EXISTENCE OF THE FROBENIUS ELEMENT AND ITS APPLICATIONS

SUN WOO PARK

Abstract. The existence of the Frobenius element in the Galois group of a finite field extension gives crucial references to certain types of Galois groups and polynomials. In this expository paper, we will first prove the existence of the Frobenius element. Then we will use the Frobenius element to show the construction of Galois groups S_p and A_p for prime p, the irreducibility of cyclotomic polynomials, and the significance of Chebotarev's Density Theorem.

Contents

Using the existence of the Frobenius element, we can understand some characteristics of cyclotomic polynomials and certain types of Galois groups, specifically the symmetric and alternating groups of prime p. In the first section, we will prove the existence of the Frobenius element. In the second section, we will use the Frobenius element to construct Galois groups isomorphic to symmetric groups and alternating groups of prime p, prove the irreducibility of cyclotomic polynomials, and apply Chebotarev's Density Theorem.

1. Frobenius Element

1.1. **Existence.** We start with the definitions and propositions needed for the proof of the existence of the Frobenius element.

Definition 1.1. A Dedekind domain R is an integral domain that satisfies either of the following equivalent properties.

(1) Every nonzero proper ideal of R factors into primes.
(2) R is an integrally closed Noetherian domain such that every nonzero prime ideal is maximal.

Proposition 1.2. *Let A be a Dedekind domain with quotient field F. Let K be a finite field extension of F and B be an integral closure of A in K. Then the following holds.*

(1) B is a finitely generated A-module.
(2) B is a Dedekind domain.

We omit the proof of the proposition which is shown in Morandi [1]. We also state the factorization of prime ideals in a finite Galois extension.

Proposition 1.3. *Let E/F be a finite Galois extension. Define A and B to be the ring of integers of the fields E and F respectively. Let $\mathfrak{p}$ be a prime ideal in A. Then the ideal $\mathfrak{p}B$ has the following unique factorization*

$$\mathfrak{p}B = (\prod_{i=1}^{g} \mathfrak{P}_i)^e$$

where $\{\mathfrak{P}_i\}$ is a set of distinct maximal ideals of B and e is the ramification index of $\mathfrak{p}$. If e is not equal to 1, we say the prime ideal $\mathfrak{p}$ is ramified in E. Otherwise, we say the prime ideal $\mathfrak{p}$ is unramified in E.

Definition 1.4. Let E/F be a finite Galois extension. Let A and B be the rings of integers of field E and F, respectively. Let $\mathfrak{p}$ be a prime ideal in A and $\mathfrak{P}$ be a prime ideal in B.

(1) $\mathfrak{p}$ is a prime ideal below $\mathfrak{P}$ if $\mathfrak{p} = \mathfrak{P} \cap A$. Equivalently, $\mathfrak{P}$ is a prime ideal lying over $\mathfrak{p}$ if the same condition holds.
(2) The decomposition group $D_{\mathfrak{P}}$ at $\mathfrak{P}$ is defined as follows.

$$D_{\mathfrak{P}} = \{\sigma \in Gal(E/F) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

It is clear that the decomposition group $D_{\mathfrak{P}}$ is a subgroup of the Galois group $Gal(E/F)$.

Now we prove the existence of the Frobenius element in the Galois group of a finite field extension.

Theorem 1.5. *Let A be a Dedekind ring with the fraction field F. Let E/F be a finite Galois extension. Let B be an integral closure of A in E and $\mathfrak{P}$ be a prime ideal in B. Define $\mathfrak{p}$ to be a prime ideal below $\mathfrak{P}$ in A such that $\mathfrak{p} = \mathfrak{P} \cap A$. Let $D_{\mathfrak{P}}$ be the decomposition group at $\mathfrak{P}$. Then the natural homomorphism ϕ is surjective:*
$D_{\mathfrak{P}} \xrightarrow{\phi} Gal((B/\mathfrak{P})/(A/\mathfrak{p}))$

Proof. By Proposition 1.2, B is a Dedekind domain and a finitely generated A-module. Hence, $B = \sum_{i=1}^{n} Aw_i$ where $w_1, w_2, ..., w_n \in B$. Notice that A is not necessarily a PID, so $\{w_i\}$ does not have to be a basis of B. We claim that there exists $\sigma \in Gal(E/F)$ such that $\overline{\sigma(x)} = \tau(\overline{x})$ where $\tau \in Gal((B/\mathfrak{P})/(A/\mathfrak{p}))$ and $\overline{x} = x \mod \mathfrak{P}$. We can show that the above claim holds for $\{w_i\}$ so that every $x \in B$ holds by A-linearity.

Consider the following polynomial g in $B[Y, X_1, X_2, ..., X_n]$.

$$g(Y, X_1, X_2, ..., X_n) = \prod_{\sigma \in G} (Y - \sum_{i=1}^{n} (\sigma(w_i) X_i))$$

Let σ^* be any element in the Galois group G. Applying σ^* to the polynomial g gives the following factorization.

$$\begin{aligned}
&\sigma^*(g(Y, X_1, X_2, ..., X_n)) \\
&= \sigma^*(\prod_{\sigma \in G}(Y - \sum_{i=1}^{n}(\sigma(w_i)X_i))) \\
&= \prod_{\sigma \in G}(Y - \sum_{i=1}^{n}(\sigma^*\sigma(w_i)X_i))
\end{aligned}$$

Obviously multiplying σ^* to each factor of the polynomial g reassigns each element σ to a different element $\sigma^*\sigma$ in the Galois group G. Notice that any two factors of the polynomial σ^*g cannot be the same. If so, then the polynomial g would have identical factors, which is a contradiction to the construction of g. Hence, for any element $\sigma^* \in G$, $\sigma^*g = g$. This clearly shows that the coefficients of the polynomial g is fixed by the elements of the Galois group G. Hence, the coefficients are in both B and F, which implies that the coefficients are in $B \cap F = A$.

