Open Journal of Discrete Mathematics, 2018, 8, 73-78
http://www.scirp.org/journal/ojdm
ISSN Online: 2161-7643
ISSN Print: 2161-7635

On Tate's Proof of a Theorem of Dedekind

Shiv Gupta

Department of Mathematics, West Chester University, West Chester, PA, USA
Email: sguptai@wcupa.edu

How to cite this paper: Gupta, S. (2018) On Tate's Proof of a Theorem of Dedekind. *Open Journal of Discrete Mathematics*, **8**, 73-78.
https://doi.org/10.4236/ojdm.2018.83007

Received: March 13, 2018
Accepted: June 29, 2018
Published: July 2, 2018

Abstract

In this note we give a complete proof of a theorem of Dedekind.

Keywords

Galois Group of a Polynomial

1. Introduction

In this note we give a complete proof of the following theorem of Dedekind. Our proof is a somewhat detailed version of the one given in *Basic Algebra* by Jacobson, Volume I, [1] and we shall keep the notations used in that proof.

Theorem 1 *Let* $f(x) \in \mathbb{Z}[x]$ *be square-free monic polynomial of degree n and p be a prime such that p does not divide the discriminant of* $f(x)$. *Let* $G \subset S_n$ *be the Galois group of* $f(x)$ *over the field* $\mathbb{Q}$ *of rational numbers. Suppose that* $f_p = \overline{f} = f(\bmod p) \in \mathbb{Z}_p[x]$ *factors as:*

$$f_p = \overline{f} = \prod_{i=1}^{r} \overline{f_i}$$

where $\overline{f_i}$ *are distinct monic irreducible polynomials in* $\mathbb{Z}_p[x]$, *degree* $(\overline{f_i}) = d_i$, $1 \le i \le r$, *and* $d_1 + d_2 + \cdots + d_r = n$.

*Then there exists an auto*morphism $\sigma \in G$ *which when considered as a permutation on the zeros of* $f(x)$ *is a product of disjoint cycles of lengths* $d_1, d_2, \cdots, d_r$.

2. Preliminary Results

We shall assume that the reader is familiar with the following well-known results.

1) Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be a polynomial of degree $n \ge 2$. Then any two splitting fields of $f(x)$ are isomorphic.

2) A finitely generated Abelian group is direct sum of (finitely many) cyclic

groups. (This is the fundamental theorem of finitely generated Abelian groups).

3) A system of n homogeneous equation in $m > n$ variables has a non-trivial solutions.

4) Let $\mathbb{E}/\mathbb{F}$ be an algebraic extension. Then any subring of $\mathbb{E}$ containing $\mathbb{F}$ is a subfield of $\mathbb{E}$. **Proof:** Let K be a ring such that $\mathbb{F} \subset K \subset \mathbb{E}$. Let $\alpha \in K - \mathbb{F}$. As α is algebraic over $\mathbb{F}$, $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$. So $\alpha^{-1} \in \mathbb{F}(\alpha) \subset K$.

5) (Dedekind's Independence Theorem). Distinct characters of a monoid (a set with associative binary operation with an identity element) into a field are linearly independent. That is if $\chi_1, \chi_2, \cdots, \chi_n$ are distinct characters of a monoid into a field $\mathbb{F}$, then the only elements $a_i \in \mathbb{F}$, $1 \le i \le n$, such that

$$a_1\chi_1(h) + a_2\chi_2(h) + \cdots + a_n\chi_n(h) = 0$$

for all $h \in H$ are $a_i = 0$, $1 \le i \le n$.

6) Let p be a prime and $GF(p^m)$ be a finite field with p^m elements. Then the group $\mathrm{Aut}(GF(p^m)) = \langle\sigma\rangle$ is cyclic of order m and the generating automorphism σ maps $\alpha \in GF(p^m)$ to α^p.

7) If R is a commutative ring with identity and M is a maximal ideal of R then R/M is a field.

8) Let $\sigma, \eta \in S_n$. Then σ and $\eta^{-1}\sigma\eta$ have same cyclic structure.

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $n \ge 1$, and p a prime number. Then $f_p(x) \in \mathbb{Z}_p[x]$ will denote the polynomial obtained by reducing the coefficients of $f(x)$ modulo p.

