Lecture 26 : Polynomials with Galois Group S_n.

Objectives

(1) Tate's proof of Dedekind's theorem for computing Galois group

(2) Construction of polynomials with Galois group S_n.

Keywords and phrases: Polyomials with Galois group S_n Dedekind's reduction modulo p Theorem, Tate's proof.

It is in general difficult to calculate the Galois groups of polynomials with rational coefficients. We have learnt various methods of computing the Galois groups of polynomials of degree ≤ 4.

In this section we learn a theorem of Dedekind which provides useful information about G_f.

First we observe that the splitting field E of a monic polynomial $f(x)$ with rational coefficients is also a splitting field of a monic polynomial with integer coefficients. In fact, let

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

where $a_i = b_i/d \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$. Then

$$f\left(\frac{x}{d}\right) = \left(\frac{x}{d}\right)^n + \frac{b_1}{d}\left(\frac{x}{d}\right)^{n-1} + \frac{b_2}{d}\left(\frac{x}{d}\right)^{n-2} + \cdots + \frac{b_n}{d}.$$

Therefore

$$d^n f\left(\frac{x}{d}\right) = x^n + b_1 x^{n-1} + b_2 d x^{n-2} + \cdots + d^{n-1} b_n.$$

It is clear that splitting fields over $\mathbb{Q}$ of $f(x)$ and $d^n f(\frac{x}{d})$ coincide. Thus we may confine our attention to monic polynomials with integral coefficients.

Theorem 26.1 (Dedekind). *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n. Put $f_p(x) = f(x)$ mod p. Let $f(x)$ and $f_p(x)$ be separable. Suppose $f_p(x)$ is a product of irreducible polynomials of degree $n_1, n_2, \ldots, n_r$ in $\mathbb{F}_p[x]$, where $n_1 + n_2 + \cdots + n_r = n$. Then G_f contains a permutation which is a product of disjoint cycles of length $n_1, n_2, \ldots, n_r$.*

We will illustrate the theorem with a few examples before we embark on Tate's elegant proof.

Example 26.2. We have shown that the Galois group of $f(x) = x^5 - x + 1$ is S_5. The irreducible factorization of $f_2(x)$ is

$$f_2(x) = x^5 - x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1).$$

Thus $\sigma = (ij)(lmn) \in G_f$. Hence $\sigma^3 = (ij) \in G_f$. Next we observe that $f_3(x)$ is irreducible over F_3. There is no root of $f_3(x)$ in F_3. If there were a quadratic irreducible factor of $f_3(x)$ over F_3 then $x^9 - x$ and $f_3(x)$ will have a common factor. Hence $x(x^9 - x) = (x^5 - x)(x^5 + x)$ and $x^5 - x + 1$ have a common factor in $F_3[x]$, which is a contradiction. Hence G_f has a 5-cycle. Hence $G_f = S_5$.

Lemma 26.3. *A transitive subgroup G of S_n containing a transposition and an $(n-1)$-cycle in S_n.*

Proof. After a suitable reordering, let $\sigma = (12 \dots n-1) \in G$ and $(ij) \in G$. Since G is transitive $\tau(ij)\tau^{-1} = (kn)$ for some $\tau \in G$. Suppose $k \leq n-2$ then $\sigma(kn)\sigma^{-1} = (k+1\ n)$. If $k = n-1$ then $\sigma(n-1\ n)\sigma^{-1} = (1n)$. Thus $(1n), (2n), \dots, (n-1\ n) \in G$, whence $G = S_n$. □

Theorem 26.4. *There exist an irreducible monic polynomial with integer coefficients whose Galois group is S_n.*

Proof. We use the fact that for each prime p there exists an irreducible polynomial of degree n, for all n, in $F_p[x]$. We have already constructed such polynomials for $n \leq 4$.

