Tate's Proof of a Theorem of Dedekind

Let $f \in \mathbb{Z}[X]$ be a monic polynomial with integer coefficients and let $E_f = \mathbb{Q}(x_1, x_2, \ldots, x_n)$ be its splitting field over $\mathbb{Q}$, where $f = (X - x_1)(X - x_2) \cdots (X - x_n)$. Let $G_f = \mathrm{Gal}(E_f/\mathbb{Q})$ be the Galois group of f. Suppose that p is a prime such that p does not divide the discriminant Δ_f of f, in particular, we suppose that the roots of f are simple. Let $\bar{f}$ be the reduction of f modulo p. Then the roots of $\bar{f}$ are also simple. Let $A_f = \mathbb{Z}[x_1, \cdots, x_n]$ and let P be a prime ideal of A_f such that $P \cap \mathbb{Z} = p\mathbb{Z}$. Such an ideal exists since the fact that A_f is integral over $\mathbb{Z}$ implies that p is not invertible in A_f; moreover, this ideal is maximal since $P \cap \mathbb{Z}$ is maximal in $\mathbb{Z}$.

Theorem 1 (Dedekind). *There exists a unique element $\sigma_P \in G_f$ such that $\sigma_P(x) \equiv x^p \mod P$ for every $x \in A_f$. Moreover, if $\bar{f} = g_1 g_2 \cdots g_s$ with g_i irreducible over $\mathbb{F}_p$ of degree n_i, then σ_P, when viewed as a permutation of the roots of f, has a cycle decomposition $\sigma_1 \sigma_2 \cdots \sigma_s$ with σ_i of length n_i.*

Proof. (**due to John Tate**) The field $E_{\bar{f}} = A_f/P = \mathbb{F}_p[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n]$ is a splitting field for $\bar{f}$, where $\bar{x}$ is the residue class of x modulo P. The group $G_{\bar{f}} = \mathrm{Gal}(E_{\bar{f}}/\mathbb{F}_p)$ is cyclic generated by the automorphism $\bar{x} \mapsto \bar{x}^p$. Let $D_P = \{\sigma \in G_f \mid \sigma(P) = P\}$. This is a subgroup of G_f called the decomposition group at P. Every automorphism $\sigma \in D_P$ induces an automorphism $\bar{\sigma} \in G_{\bar{f}} = \mathrm{Gal}(E_{\bar{f}})$, where $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)}$. The homomorphism $\phi : D_P \to G_{\bar{f}}$ sending σ to $\bar{\sigma}$ is injective. We now show that it is surjective by showing that the fixed field of $\phi(D_P)$ has $\mathbb{F}_p$ as its fixed field.

Let $a \in A_f$. Then, by the Chinese Remainder Theorem, there an element $x \in A_f$ such that $x \equiv a \bmod P$ and $x \equiv 0 \bmod \sigma^{-1}(P)$ for all $\sigma \in G_f, \sigma \notin D_P$. Then $g = \prod_{\sigma \in G_f}(X - \sigma(x) \in \mathbb{Z}[X]$ and $\bar{g} = X^m \prod_{\sigma \in D_P}(X - \bar{\sigma}(\bar{a})) \in \mathbb{F}_p[X]$. It follows that the conjugates of $\bar{a}$ are all of the form $\bar{\sigma}(\bar{a})$ which implies that the fixed field of $\phi(D_P)$ is $\mathbb{F}_p$.

Let $\sigma_P \in D_P$ be the unique element such that $\bar{\sigma}_P(\bar{x}) = \bar{x}^p$. Then σ_P is the unique element of G_f such that $\sigma_P(x) \equiv x^p$ for every $x \in A_f$. Since the homomorphism $x \mapsto \bar{x}$ maps the roots of f bijectively onto the roots of $\bar{f}$ we see that the groups D_P and $G_{\bar{f}}$, when viewed as permutation groups of the roots of $f, \bar{f}$ respectively, are also isomorphic as permutation groups. Since the cycle decompostion of $\bar{\sigma}$ is determined by the orbits of the action of $G_{\bar{f}}$ on the roots of $\bar{f}$ and since the group $G_{\bar{f}}$ acts transitively on the roots of each polynomial g_i, we obtain the stated cycle decomposition of σ_P. □