Substitute Y with $\sum_{i=1}^{n}(w_iX_i)$, which allows the polynomial g to be an element of $B[X_1, X_2, ..., X_n]$. Then the following holds because the Galois group G has the identity automorphism.

$$\begin{aligned}
&g(\sum_{i=1}^{n}(w_iX_i), X_1, X_2, ..., X_n) \\
&= \prod_{\sigma \in G}(\sum_{i=1}^{n}(w_iX_i) - \sum_{i=1}^{n}(\sigma(w_i)X_i)) \\
&= \prod_{\sigma \in G}(\sum_{i=1}^{n}(w_i - \sigma(w_i))X_i) \\
&= 0
\end{aligned}$$

Reducing $g(\sum_{i=1}^{n}(w_iX_i), X_1, X_2, ..., X_n)\ mod\ \mathfrak{P}$ gives

$$\overline{g}(\sum_{i=1}^{n}(\overline{w_i}X_i), X_1, X_2, ..., X_n) = \overline{0}$$

in $(B/\mathfrak{P})[X_1, X_2, ..., X_n]$. Observe that $\overline{g}$ is in $A/\mathfrak{p}[X_1, X_2, ..., X_n]$ because the coefficients of g are in A.

Extend $\tau \in Aut(B/\mathfrak{P})$ to $\tau^* \in Aut(B/\mathfrak{P}[X_1, X_2, ..., X_n])$ by acting on the coefficients, i.e. by fixing each X_i. Apply τ^* to $\overline{g}$. The following procedure holds because τ fixes the coefficients of $\overline{g}$.

$$\begin{aligned}
&\tau^*(\overline{g}(\sum_{i=1}^{n}(\overline{w_i}X_i), X_1, X_2, ..., X_n)) \\
&= \overline{g}(\tau^*(\sum_{i=1}^{n}(\overline{w_i}X_i)), \tau^*(X_1), \tau^*(X_2), ..., \tau^*(X_n)) \\
&= \overline{g}(\sum_{i=1}^{n}(\tau(\overline{w_i})X_i), X_1, X_2, ..., X_n) \\
&= \overline{0}
\end{aligned}$$

Then the following holds by the construction of g.

$$\begin{aligned}
&\overline{g}(\sum_{i=1}^{n}(\tau(\overline{w_i})X_i), X_1, X_2, ..., X_n) \\
&= \prod_{\sigma\in G}(\sum_{i=1}^{n}(\tau(\overline{w_i})X_i) - \sum_{i=1}^{n}(\overline{\sigma(w_i)}X_i)) \\
&= \prod_{\sigma\in G}(\sum_{i=1}^{n}(\tau(\overline{w_i}) - \overline{\sigma(w_i)})X_i) \\
&= \overline{0}
\end{aligned}$$

It is clear that $(B/\mathfrak{P})[X_1, X_2, ..., X_n]$ is an integral domain, which shows that one of the factors of the product above is zero. Hence, there exists an automorphism $\sigma \in Gal(E/F)$ such that $\overline{\sigma(x)} = \tau(\overline{x})$ for every $x \in B$. Thus, $\sigma(\mathfrak{P}) = \mathfrak{P}$, which implies that $\sigma \in D_{\mathfrak{P}}$. The homomorphism ϕ is clearly surjective.

□

Notice that if $\mathfrak{p}$ is unramified, then the homomorphism ϕ becomes an isomorphism. The order of the kernel of the surjective homomorphism ϕ is same as the ramification index of $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified, the ramification index is 1, which implies that the kernel is trivial. Hence, ϕ is injective, so ϕ is an isomorphism. The isomorphism between the decomposition group $D_{\mathfrak{P}}$ and the Galois group $Gal((B/\mathfrak{P})/(A/\mathfrak{p}))$ gives the definition of the Frobenius element.

Definition 1.6. Let ϕ be the homomorphism defined in Theorem 1.5. with the additional condition that $\mathfrak{p}$ is unramified. Define $Fr(\mathfrak{P}/\mathfrak{p}) \in D_{\mathfrak{P}}$ to be the Frobenius element such that $\phi(Fr(\mathfrak{P}/\mathfrak{p}))$ is the Frobenius automorphism in $Gal((B/\mathfrak{P})/(A/\mathfrak{p}))$, i.e. the generator of $Gal((B/\mathfrak{P})/(A/\mathfrak{p}))$. The Frobenius automorphism is characterized by

$$\phi(Fr(\mathfrak{P}/\mathfrak{p}))(x) \equiv x^q \, mod \, \mathfrak{P}$$

for every $x \in B$, where $q = |A/\mathfrak{p}|$.

1.2. **Dedekind's Theorem.** In this section, we will prove Dedekind's theorem on the cycle decomposition of the Frobenius element. We will use the theorem extensively in subsequent sections. We first state the Kummer-Dedekind Theorem which shows the factorization of prime ideals in a finite number field extension.

Theorem 1.7. *Kummer-Dedekind Theorem*

Let E/F be a finite number field extension. Suppose $f(x) \in \mathscr{O}_F[x]$ is the minimal polynomial of α such that the index $N = |\mathscr{O}_E/\mathscr{O}_F[\alpha]|$ is finite. Let $\mathfrak{p}$ be a prime ideal of F such that $gcd(N, |\mathscr{O}_F/\mathfrak{p}|) = 1$. If $f(x) \equiv \prod_{i=1}^{j} \overline{g_i(x)} \bmod \mathfrak{p}$ where $\overline{g_i(x)} \equiv g_i(x) \bmod \mathfrak{p}$ and are distinct, then

$$\mathfrak{p}\mathscr{O}_E = \prod_{i=1}^{j} \mathfrak{P}_i^{e_i}$$

with the following properties:

(1) $\mathfrak{P}_i$ are distinct prime ideals of $\mathscr{O}_E$
(2) $\mathfrak{P}_i = \mathfrak{p}\mathscr{O}_E + g_i(\alpha)\mathscr{O}_E$

Corollary 1.8. *Let E/F be a finite number field extension with $E = F(\beta)$ where $\beta \in E$. Let $f(x) \in F[x]$ be a monic minimal polynomial of β. Let $\mathfrak{p}$ be a prime ideal in F. If $\overline{f(x)} = f(x) \bmod \mathfrak{p}$ is separable, then $\mathfrak{p}$ is unramified in the field extension $F(\beta)/F$.*

We now prove the following theorem by Dedekind which is similar to Kummer-Dedekind theorem.