Let $n \geq 5$. Let $g(x) \in F_2[x]$ be irreducible monic polynomial of degree n, $h(x) \in F_3[x]$ be irreducible monic polynomial of deg $n-1$ and $k(x) \in F_p[x]$ be irreducible monic quadratic, where $p \geq n-1$. By Chinese Remainder Theorem there exists $a, b \in \mathbb{Z}$ such that

$$\begin{aligned} a &\equiv 1 \pmod 2 \text{ and b} &&\equiv 0 \pmod 2 \\ &\equiv 0 \pmod 3 &&\equiv 1 \pmod 3 \\ &\equiv 0 \pmod p &&\equiv 0 \pmod p. \end{aligned}$$

Now consider the polynomial

$$f(x) = ag(x) + bxh(x) + (1 - a - b)x(x+1)...(x+n-3)k(x).$$

Then $f(x)$ is monic and irreducible in $\mathbb{Z}[x]$, since $f_2(x) \equiv g(x)$ which is irreducible mod 2. Since

$$\begin{aligned} f_3(x) &= xh(x) \text{ and} \\ f_p(x) &= x(x+1)\cdot(x+n-3)k(x), \end{aligned}$$

using Dedekind's Theorem, we see that G_f has an $(n-1)$-cycle and a transposition. But G_f is transitive. Hence $G_f = S_n$. □

Example 26.5. We construct a monic irreducible sextic polynomial in $\mathbb{Z}[x]$ with Galois group S_6 using the above theorem. Notice that

$$x^2+x+1,\ x^3+x+1,\ x^3+x^2+1,\ x+1,\ x$$

are all the monic irreducible polynomials of degree ≤ 3 over $\mathbb{F}_2$. None of these divide $f(x) = x^6+x^4+x^2+x+1$. Hence $f(x)$ is irreducible in $F_2[x]$. Note that x^5+x^4-x+1 is irreducible modulo 3. Put

$$\begin{aligned} g(x) &= x(x^5+x^4-x+1) \\ h(x) &= x(x-1)(x+1)(x+2)(x^2+2) \\ F(x) &= 15f(x)+10g(x)-24h(x). \end{aligned}$$

Since $F_2(x) = f(x)$ is irreducible in $\mathbb{F}_2[x]$, $F(x)$ is irreducible over $\mathbb{Q}$. Hence G_F has a 6-cycle. Since $F_3(x) = g(x)$ there exists a 5-cycle in G_F. As $F_5(x) = h(x)$ we see that there exists a 2-cycle in G_F. Therefore $G_F = S_6$.

Theorem 26.6 (Dedekind). *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n. Let E be the splitting field of $f(x)$ over $\mathbb{Q}$ and let $R = \{r_1, r_2, \ldots, r_n\}$ be the set of roots of $f(x)$ in E. Let E_p be the splitting field of $f_p(x) \in F_p(x)$ where p is a prime such that disc $(f_p(x)) \neq 0$. Let $R_p = \{s_1, s_2, \ldots, s_n\}$ be the set of roots of $f_p(x)$ in E_p Let $D = \mathbb{Z}[r_1, r_2, \ldots, r_n]$. Then*

(a) *There exists a ring homomorphism $\psi : D \to E_p$.*

(b) *Any ring homomorphism from $D \to E_p$ maps R onto R_p bijectively.*

(c) *The Galois group $G(E/\mathbb{Q})$ acts transitively on Hom (D, E_p), i.e. if $\psi_1, \psi_2 : D \to E_P$ are ring homomorphisms, then there exists $\sigma \in G(E/\mathbb{Q})$ such that $\psi_2 = \psi_1 \circ \sigma$.*

Proof. **(John Tate)** Since $\deg f(x) = n$, we have

$$\mathbb{Z} \subset D = \sum_{0 \le e_1, \ldots, e_n \le n-1} \mathbb{Z} r_1^{e_1} r_2^{e_2} \ldots r_n^{e_n}.$$

It is easy to show that pD is a proper ideal of D. Let $\mathfrak{m} \supseteq pD$ be a maximal ideal of D. The field $D/\mathfrak{m}$ is an extension of $\mathbb{F}_p$ generated by $r_i + \mathfrak{m}$, for $i = 1, 2, \ldots, n$ over $\mathbb{F}_p$. Hence $D/\mathfrak{m}$ is a finite $\mathbb{F}_p$- extension. Let $v : D \to D/\mathfrak{m}$ be the natural map. Then

$$f_p(x) = v(f(x)) = \prod_{i=1}^{n} (x - s_i).$$

Hence $D/\mathfrak{m}$ is a splitting field of $f_p(x)$, whence $D/\mathfrak{m} \simeq E_p$. Thus we have maps

$$D \xrightarrow{v} D/\mathfrak{m} \xrightarrow{\phi} E_p.$$

Hence $\phi \circ v : D \to E_p$ is a ring homomorphism.