Theorem 2 *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree $n \ge 1$ and p be a prime number which does not divide the discriminant of $f(x)$. Let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{Q}$. Let $\mathbb{E}_p$ be a splitting field of $f_p(x)$ over $\mathbb{Z}_p = \mathbb{Z}/(p)$. Let*

$$f(x) = (x - r_1)(x - r_2)\cdots(x - r_n), \quad r_i \in \mathbb{E} \subset \mathbb{C}, 1 \le i \le n$$

$$R = \{r_1, r_2, \cdots, r_n\},$$

$$R_p = \{\overline{r_1}, \overline{r_2}, \cdots, \overline{r_n}\} \subset \mathbb{E}_p$$

where $\overline{r_i}$, $1 \le i \le n$ are the roots of $f_p(x) \in \mathbb{Z}_p[x]$ and

$$\mathbb{E} = \mathbb{Q}(r_1, r_2, \cdots, r_n), \quad \mathbb{E}_p = \mathbb{Z}_p(\overline{r_1}, \overline{r_2}, \cdots, \overline{r_n})$$

Let $D = \mathbb{Z}[r_1, r_2, \cdots, r_n]$ be the subring generated by the roots of $r_1, r_2, \cdots, r_n$ of $f(x)$ in $\mathbb{C}$. Then

- 1) *There exists a homomorphism ψ of D onto $\mathbb{E}_p$.*
- 2) *Any such homomorphism ψ gives a bijection of the set R of the roots of $f(x)$ in $\mathbb{E}$ onto the set R_p of the roots of the $f_p(x)$ in $\mathbb{E}_p$.*
- 3) *If ψ and ψ' are two such homomorphisms then there exist $\sigma \in Aut(\mathbb{E}/\mathbb{Q}) = Gal(f(x))$, such that $\psi' = \psi \cdot \sigma$. (Note that the restriction of σ to D is an automorphism of D).*

Proof 1) One has that:

$$\mathbb{E} = \mathbb{Q}(r_1, r_2, \cdots, r_n) = \mathbb{Q}[r_1, r_2, \cdots, r_n]$$

We claim that $D=\mathbb{Z}[r_1,r_2,\cdots,r_n]$ is a finitely generated (additive) Abelian group. Since each r_i is a root of the monic polynomial $f(x)\in\mathbb{Z}[x]$ of degree n any positive power of $r_i, 1\le i\le n$ can be expressed as an integral linear combination of $1,r_i,r_i^2,\cdots r_i^{n-1}$. It follows that

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

Therefore D is a finitely generated (additive) Abelian group generated by at most n^n elements. By the *Fundamental Theorem for Finitely Generated Abelian Groups* D is a direct sum of finitely many cyclic groups. Since $D\subset\mathbb{C}$, none of these cyclic groups is finite. So D is a direct sum of finitely many infinite cyclic groups. Let $\{u_1,u_2,\cdots,u_N\}$ be a set consisting of an independent generating system of D. We have

$$D=\mathbb{Z}u_1\oplus\mathbb{Z}u_2\oplus\cdots\oplus\mathbb{Z}u_N,\quad N\le n^n.$$

We claim that $\{u_1,u_2,\cdots,u_N\}$ is a basis of $\mathbb{E}/\mathbb{Q}$. Obviously $\{u_1,u_2,\cdots,u_N\}$ is linearly independent over $\mathbb{Q}$. Let $\mathbb{Q}D=\sum_{1\le i\le N}\mathbb{Q}u_i$. Then $\mathbb{Q}D$ is a ring and $\mathbb{Q}\subset\mathbb{Q}D\subset\mathbb{E}$ therefore $\mathbb{Q}D$ is a field. Since $r_i\in D$ for $1\le i\le n$, by (4) $\mathbb{Q}D=\mathbb{E}$ and $\{u_1,u_2,\cdots,u_N\}$ is a basis of $E/\mathbb{Q}$. As $D=\mathbb{Z}u_1\oplus\mathbb{Z}u_2\oplus\cdots\oplus\mathbb{Z}u_N$,

$$pD=\mathbb{Z}(pu_1)\oplus\mathbb{Z}(pu_2)\oplus\cdots\oplus\mathbb{Z}(pu_N)$$

is an ideal of D and

$$D/pD=\left\{\overline{a_1u_1+a_2u_2+\cdots+a_Nu_N}:0\le a_i\le p-1\right\}.$$

Therefore the D/pD is finite of order p^N. Let M be a maximal ideal of D containing pD. That is $pD\subset M\subset D$ and D/M is a finite field of characteristic p and so it has a subfield isomorphic to $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$ which we will identify as $\mathbb{Z}_p$ in what follows. As

$$D/M\approx\frac{D/pD}{M/pD}$$

the order of D/M is p^m, $1\le m\le N$. Consider the canonical epimorphism

$$\nu:D\to D/M$$

whose kernel is M and $p\mathbb{Z}\subset M$. Therefore $\nu(\mathbb{Z})=\mathbb{Z}_p$. We note that as $D=\mathbb{Z}[r_1,r_2,\cdots,r_n]$ we have for $1\le i\le n$

$$\nu(r_i)=r_i+M=\overline{r_i},\quad \nu(D)=\mathbb{Z}_p\left[\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\right]$$