Theorem 1.9. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n and let $E = \mathbb{Q}(x_1, x_2, ..., x_n)$ be the splitting field of f over $\mathbb{Q}$ where $x_1, x_2, ..., x_n$ are roots of $f(x)$. Choose a prime $p \in \mathbb{Z}$ such that $p \nmid \Delta f$, the discriminant of f. Let $B = \mathbb{Z}[x_1, x_2, ..., x_n]$ and let $\mathfrak{P}$ be a prime ideal of B lying over (p), i.e. $\mathfrak{P} \cap \mathbb{Z} = (p)$. Denote $f \bmod p$ as $\overline{f}$. If $\overline{f} = \prod_{i=1}^{r} \overline{f_i}$ with $\overline{f_i} = f_i \bmod p$ are irreducible polynomials over $\mathbb{F}_p$ of degree n_i, then $Fr(\mathfrak{P}/(p))$, when viewed as permutation of roots of f, has the cycle decomposition $\delta_1\delta_2...\delta_r$, each δ_i with length n_i such that $n_1 + n_2 + ... + n_r = n$.*

Proof. Since p does not divide Δf, $f \bmod p$ is separable. Hence, (p) is unramified. Recall from the construction of the Frobenius element that the homomorphism

$$\phi : \ D_{\mathfrak{P}} \longrightarrow Gal((\mathbb{Z}[x_1, x_2, ..., x_n]/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$$

is an isomorphism if (p) is unramified. Observe that the isomorphism ϕ sends $\sigma \in D_{\mathfrak{P}}$ to $\overline{\sigma}$ where $\overline{\sigma a_i} = \overline{\sigma(a_i)}$ for all $\overline{a_i}$. To elaborate, σ and $\overline{\sigma}$ correspond to the same permutation if we identify $D_{\mathfrak{P}}$ and $Gal((\mathbb{Z}[x_1, x_2, ..., x_n]/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$ as subgroups of S_n.

Notice that $Gal((\mathbb{Z}[x_1, x_2, ..., x_n]/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$ is cyclic because it is the Galois group of a finite field extension. Denote $\pi = \phi(Fr(\mathfrak{P}|\mathfrak{p}))$ as the generator of the Galois group, i.e. the Frobenius element. Notice that we can determine the cycle decomposition of π by observing the action of π on the roots of $\overline{f}$ and calculating their orbits. Since $\overline{f} = \prod_{i=1}^{r} \overline{f_i}$, each root of $\overline{f}$ corresponds to a root of f_i for some i. For each i, denote the roots of $\overline{f_i}$ as $\overline{x_{i1}}, \overline{x_{i2}}, ..., \overline{x_{in_i}}$.

Without loss of generality, consider the orbit of $\overline{x_{11}}$: $\{\overline{x_{11}}, \pi(\overline{x_{11}}), ..., \pi^{a-1}(\overline{x_{11}})\}$ where a is the least positive number such that $\pi^a(\overline{x_{11}}) = \overline{x_{11}}$. We claim that $a = n_1$. Notice that π is the automorphism of $\mathbb{Z}[x_1, x_2, ..., x_n]/\mathfrak{P}$ that fixes $\mathbb{Z}/p\mathbb{Z}$. Since $\overline{f_1}$ is a factor of $f \bmod p$, each $\pi^k(\overline{x_{11}})$ is a root of $\overline{f_1}$ for $1 \leq k \leq a-1$. Hence, $a \leq n_1$.

Conversely, given any root $\overline{x_{1j}}$ of $\overline{f_1}$, there exists a field isomorphism

$$\varphi : \ \mathbb{Z}/p\mathbb{Z}(\overline{x_{11}}) \longrightarrow \mathbb{Z}/p\mathbb{Z}(\overline{x_{1j}})$$

that sends $\overline{x_{11}}$ to $\overline{x_{1j}}$ and fixes $\mathbb{Z}/p\mathbb{Z}$. Extend φ to the field homomorphism

$$\varphi^* : \ \mathbb{Z}[x_1, x_2, ..., x_n]/\mathfrak{P} \longrightarrow \mathbb{Z}[x_1, x_2, ..., x_n]/\mathfrak{P}$$

Observe that φ^* sends $\overline{x_{11}}$ to $\overline{x_{1j}}$ and fixes $\mathbb{Z}/p\mathbb{Z}$. This clearly shows that $\varphi^* \in Gal((\mathbb{Z}[x_1, x_2, ..., x_n]/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$. Because the Galois group is cyclic, $\varphi^* = \pi^s$ for some integer s. Hence, $\overline{x_{1j}}$ is in the orbit of $\overline{x_{11}}$. Thus, $a = n_1$, which clearly implies that $(\overline{x_{11}} \ \ \pi(\overline{x_{11}}) \ \ ... \ \ \pi^{a-1}(\overline{x_{11}}))$ is a part of the cycle decomposition of π. Apply the same procedure to the roots of $\{\overline{f_i}\}$ for each i. The processes produce r disjoint cycles, each of length n_i. □

2. Application

In this section we will deduce several mathematical results in abstract algebra by using the existence of the Frobenius elements. In the first subsection, we will construct polynomials which have Galois groups isomorphic to symmetric and alternating groups of prime p. In the second subsection, we will give a proof of the irreducibility of cyclotomic polynomials. In the third subsection, we will state Chebotarev's density theorem and use the theorem to deduce Dirichlet's theorem on density of primes and the number of zeroes of $f \ mod \ p$ for polynomial $f \in \mathbb{Q}[x]$ and for any prime p.

2.1. Construction of Galois Groups: S_p and A_p for prime p.

We first observe the Galois groups isomorphic to symmetric groups of prime p.

