Frobenius element $\mathrm{Fr}(\mathfrak{p}|p)$ in $\mathrm{Gal}(K/\mathbf{Q})$ permutes the roots of $f(T)$ with the desired cycle type.

Since $p \nmid \operatorname{disc} f$, p is unramified in $\mathbf{Q}(\alpha_1)$, so p is also unramified in the Galois closure of $\mathbf{Q}(\alpha_1)$ over $\mathbf{Q}$, which is K. Thus $\mathrm{Fr}(\mathfrak{p}|p)$ is a uniquely defined element of $\mathrm{Gal}(K/\mathbf{Q})$.

Reducing the factorization $f(T) = (T - \alpha_1) \cdots (T - \alpha_n)$ in $\mathcal{O}_K[T]$ modulo the ideal $\mathfrak{p}$,

$$\overline{f}(T) = (T - \overline{\alpha}_1) \cdots (T - \overline{\alpha}_n) \text{ in } (\mathcal{O}_K/\mathfrak{p})[T]. \tag{2}$$

Since $p \nmid \operatorname{disc} f$ we know $f(T) \bmod p$ is separable, so the reductions $\overline{\alpha}_i$ are distinct. Comparing (1) in $\mathbf{F}_p[T]$ and (2) in the larger ring $(\mathcal{O}_K/\mathfrak{p})[T]$, the reductions $\overline{\alpha}_i$ are the roots of $\overline{\pi}_1(T), \ldots, \overline{\pi}_k(T)$ in $\mathcal{O}_K/\mathfrak{p}$ in some order with no repetitions.

Let $\overline{\pi}_1(T)$ have a root $\overline{\alpha}_i$. By the theory of finite fields, if γ is one root of an irreducible in $\mathbf{F}_p[T]$ of degree d, then all the roots are iterated pth powers $\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{d-1}}$. Thus the roots of $\overline{\pi}_1(T)$ are $\overline{\alpha}_i, \overline{\alpha}_i^p, \ldots, \overline{\alpha}_i^{p^{d_1-1}}$, and $\overline{\alpha}_i^{p^{d_1}} = \overline{\alpha}_i$. The effect of $\varphi := \mathrm{Fr}(\mathfrak{p}|p)$ on $\mathcal{O}_K/\mathfrak{p}$ is to act as the pth power, so we can rewrite the roots of $\overline{\pi}_1(T)$ as $\overline{\alpha}_i, \overline{\varphi(\alpha_i)}, \ldots, \overline{\varphi^{d_1-1}(\alpha_i)}$, and $\overline{\varphi^{d_1}(\alpha_i)} = \overline{\alpha}_i$. Since distinct roots of $f(T)$ stay distinct mod $\mathfrak{p}$, $\varphi^{d_1}(\alpha_i) = \alpha_i$ in K and no smaller iterate of φ can fix α_i. Thus φ *acts as a d_1-cycle* on the roots of $f(T)$ that reduce mod $\mathfrak{p}$ to roots of $\overline{\pi}_1(T)$.

We can apply the same argument to the roots of $f(T)$ that reduce mod $\mathfrak{p}$ to roots of each of the other polynomials $\overline{\pi}_2(T), \ldots, \overline{\pi}_k(T)$: the roots of $f(T)$ that reduce mod $\mathfrak{p}$ to the roots of $\overline{\pi}_j(T)$ are permuted by $\mathrm{Fr}(\mathfrak{p}|p)$ as a d_j-cycle. Different $\overline{\pi}_j(T)$ have different roots since $\overline{f}(T)$ is separable, so $\mathrm{Fr}(\mathfrak{p}|p)$ acts on the roots of $f(T)$ with cycle type $(d_1, d_2, \ldots, d_k)$. ◻

[1] Changing the indexing of the roots will change this embedding by conjugation in S_n, so $\mathrm{Gal}(K/\mathbf{Q})$ as a subgroup of S_n is well-defined *up to conjugation.*