As ν is an epimorphism we have

$$\nu(D)=D/M=\mathbb{Z}_p\left[\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\right]$$

is a splitting field of $f_p(x)$ over $\mathbb{Z}_p$. As both D/M and $\mathbb{E}_p$ are splitting fields of $f_p(x)$ over $\mathbb{Z}_p$ they are isomorphic. Let

$$\phi:D/M\to\mathbb{Z}_p$$

be such an isomorphism. Then $\psi=\phi\cdot\nu$ is a homomorphism of D onto $\mathbb{E}_p$.

2) Let $\psi : D \to \mathbb{E}_p$ be a homomorphism. So $\psi(1)=1$. As $\mathbb{Z} \subset D$, and $\mathbb{E}_p$ has characteristic *p*, $\psi(p)=0$, so $\psi(\mathbb{Z}) = \mathbb{Z}_p \subset \mathbb{E}_p$. ψ can be extended to a homomorphism of the polynomial rings $D[x] \to \mathbb{E}_p[x]$. Under this mapping $f(x) \to f_p(x)$. As

$$f(x) = (x-r_1)(x-r_2)\cdots(x-r_n)$$

$$\psi(f(x)) = f_p(x) = (x-\psi(r_1))(x-\psi(r_2))\cdots(x-\psi(r_n)),$$

$\psi(r_i), 1 \le i \le n$ are the roots of the $f_p(x)$ in $\mathbb{E}_p$ and therefore the restriction of ψ to *R*

$$\psi_{|R} : \{r_1, r_2, \cdots, r_n\} \to \{\overline{r_1}, \overline{r_2}, \cdots, \overline{r_n}\}$$

is a bijection of the set *R* of roots of $f(x)$ in $\mathbb{E}$ to the set R_p of the roots of $f_p(x)$ in $\mathbb{E}_p$.

3) We have seen that given a homomorphism $\psi : D \to \mathbb{E}_p$, and $\sigma \in Gal(f) = Aut(\mathbb{E}/\mathbb{Q})$, $\psi' = \psi \cdot \sigma$ is also a homomorphism from *D* to $\mathbb{E}_p$. We note that the restriction of $\sigma \in Aut(\mathbb{E}/\mathbb{Q})$ to $D = \mathbb{Z}[r_1, r_2, \cdots, r_n]$ is also an automorphism of the ring *D*. Since $[\mathbb{E} : \mathbb{Q}] = N$, the group $Aut(\mathbb{E}/\mathbb{Q})$ has order *N*. Let

$$Aut(\mathbb{E}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \cdots, \sigma_N\}$$

So given a non-trivial homomorphism $\psi : D \to \mathbb{E}_p$, we get *N* distinct homomorphisms $\psi_j = \psi \cdot \sigma_j$, $1 \le j \le N$, from *D* to $\mathbb{E}_p$. We claim that these are all the homomorphisms from *D* to $\mathbb{E}_p$. Suppose that there is a homomorphism from *D* to $\mathbb{E}_p$ which is different from ψ_j, $1 \le j \le N$. Let us denote it by ψ_{N+1}. By *Dedekind Independence Theorem* the set $\{\psi_1, \psi_2, \cdots, \psi_N, \psi_{N+1}\}$ of $N+1$ homomorphisms from *D* to $\mathbb{E}_p$ is linearly independent over the field $\mathbb{E}_p$.

Consider the following system of *N* homogeneous equations in $N+1$ variables $\{x_1, x_2, \cdots, x_N, x_{N+1}\}$,

$$\sum_{i=1}^{N+1} x_i \psi_i(u_j) = 0, \quad 1 \le j \le N.$$

Since there are more variables than the equations this system of equations has a non-trivial solution. Let this non-trivial solution be $x_i = a_i \in \mathbb{E}_p$, $1 \le i \le N+1$. So we have

$$\sum_{i=1}^{i=N+1} a_i \psi_i(u_j) = 0, \quad 1 \le j \le N.$$

Let $y \in D = \mathbb{Z}u_1 \oplus \mathbb{Z}u_2 \oplus \cdots \oplus \mathbb{Z}u_N$. So $y = n_1u_1 + n_2u_2 + \cdots + n_Nu_N$, $n_k \in \mathbb{Z}$, $1 \le k \le N$. Then for $1 \le i \le N+1$ we have