Proposition 2.1. *For $n \geq 3$, the cycles $(1\ 2)$ and $(1\ 2\ ...\ n)$ generate the symmetric group S_n. In particular, for $p \geq 3$ prime, any p-cycle and 2-cycle generate the symmetric group S_p.*

Proof. We claim that the set of $n-1$ transpositions $\{(1\ 2), (2\ 3), ..., (n-1\ n)\}$ generates S_n. Notice that for any transposition $(a\ b)$ such that $a < b$, $(a\ b) = (a\ a+1)(a+1\ b)(a\ a+1)$. Using induction on a, we can observe that for some i, $(a+i\ \ b)$ is of the form $(j\ \ j+1)$. Since S_n is generated by the set of transpositions, the set $\{(1\ 2), (2\ 3), ..., (n-1\ n)\}$ generates S_n. Denote $\tau = (1\ 2\ ...\ n)$. Notice that for any integer $1 \leq i \leq n-2$, we have the following.

$$\tau^i(1\ 2)\tau^{-i} = (\tau^i(1)\ \tau^i(2)) = (i+1\ i+2)$$

The products of the permutations $(1\ 2)$ and $(1\ 2\ ...\ n)$ create all of the transpositions of the form $(j\ j+1)$. Hence, by using the claim above, the cycles $(1\ 2)$ and $(1\ 2\ ...\ n)$ generate the symmetric group S_n.

The case for S_p for prime p is a direct result of relabelling the permuted objects. First we relabel the objects of arbitrarily chosen 2-cycle as $(1\ 2)$. For p-cycle, any suitable power of a p-cycle has the form $(1\ 2\ ...k)$ for integer k. Relabeling the objects other than 1 and 2 gives the standard p-cycle $(1\ 2\ ...p)$. By the first part of the proposition, any p-cycle and 2-cycle generate the symmetric group S_p. □

Theorem 2.2. *Let $f(x) \in \mathbb{Q}[x]$ be a monic, separable, and irreducible polynomial of prime degree $p \geq 3$. Define E to be the splitting field of f over $\mathbb{Q}$. If there exists a prime number q such that $f(x) \ mod \ q$ has all but two roots in $\mathbb{F}_q$, where q does not divide the discriminant of f, then the Galois group $Gal(E/\mathbb{Q})$ is isomorphic to S_p.*

Proof. Let $r_1, r_2, ..., r_p$ be the roots of $f(x)$ and let $E = \mathbb{Q}(r_1, r_2, ..., r_p)$ be the splitting field of f over $\mathbb{Q}$. Notice that the Galois group $Gal(E/\mathbb{Q})$ is the permutation on the roots of f. Hence we have an embedding $Gal(E/\mathbb{Q}) \hookrightarrow S_p$. The Galois group $Gal(E/\mathbb{Q})$ has order divisible by p because for any r_i, root of f, $[\mathbb{Q}(r_i) : \mathbb{Q}] = p$ is a factor of the degree of splitting field over $\mathbb{Q}$. By Cauchy's theorem, $Gal(E/\mathbb{Q})$ includes an element of order p. Since we have an embedding from the Galois group to the symmetric group S_p, it follows that the image of $Gal(E/\mathbb{Q})$ contains a permutation of order p, which is precisely a p-cycle.

Since $f(x)$ *mod* q has all but two roots in $\mathbb{F}_q$, by Theorem 1.9 the image of $Gal(E/\mathbb{Q})$ in S_p contains a cycle decomposition of the Frobenius element, which is precisely a 2-cycle. By Proposition 2.2, $Gal(E/\mathbb{Q})$ is isomorphic to S_p. □

Example 2.3. Consider the irreducible polynomial $x^3 - x - 1$ which has discriminant -23. Notice that the polynomial has only one root in $\mathbb{Z}/5\mathbb{Z}$. Hence, the polynomial has Galois group isomorphic to S_3 by Theorem 2.3. Also consider the irreducible polynomial $x^5 - 4x - 1$ such that the discriminant is $-2^{18} + 5^5 = -259019$ which is a prime number (The discriminant formula for any quintic polynomial of the form $x^5 + ax + b$ is in p.267 of Jacobson [12]). Observe that $x^5 - 4x - 1$ has three roots in $\mathbb{Z}/19\mathbb{Z}$: $\overline{4}$, $\overline{10}$, and $\overline{11}$. Hence, the polynomial has Galois group isomorphic to S_5.

Now we analyze the Galois groups isomorphic to the alternating groups of prime p.

Proposition 2.4. *For $n \geq 3$, the following holds:*

(1) If n is odd, then $\{(1\ 2\ 3), (1\ 2\ ...\ n)\}$ is a set of generators of A_n.
(2) If n is even, then $\{(1\ 2\ 3), (2\ 3\ ...\ n)\}$ is a set of generators of A_n.

In particular, for $p \geq 3$ prime, any p-cycle and 3-cycle generate the alternating group A_p.

Proof. We claim that the group A_n is generated by 3-cycles of the form $(1\ 2\ i)$. Notice that any 3-cycle in A_n containing 1 and 2 is generated by 3-cycles of the form $(1\ 2\ i)$ because $(1\ i\ 2) = (1\ 2\ i)^{-1}$. Also, for any 3-cycle containing 1 but not 2, we have $(1\ i\ j) = (1\ 2\ j)(1\ 2\ j)(1\ 2\ i)(1\ 2\ j)$. Observe that A_n is generated by the set of 3-cycles of the form $(1\ i\ j)$ because for any 3-cycle $(i\ j\ k)$ we have $(i\ j\ k) = (1\ i\ j)(1\ j\ k)$. Hence, A_n is generated by the set of 3-cycles of the form $(1\ 2\ i)$.

We make another claim that the set of consecutive 3-cycles $(i\ i+1\ i+2)$ for $1 \geq i \geq n-2$ generates A_n. Notice that A_3 is generated by $(1\ 2\ 3)$. Also observe that A_4 is generated by $(1\ 2\ 3)$ and $(1\ 2\ 4)$ by the previous claim. Since $(1\ 2\ 4) = (1\ 2\ 3)(1\ 2\ 3)(2\ 3\ 4)(1\ 2\ 3)$, the set $\{(1\ 2\ 3), (2\ 3\ 4)\}$ generates A_4. The following holds for $5 \leq j \leq n$.

$$(1\ 2\ j) = (1\ 2\ j-2)(1\ 2\ j-1)(j-2\ \ j-1\ \ j)(1\ 2\ j-2)(1\ 2\ j-1)$$

Induction on j shows that $(1\ \ 2\ \ \text{j})$ is a product of consecutive 3-cycles. Hence, the set of consecutive 3-cycles $\{(i\ i+1\ i+2) | 1 \geq i \geq n-2\}$ generates A_n.