If R_f is the ring of integers of E_f, i.e., the elements of E_f which are integral over $\mathbb{Z}$ and Q is a prime ideal of R_f such that $Q \cap \mathbb{Z} = p\mathbb{Z}$ then, as above, one can prove the existence of a unique automorphism $s_Q \in G_f$ such that $s_Q(x) \equiv x^p \pmod{Q}$ for all $x \in R_f$. This automorphism is called the Frobenius automorphism at Q. Since the elements of G_f are uniquely determined by their restriction to A_f, we see that $s_Q = \sigma_P$, where $P = Q \cap A_f$. If Q' is any ideal of R_f such that $Q' \cap \mathbb{Z} = Q \cap \mathbb{Z}$ and $x \in Q'$ then $\prod_{\sigma \in G_f} \sigma(x) \in Q' \cap \mathbb{Z} \subseteq Q$ which shows that $\sigma(x) \in Q$ for some $\sigma \in G_f$. Hence $Q' \subseteq \bigcup_{\sigma \in G_f} \sigma(Q)$. By the following Lemma, we have $Q' \subseteq \sigma(Q)$ and hence $Q' = \sigma(Q)$ for some $\sigma \in G_f$ Since $D_{\sigma(Q)} = \sigma D_Q \sigma^{-1}$, it follows that $s_{Q'} = \sigma Q \sigma^{-1}$. Thus two Frobenius automorphisms at primes over the same prime p of $\mathbb{Z}$ are conjugate. The conjugacy class of s_Q is called the Frobenius class at p. If G is abelian, this class reduces to a single element called the Frobenius automorphism at p.

Lemma 2. *Let I be an ideal of a ring A which is contained in the union of prime the ideals $P_1, P_2, \ldots, P_n$ of A. Then $I \subseteq P_i$ for some i.*

Proof. Assume the theorem is false and let n be smallest for which the lemma fails. Then $n > 1$ and $P_i \not\subseteq P_i$ for $i \neq j$. Moreover, I is not contained in the union of fewer prime ideals P_i. Then, since $I \subseteq \bigcup P_i \iff I = \bigcup I \cap P_i$, we see that $I \cap P_i \nsubseteq P_j$ for $i \neq j$. Let $x_{ij} \in I \cap P_i,\ x_{ij} \notin P_j$ for all $i \neq j$ and let $x_j = \prod_{i \neq j} x_{ij}$. Then $x_j \in I \cap P_i$ for $i \neq j$ but $x_j \notin P_j$ since P_j is prime. Let $x = \sum x_j$. Then $x \in I$ but $x \notin P_j$ for any j since $x_j = x - \sum_{i \neq j} x_i \in P_j$ and $\sum_{i \neq j} x_i \in P_j$. This contradicts the fact that I is contained in the union of the prime ideals P_i. $\square$

As an application of Dedekind's Theorem we give a proof of the irreducibility of of the cyclotomic polynomials over $\mathbb{Q}$.

Theorem 3. *The cyclotomic polynomials are irreducible over* $\mathbb{Q}$.

Proof. Let E be the splitting field of $X^n - 1$ over $\mathbb{Q}$ and let G be the galois group of E over Q. We have an injective homomorphism $\pi : G \to (\mathbb{Z}/n\mathbb{Z})^\times$, where $\sigma(\zeta) = \zeta^{\pi(\sigma)}$ for any n-th root of unity ζ. This homomorphism is surjective if and only if the the n-th cyclotomic polynomial Φ_n is irreducible. This is due to the fact that, for any primitive n-th root ζ_n, we have $E = \mathbb{Q}(\zeta_n)$, $\Phi_n(\zeta_n) = 0$ and degree$(\Phi_n) = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. If p is any prime not dividing n, the reduction of $X^n - 1$ mod p has simple roots. Let σ_p be the Frobenius autopmorphism at p. Then, for any n-th root of unity ζ, we have $\sigma(\zeta) = \zeta^p$ since ζ^p is also an n-th root of unity. Hence $\pi(\sigma_p) = p \mod n$. But $(\mathbb{Z}/n\mathbb{Z})^\times$ is generated by the residue classes of the primes p which do not divide n. Hence π is surjective. $\square$

As another application of Dedekind's Theorem let us find a monic polynomial of degree 5 with integer coeficients whose Galois group over Q is S_5. Our construction is based on the following Lemma:

Lemma 4. *If p is prime and H is a subgroup of S_p which contains a p-cycle and a 2-cycle, then $H = S_p$.*

Proof. Let τ be a two-cycle in H. After a relabelling of the objects permuted, we may assume $\tau = (12)$. Then a suitable power of a p-cycle in H has the form $\sigma = (12\cdots)$. After relabelling the objects other than $1, 2$, we can assume $\sigma = (123\cdots p)$. But then $\sigma^i \tau \sigma^{-i} = (i+1\ i+2) \in H$ for $0 \leq i \leq p-2$. But these elements generate S_p. $\square$

Thus, in virtue of Dedekind's Theorem, it suffices to choose our polynomial so that modulo 2 is is irreducible and modulo 3 is is a product of an ireducible quadratic and three distinct linear factors. Now $X^5 + X^2 + 1$ is irreducible modulo 2 and $X^2 + 1$ is irreducible modulo 3. So we want to choose $f = X^5 + aX^4 + bX^3 + cX^2 + dX + e$ so that f is congruent to $X^5 + X^2 + 1$ modulo 2 and to $(X^2+1)X(X-1)(X+1) = X^5 - X$ modulo 3. Applying the Chinese Remainder Theorem to the coefficients of f yields a solution $a = b = 0$, $c = e = 3$, $d = 2$ so that $X^5 + 3X^2 + 2X + 3$ has Galois group S_5 over $\mathbb{Q}$.