$$\psi_i(y) = \overline{n_1}\psi_i(u_1) + \overline{n_2}\psi_i(u_2) + \cdots + \overline{n_N}\psi_i(u_N) = \sum_{j=1}^{j=N} \overline{n_j}\psi_i(u_j)$$

where $\overline{n_j} = n_j + (p)$. We shall show that

$$\sum_{i=1}^{i=N+1} a_i \psi_i(y) = 0,$$

which will contradict the linear independence of $\{\psi_1,\psi_2,\cdots,\psi_N,\psi_{N+1}\}$ over $\mathbb{E}_p$.

$$
\begin{aligned}
&\sum_{i=1}^{i=N+1} a_i\psi_i(y)\\
&=\sum_{i=1}^{i=N+1} a_i\sum_{j=1}^{j=N}\overline{n_j}\psi_i(u_j)\\
&=\sum_{i=1}^{i=N+1} a_i\left(\overline{n_1}\psi_i(u_1)+\overline{n_2}\psi_i(u_2)+\cdots+\overline{n_N}\psi_i(u_N)\right)\\
&=\overline{n_1}\sum_{i=1}^{i=N+1} a_i\psi_i(u_1)+\overline{n_2}\sum_{i=1}^{i=N+1} a_i\psi_i(u_2)+\cdots+\overline{n_N}\sum_{i=1}^{i=N+1} a_i\psi_i(u_N)\\
&=0.
\end{aligned}
$$

3. Proof of the Main Theorem

Since the field $\mathbb{E}_p$ has order p^m, the group $Aut(\mathbb{E}_p)$ has order m and $\pi:\mathbb{E}_p\to\mathbb{E}_p$ where $\pi(a)=a^p$ for all $a\in\mathbb{E}_p$, is the generating automorphism of $Aut(\mathbb{E}_p)$. So if $\psi:D\to\mathbb{E}_p$ is any homomorphism then so is $\pi\cdot\psi$. Since ψ and $\pi\cdot\psi$ are two homomorphisms from D to $\mathbb{E}_p$ there exist $\sigma\in Aut(\mathbb{E}/\mathbb{Q})$ such that $\pi\cdot\psi=\psi\cdot\sigma$ or $\psi^{-1}\cdot\pi\cdot\psi=\sigma$. This proves that the action on σ on $\{r_1,r_2,\cdots,r_n\}$ is similar to the action of π on $\{\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\}$. **Note:** In the following diagram the mapping

$$D\xrightarrow{\sigma}D$$

is the restriction of $\sigma\in Aut(\mathbb{E}/\mathbb{Q})$ to D and we are only concerned with the effect of the mappings σ, ψ and π on $\{r_1,r_2,\cdots,r_n\}$ and $\{\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\}$. Clearly

$$\{r_1,r_2,\cdots,r_n\}\xrightarrow{\sigma}\{r_1,r_2,\cdots,r_n\}$$
$$\{\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\}\xrightarrow{\pi}\{\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\}$$
$$\{r_1,r_2,\cdots,r_n\}\xrightarrow{\psi}\{\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\}$$

$$
\begin{tikzcd}
D \arrow[r, "\sigma"] \arrow[d, "\psi"'] & D \arrow[d, "\psi"] \\
\mathbb{E}_p \arrow[r, "\pi"] & \mathbb{E}_p
\end{tikzcd}
$$

As $\psi^{-1}\cdot\pi\cdot\psi=\sigma$ and $\psi\cdot\sigma\cdot\psi^{-1}=\pi$ the effect of σ on $\{r_1,r_2,\cdots,r_n\}$ is similar to the effect of π on $\{\overline{r_1},\overline{r_2},\cdots,\overline{r_n}\}$. This is further illustrated by the following:

$$\sigma(r_i)=r_j\Rightarrow\pi(\overline{r_i})=\overline{r_j}$$

$$\overline{r_i}\xrightarrow{\psi^{-1}}r_i\xrightarrow{\sigma}r_j\xrightarrow{\psi}\overline{r_j}$$

$$\pi(\overline{r_i})=\overline{r_j}\Rightarrow\sigma(r_i)=r_j$$

$$r_i\xrightarrow{\psi}\overline{r_i}\xrightarrow{\pi}\overline{r_j}\xrightarrow{\psi^{-1}}r_j$$

References

[1] Jacobson, N. (2014) Basic Algebra. 2nd Edition, Dover Publications, Inc., Mineola, New York.