Suppose n is odd. Denote $\tau = (1\ 2\ ...\ n)$ such that $\tau \in A_n$. Then for $1 \leq i \leq n-3$ the following holds.

$$\tau^i(1\ 2\ 3)\tau^{-i} = (\tau^i(1)\ \tau^i(2)\ \tau^i(3)) = (i+1\ i+2\ i+3)$$

Hence, the set $\{(1\ 2\ 3), \tau\}$ is a set of generators of A_n for n odd.

Suppose n is even. Denote $\upsilon = (2\ ...\ n)$ such that $\upsilon \in A_n$. Then for $1 \leq i \leq n-3$ the following holds.

$$\upsilon^i(1\ 2\ 3)\upsilon^{-i} = (\upsilon^i(1)\ \upsilon^i(2)\ \upsilon^i(3)) = (1\ i+2\ i+3)$$

Notice that $(i\ i+1\ i+2) = (1\ i\ i+1)(1\ i+1\ i+2)$. Hence, the set $\{(1\ 2\ 3), \upsilon\}$ is a set of generators of A_n for n even.

We can deduce the set of generators of A_p for prime p from observing the result of Proposition 2.2 and the set of generators of A_n for n odd. □

Lemma 2.5. *Let F be a field such that $char(F) \neq 2$. Let $f(x) \in F[x]$ be a separable polynomial of degree n such that its roots are $x_1, x_2, ..., x_n$. Then the following statements are equivalent:*

1. *The embedding of the Galois Group $Gal(F(x_1, x_2, ..., x_n)/F) \hookrightarrow S_n$ as permutations of the roots of $f(x)$ has its image in A_n.*
2. *The discriminant of f, Δf, is square in F.*

Proof. Define $\delta = \prod_{i<j}(x_i - x_j) \neq 0$ such that $\delta^2 = \Delta f \in F$. Clearly $\delta \in F(x_1, x_2, ..., x_n)$. For any $\sigma \in Gal(F(x_1, x_2, ..., x_n)/F)$, let $\epsilon_\sigma = \pm 1$ be the sign of σ as a permutation of $\{x_i\}$. Then the following procedure holds.

$$\sigma(\delta) = \prod_{i<j}(\sigma(x_i) - \sigma(s_j)) = \epsilon_\sigma \prod_{i<j}(x_i - x_j) = \epsilon_\sigma \delta = \pm\delta$$

Notice that $\delta \neq -\delta$ because $char(F) \neq 2$ and $\delta \neq 0$. The following equivalence clearly holds.

$$\begin{aligned}
\sigma \in A_n &\iff \epsilon_\sigma = 1 \\
&\iff \sigma(\delta) = \delta \\
&\iff \delta\ is\ fixed\ by\ Galois\ group\ Gal(F(x_1, x_2, ..., x_n)/F) \\
&\iff \delta \in F \\
&\iff \Delta f\ is\ square\ in\ F
\end{aligned}$$

□

Using Proposition 2.5 and Lemma 2.6, we can deduce the following theorem.

Theorem 2.6. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, separable, and irreducible polynomial of prime degree $p \geq 3$. Assume Δf, the discriminant of f, is square in $\mathbb{Q}$. Define E to be the splitting field of f over $\mathbb{Q}$. If there exists a prime number q such that $f(x) mod q$ has all but three roots in $\mathbb{F}_q$, where q does not divide Δf, then the Galois group $Gal(E/\mathbb{Q})$ is isomorphic to A_p.*

Proof. Let $r_1, r_2, ..., r_p$ be the roots of $f(x)$ and let $E = \mathbb{Q}(r_1, r_2, ..., r_p)$ be the splitting field of f over $\mathbb{Q}$. Notice that the Galois group $Gal(E/\mathbb{Q})$ is the permutation on the roots of f. Also notice that Δf is square in $\mathbb{Q}$. Hence, by Lemma 2.6, we have an embedding $Gal(E/\mathbb{Q}) \hookrightarrow A_p$. The Galois group $Gal(E/\mathbb{Q})$ has order divisible by p because for any r_i, root of f, $[\mathbb{Q}(r_i) : \mathbb{Q}] = p$ is a factor of the degree of the field extension $E/\mathbb{Q}$. By Cauchy's theorem, $Gal(E/\mathbb{Q})$ includes an element of order p. Since there exists an embedding from the Galois group to the alternating group A_p,the image of $Gal(E/\mathbb{Q})$ contains a permutation of order p, which is precisely a p-cycle.

Since $f(x)$ *mod* q has all but three roots in $\mathbb{F}_q$, by Theorem 1.9 the image of $Gal(E/\mathbb{Q})$ in A_p contains a cycle decomposition of Frobenius element, which is precisely a 3-cycle. By Proposition 2.5, $Gal(E/\mathbb{Q})$ is isomorphic to A_p. □

Example 2.7. Consider the irreducible polynomial $x^5 + 20x - 16$ such that the discriminant is $2^{18}5^5+2^{16}5^5 = 2^{16}5^6$ which is square in $\mathbb{Z}$. Observe that $x^5+20x-16$ has two roots, specifically 2 and 3, in $\mathbb{Z}/7\mathbb{Z}$. Hence, the polynomial has the Galois group isomorphic to A_5.

2.2. **Irreducibility of Cyclotomic Polynomials.** We can also use the existence of the Frobenius element to prove that cyclotomic polynomials are irreducible over $\mathbb{Q}$. Here we state Gauss's lemma, which we will use to prove the irreducibility of cyclotomic polynomials. The proof of the lemma is in Chapter 9.3 of Dummit and Foote [3].