Next we show that any ring homomorphism $\psi : D \to E_p$ maps R to R_p bijectively. Since $\psi(\mathbb{Z}) = \mathbb{F}_p$ and

$$\psi(f(x)) = f_p(x) = \prod_{i=1}^{n} (x - \psi(r_i)).$$

Notice that $f_p(x)$ has distinct roots. Hence $\psi(r_i)$ are the roots of $f_p(x)$.

Since any $\sigma \in G(E/\mathbb{Q})$ permutes the roots of $f(x)$, it induces an automorphism of D. Let $\psi : D \to E_p$ be any ring homomorphism. If $\sigma, \tau \in G(E/\mathbb{Q})$, then $\psi \circ \sigma$ and $\psi \circ \tau$ restricted to R are bijections onto R_p. Hence they are not equal. Let $G(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_N\}$. We claim that

$$\text{Hom } (D, E_p) \quad = \quad \{\psi \circ \sigma_1, \ldots, \psi \circ \sigma_N\}. \tag{1}$$

Let ψ_{N+1} be different from $\psi_i := \psi \circ \sigma_i$, for $i = 1, 2, \ldots, N$. By Dedekind independence theorem, $\psi_1, \ldots, \psi_{N+1} : D^\times \to E_p^\times$ are E_p-independent. The monomials $r_1^{e_1} \ldots r_n^{e_n}$, $0 \le e_1, \ldots, e_n \le n-1$ generate $E/\mathbb{Q}$. Among them we have N, $\mathbb{Q}$-linearly independent monomials, say $u_1, u_2, \ldots, u_N$. Consider the system of equations

$$\begin{bmatrix} \psi_1(u_1) & \psi_1(u_2) & \cdots & \psi_1(u_N) \\ \psi_2(u_1) & \psi_2(u_2) & \cdots & \psi_2(u_N) \\ \vdots & \vdots & \vdots & \vdots \\ \psi_{N+1}(u_1) & \psi_{N+1}(u_2) & \cdots & \psi_{N+1}(u_N) \end{bmatrix}^t \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{N+1} \end{bmatrix} = 0.$$

Let $(a_1, a_2, \ldots, a_{N+1}) \in E_P^{N+1}$ be a nontrivial solution of the above system. The monomials $u_1, u_2, \ldots, u_N$ from a $\mathbb{Z}$-basis of D. Any $y \in D$ has a unique expression, say $y = \sum_{j=1}^{N} n_j u_j$, for $n_1, n_2, \ldots, n_N \in \mathbb{Z}$. Hence

$$\psi_i(y) = \sum_j \overline{n_j}\psi_i(u_j) \Rightarrow \sum_{i=1}^{N+1} a_i\psi_i(y) = \sum_{i,j} a_i\overline{n_j}\psi_i(u_j) = 0.$$

This contradicts the independence of $\psi_i, \psi_2, \ldots, \psi_{N+1}$. This establishes the equality (1).

The Frobenious automorphism $\pi : a \longmapsto a^p$ generates $G(E_p/\mathbb{F}_p)$. The map $\pi \circ \psi$ is a homomorphism from $D \to E_p$, for any $\psi : D \to E_p$. Hence by (1) there exists an automorphism, $\tau \in G(E/\mathbb{Q})$ such that $\pi \circ \psi = \psi \circ \tau$.

Restrict ψ to R to get $\psi^{-1} \circ \pi \circ \psi = \tau$. Hence thought of as permutations, π and τ have same cycle structure. The permutation π acts on R_p and decomposes it into orbits. Since $\langle \pi \rangle = G(E_p/F_p)$, the cycle decomposition of π has disjoint cycles of lengths $deg f_1, \ldots, \deg f_r$ where $f_p(x) = f_1 f_2 \ldots f_r$ is the unique factorization of $f_p(x)$ in $F_p[x]$. The automorphism τ also decomposes R into orbits. The orbits of R_p under π-action are mapped by ψ^{-1} into orbits of R under the action of τ. This completes the proof of Dedekind's theorem. $\square$