Lemma 2.8. *Gauss's Lemma Let R be a Unique Factorization Domain with the field of fractions F. Let $f(x) \in F[x]$.*

1. *If $f(x)$ is a reducible polynomial in $F[x]$, then $f(x)$ is a reducible polynomial in $R[x]$. In other words, if $f(x) = P(x)Q(x)$ for some non-constant polynomials $P(x), Q(x) \in F[x]$, then there are nonzero elements $a, b \in F$ such that $aP(x) = p(x)$ and $bQ(x) = q(x)$ both lie in $R[x]$ and $f(x) = p(x)q(x)$ in $R[x]$.*
2. *Suppose $f(x)$ is a primitive polynomial in $F[x]$, i.e. the greatest common divisor of the coefficients of $f(x)$ is 1. Then $f(x)$ is irreducible in $R[x]$ if and only if $f(x)$ is irreducible in $F[x]$.*

Theorem 2.9. *Cyclotomic polynomials are irreducible over $\mathbb{Q}$.*

Proof. Let E be the splitting field of x^n-1 and let G be the Galois group $Gal(E/\mathbb{Q})$. Define $\Phi_n(x)$ to be the nth cyclotomic polynomial. Consider the multiplicative group of nth roots of unity in $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, as μ_n. Let $\zeta \in \mu_n$ be a primitive nth root of unity. Clearly E contains μ_n since we can write E as $\mathbb{Q}(\zeta)$.

Consider the following homomorphism $\psi : \ Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \longrightarrow Aut(\mu_n)$ It is clear that $Aut(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^{\mathrm{x}}$ because each automorphism is uniquely determined by sending a primitive nth root of unity ζ to ζ^i for every i such that $(i, n) = 1$.

We can then define the homomorphism π from ψ. $\pi : \ Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{\mathrm{x}}$

where $\sigma \longmapsto a_\sigma \ mod \ n$ such that $\sigma(\zeta) = \zeta^{a_\sigma}$.

Notice that π is injective. If $\sigma \in Ker(\pi)$, then $a_\sigma \equiv 1 \ mod \ n$, which implies that $\sigma(\zeta) = \zeta$. Notice that σ then fixes $\mathbb{Q}(\zeta)$, which shows that σ is the identity. We claim that π is surjective. If we prove the claim, then $|\mathbb{Q}(\zeta) : \mathbb{Q}| = |\mathbb{Z}/n\mathbb{Z}|^{\mathrm{x}} = deg(\Phi_n(x))$, which clearly shows $\Phi_n(x)$ is a minimal polynomial of ζ. Hence $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

We now prove the claim. Assume $(\mathbb{Z}/n\mathbb{Z})^{\mathrm{x}}$ is cyclic. Pick a prime number p such that generates $(\mathbb{Z}/n\mathbb{Z})^{\mathrm{x}}$. Then $\Phi_n(x)$ *mod* p is separable. By Corollary 1.8, (p) is unramified in $\mathcal{O}_{\mathbb{Q}(\zeta)}$.

Define (q) to be a prime ideal lying over (p) and define $\overline{\zeta}$ to be the image of ζ in $\mathcal{O}_{\mathbb{Q}(\zeta)}/(q)$. Let $overline\Phi_n(x)$ be the image of $\Phi_n(x)$ in $\mathcal{O}_{\mathbb{Q}(\zeta)}/(q)$. Notice that $\overline{\zeta}$ is the root of the polynomial $\Phi_n(x)$. In other words, $\overline{\zeta}$ is a primitive nth root of unity.

By the similar argument used for showing π is injective, the following homomorphism $\varphi \quad Gal((\mathcal{O}_{\mathbb{Q}(\zeta)}/(q))/(\mathbb{Z}/p\mathbb{Z})) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^{\times}$ is injective. Since (p) is unramified in $\mathcal{O}_{\mathbb{Q}(\zeta)}$, the decomposition group $D_{(q)}$ at (q), which is the subgroup of the Galois group $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, is isomorphic to $Gal((\mathcal{O}_{\mathbb{Q}(\zeta)}/(q))/(\mathbb{Z}/p\mathbb{Z}))$. By Definition 1.6, there exists the Frobenius element $Fr((q)/(p)) \in D_{(q)}$ such that its image is the generator of the Galois group $Gal((\mathcal{O}_{\mathbb{Q}(\zeta)}/(q))/(\mathbb{Z}/p\mathbb{Z}))$, i.e. the Frobenius automorphism that sends $\overline{\zeta}$ to $\overline{\zeta}^p$. Hence, the image of the Frobenius automorphism in $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is p. Since p generates $(\mathbb{Z}/n\mathbb{Z})^{\times}$, we have the following diagram which shows π is surjective.

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \twoheadrightarrow D_{(q)} = Gal((\mathcal{O}_{\mathbb{Q}(\zeta)}/(q))/(\mathbb{Z}/n\mathbb{Z})) \xrightarrow{\varphi} (\mathbb{Z}/n\mathbb{Z})^{\times}$$

Now assume $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is not cyclic. We will prove the claim that for every prime $p \in \mathbb{Z}$ such that $(p, n) = 1$, the minimal polynomials of ζ and ζ^p over $\mathbb{Q}$ agree. If we prove the claim, then we can show that for any $m \in \mathbb{Z}$ such that $(m, n) = 1$, the minimal polynomials of ζ and ζ^m over $\mathbb{Q}$ agree. Observe that m is a product of primes, i.e. $m = p_1p_2...p_k$, such that each p_i does not divide n. Proving the claim assures that the following sequence of primitive nth roots of unity

$$\zeta,\ \zeta^{p_1},\ \zeta^{p_1p_2},\ ...,\ \zeta^{p_1p_2\cdots p_k} = \zeta^m$$

have the same minimal polynomials over $\mathbb{Q}$.

Assume not. Let $r(x)$ be the monic minimal polynomial of ζ over $\mathbb{Q}$ and $s(x)$ be the monic minimal polynomial of ζ^p over $\mathbb{Q}$. Assume that $r(x) \neq s(x)$. Notice that both $r(x)$ and $s(x)$ divide $x^n - 1$ because any nth root of unity is a root of $x^n - 1$. Using Lemma 2.8, any monic factor of $x^n - 1$ in $\mathbb{Q}[x]$ is in $\mathbb{Z}[x]$. Hence, both $r(x)$ and $s(x)$ are in $\mathbb{Z}[x]$. Since $r(x) \neq s(x)$, we can factorize the polynomial $x^n - 1$ as follows.

$$x^n - 1 = r(x)s(x)t(x)$$

where $t(x)$ is a monic polynomial in $\mathbb{Q}$. By Lemma 2.8, $t(x) \in \mathbb{Z}$. Reduce $x^n - 1$ *mod* p, which gives the following factorization in $\mathbb{Z}/p\mathbb{Z}$.

$$x^n - \overline{1} = \overline{r(x)}\ \overline{s(x)}\ \overline{t(x)}$$

Notice that $\overline{r(x)}$ and $\overline{s(x)}$ are not constant because both $r(x)$ and $s(x)$ are monic polynomials. As aforementioned, since p does not divide n, by Corollary 1.8, $x^n - \overline{1}$ is separable in $\mathbb{Z}/p\mathbb{Z}$. Hence, $\overline{r(x)}$ and $\overline{s(x)}$ are relatively prime in $\mathbb{Z}/p\mathbb{Z}$.

Since $s(\zeta^p) = 0$, $s(x^p)$ has ζ as a root. Hence, $r(x)$ divides $s(x^p)$ in $\mathbb{Q}[x]$, i.e. $s(x^p) = r(x)u(x)$ where $u(x)$ is a monic polynomial in $\mathbb{Q}[x]$. Since both $s(x^p)$ and $r(x)$ are monic polynomials, $u(x) \in \mathbb{Z}[x]$ by Lemma 2.8. Denote $s(x^p)$ *mod* p as $\overline{s(x^p)}$. Observe that $\overline{s(x^p)} = \overline{s(x)}^p$ in $\mathbb{Z}/p\mathbb{Z}$ by binomial theorem, which gives the following factorization.

$$\overline{s(x)}^p = \overline{r(x)}\ \overline{u(x)}$$

Hence, $\overline{r(x)}$ and $\overline{s(x)}$ are not relatively prime, a contradiction.

□

2.3. **Chebotarev's Density Theorem.** Chebotarev's density theorem statistically shows the splitting of prime ideals in Galois extension E of field F, i.e. the Galois extension E on $\mathbb{Q}$. Before stating the theorem, the following is a well-known theorem by Dirichlet.

Theorem 2.10. *Dirichlet's Theorem*

Let X be a subset of the set of prime numbers. Define the Dirichlet density of set X as follows.

$$\mathfrak{D}(X) = \lim_{s \to 1+} \frac{\sum_{p \in X} \frac{1}{p^s}}{log(\frac{1}{s-1})}$$

Then for $a, m \in \mathbb{N}$ such that $(a, m) = 1$, there are infinitely many primes p such that $p \equiv a \bmod m$. The Dirichlet density of set A of such primes p is.

$$\mathfrak{D}(A) = \frac{1}{\phi(m)}$$

where $\phi(m)$ is the Euler's phi function for integer m.

Dirichlet's theorem states that the proportion of primes p such that $p \equiv a mod m$ is asymptotic to $\frac{1}{\phi(m)}$. The generalization of Dirichlet's theorem is Chebotarev's Density Theorem.

Theorem 2.11. *Chebotarev's Density Theorem*

Let E/F be a finite field extension. Let A and B be the rings of integers of the fields E and F respectively. Let $\mathfrak{p}$ be a prime ideal in A and $\mathfrak{P}$ be a prime ideal in B. Define H_σ as the conjugacy class of an element σ in $G = Gal(E/F)$. Let P be the following set:

$$P = \{\mathfrak{p} \mid \mathfrak{p} \text{ is unramified in } E/F,\ Fr(\mathfrak{P}/\mathfrak{p}) \in H\}$$

Let X be a subset of the set of primes unramified in the field extension E/F. Define the density of the set X as follows:

$$\delta(X) = \lim_{N to \infty} \frac{\#\{\mathfrak{p} \mid |\mathcal{O}_F/\mathfrak{p}| \leq N,\ \mathfrak{p} \in X\}}{\#\{\mathfrak{p} \mid |\mathcal{O}_F/\mathfrak{p}| \leq N,\ \mathfrak{p}\ prime\}}$$

Then the following holds:

$$\delta(P) = \frac{|H_\sigma|}{|G|}$$

We omit the proof of both theorems. Notice that Dirichlet's theorem is precisely the result of Chebotarev's density theorem where F is $\mathbb{Q}$ and the extension E is $\mathbb{Q}(\zeta_m)$, the mth cyclotomic field. Using the proof of Theorem 2.9, we can identify $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ with $(\mathbb{Z}/m\mathbb{Z})^{\times})$. Observe that $E/\mathbb{Q}$ is an Abelian field extension. Hence, the conjugacy class $H = \{\sigma\}$ for all $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, which implies $|H_\sigma| = 1$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}$ with $\mathfrak{P}$ a prime ideal lying over $\mathfrak{p}$. As shown in the proof of Theorem 2.9, the image of the Frobenius element of the prime ideal $\mathfrak{P}$ in $(\mathbb{Z}/m\mathbb{Z})^{\times}$ is the prime number p which does not divide m. Hence we get a bijection between the Galois group $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and the conjugacy class of p in $(\mathbb{Z}/m\mathbb{Z})^{\times})$. Thus, $|G| = \phi(m)$. By Theorem 2.11, it is clear that the density of set P is $\frac{1}{\phi(m)}$.

Chebotarev's Density Theorem also provides some insights on the number of zeroes of $f \bmod p$ for any prime p.

Definition 2.12. Let S be a subset of G. We notate the following value $\frac{1}{|G|}\sum_{g \in S} \phi(g)$ as $\int_S \phi$ for function ϕ. When S is equal to G, we abbreviate the value as $\int \phi$.

Lemma 2.13. *Burnside's Lemma*

Let G be a group that acts on set X. Define $\chi(g)$ to be the number of fixed points of $g \in G$ on X. Then the number of orbits of G is equal to

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \int \chi$$

Proof. For each $\sum_{g\in G}\chi(g)$, each $x \in X$ is counted $|Stab(x)|$ times where $Stab(x)$ is the stabilizer of x. Assume x and y are on the same orbit. Then $|Stab(x)| = |Stab(y)|$. In other words, we count $(G : Stab(x))$ elements, all of which constitute the orbits of x, a total of $(G : Stab(x))(Stab(x)) = G$ times. Hence, each orbit constitutes $|G|$ times to the sum. Hence the number of orbits is equal to $\frac{1}{|G|}\sum_{g\in G}\chi(g)$. □

Corollary 2.14. *Let G be a group that acts transitively on non-trivial set X. Then there exists an element $g \in G$ such that it has no fixed points.*

Proof. Since G acts transitively on X, the number of orbit of G is equal to 1, which implies that $\frac{1}{|G|}\sum_{g\in G}\chi(g) = 1$. Observe that $\chi(1) = |X| > 1$ since X is non-trivial. If $\chi(g) \geq 1$ for every $g \in G$, then the left hand side of the above equality in Lemma 2.13 is definitely bigger than the right hand side, a contradiction. □

Now we observe the number of zeroes of $f \bmod p$ for any prime p.

Theorem 2.15. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $n \geq 2$. Define $N_p(f)$ as the number of zeroes of f in $\mathbb{Z}/p\mathbb{Z}$ for prime p. Then there exist infinitely many primes p such that $N_p(f) = 0$.*

Proof. Define the function $\chi^2(g)$ to be the number of fixed points by $g \in G$ in $X \times X$ with G acting transitively on X. Let $\int \chi^2$ be the number of orbits of G on $X \times X$. Clearly, $\int \chi^2 \geq 2$.

Denote the set $\{g \in G \mid \chi(g) = 0\}$ as G_0. Assume $g \notin G_0$. Then $1 \geq \chi(g) \geq n$, which implies the following procedure.

$$\begin{aligned}
&(\chi(g)-1)(\chi(g)-n) \leq 0\\
&\implies \int_{G-G_0}(\chi(x)-1)(\chi(x)-n) \leq 0\\
&\implies \int_{G}(\chi(x)-1)(\chi(x)-n) \leq \int_{G_0}(\chi(x)-1)(\chi(x)-n) = \int_{G_0} n
\end{aligned}$$

Since G acts transitively on X, $\int \chi = 1$ by Lemma 2.13. Then the left hand side of the inequality is as follows.

$$\begin{aligned}
\int_G(\chi(x)-1)(\chi(x)-n) &= \int_G(\chi^2(x)-(n+1)\chi(x)+n)\\
&= \int_G(\chi^2(x)) - (n+1) + n\\
&\geq 2-(n+1)+n = 1
\end{aligned}$$

The right hand side of the inequality is as follows.

$$\int_{G_0} n = n\int_{G_0} 1 = \frac{n}{|G|}\sum_{g\in G_0} 1 = \frac{n|G_0|}{|G|}$$

Hence we get the following inequality by comparing the left hand side and the right hand side.

$$\frac{|G_0|}{|G|} \geq \frac{1}{n}$$

We now consider $f(x) \in \mathbb{Z}[x]$ with $X = \{r_1, r_2, ..., r_n\}$, the set of distinct roots of f. Denote E as the splitting field of f over $\mathbb{Q}$. Then the Galois group $G = Gal(E/\mathbb{Q})$ acts transitively on X. Let G_0 be the set $\{\sigma \in G \mid \chi(\sigma) = 0\}$. If $N_p(f) = 0$ for prime p, then by Theorem 1.9. $Fr(p)$ does not have any fixed points. Hence, $Fr(p) \in G_0$. It is clear that G_0 is stable under conjugation. By Theorem 2.11, the set $P = \{p \mid Fr(p) \in G_0\}$ has density

$$\delta(P) = \frac{|G_0|}{|G|} \geq \frac{1}{n}$$

Thus, there exist infinitely many primes p such that $N_p(f) = 0$. □

Understanding the distribution of number of zeroes of polynomial f *mod* p for prime p may give some information about $f(x)$.

Corollary 2.16. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial such that f mod p has zeroes for almost every prime p. Then $f(x)$ is linear.*

Proof. The corollary is the contrapositive of Theorem 2.15. Assume f is an irreducible polynomial that has degree $n \geq 2$. Then by Theorem 2.15, there exist infinitely many primes p such that the number of zeroes of f in $\mathbb{Z}/p\mathbb{Z}$ is 0, which is a contradiction. □

Acknowledgments. It is a pleasure to thank my mentor, Yun Cheng and Zhiyuan Ding, for introducing me into Galois theory and Field theory, for guiding me on writing this paper, for providing me with adequate resources needed for this paper, and for advising me in mathematics consistently. I also sincerely thank professor Peter May and other professors for organizing the REU and for giving me again this wonderful opportunity to delve in mathematics.

References

[1] Patrick J. Morandi. Dedekind Domains.
https://www.math.nmsu.edu/ pmorandi/math601f01/DedekindDomains.pdf
[2] Robert B.Ash A Course in Algebraic Number Theory
Courier Corporation. 2010.
[3] David S. Dummit and Richard M. Foote. Abstract Algebra, Third Ed.
John Wiley and Sons, Inc. 2004.
[4] Akhil Mathew. The CRing project - Dedekind Domains.
http://people.fas.harvard.edu/ amathew/chdedekind.pdf
[5] Keith Conrad. Existence of Frobenius Elements (D'Apres Frobenius).
http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/frobeniuspf.pdf
[6] John Labute. Tate's Proof of a Theorem of Dedekind.
http://www.math.mcgill.ca/labute/courses/371.98/tate.pdf
[7] Daniel Katz. Galois Groups and Reduction Modulo a Prime.
https://www.math.ku.edu/ dlk/Galois
[8] Keith Conrad. Galois Groups as Permutation Groups.
http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/galoisaspermgp.pdf
[9] Keith Conrad. Cyclotomic Extensions.
http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/cyclotomic.pdf

[10] Alfonso Pesiri. The Chebotarev Density Theorem Applications.
Universita Delgi Studi Roma. 2007.
http://www.mat.uniroma3.it/scuola_orientamento/alumni/laureati/pesiri/sintesi.pdf
[11] Gil Moss. Chebotarev's Theorem and Artin L-Functions.
Harvard University. 2009.
http://www.ma.utexas.edu/users/gmoss/thesis_draft.pdf
[12] Nathan Jacobson. Basic Algebra I, Second Ed.
W.H. Freeman and Company. 1985.