Abstract

We discuss principality of prime ideals of finite algebraic number fields \( L = K(\theta) \) over an algebraic number field \( K([K : \mathbb{Q}] < \infty) \) defined by irreducible polynomials \( f(x) \in \mathcal{O}_K[x] \) and \( f(\theta) = 0 \). Our main Theorem says that if a principal prime ideal \((\pi)\) of \( \mathcal{O}_K \) is relatively prime to conductor \( \mathfrak{F} = \{ \alpha \in \mathcal{O}_L \mid \text{a principal ideal } (\alpha) \text{ of } \mathcal{O}_L \subset \mathcal{O}_K[\theta] \} \) and splits completely over \( L : (\pi)\mathcal{O}_L = \prod p_i \), then \( p_i \) is a principal ideal of \( \mathcal{O}_L \) for all \( i \). We use Jacobian Varieties of non-singular projective curve model of super elliptic curves \( y^l = f(x) \) to show the main Theorem, where \( l \) is a large enough prime number which is relatively prime to degree of \( f(x) \) and \( (\pi) \).

Keywords: Class numbers, class groups, discriminants

1 Introduction

Let \( f(x) = x^d + a_1x^{d-1} + a_2x^{d-2} + \cdots + a_{d-1}x + a_d \) be an irreducible polynomial over an algebraic integer ring \( \mathcal{O}_K \), \( \theta \) be one of the roots of \( f(x) = 0 \), \( L = K(\theta) \) and \( \mathcal{O}_K = K \cap \mathbb{Z} \), where \( K \) is an finite algebraic field \([K : \mathbb{Q}] < \infty\). In section 3, we see that if a principal prime ideal \((\pi)\) of \( \mathcal{O}_K \) is relatively prime to 6 and conductor \( \mathfrak{F} = \{ \alpha \in \mathcal{O}_L \mid \text{a principal ideal } (\alpha) \text{ of } \mathcal{O}_L \subset \mathcal{O}_K[\theta] \} \), and splits completely over \( L : (\pi)\mathcal{O}_L = \prod p_i \), \( p_i \) is a principal ideal of \( \mathcal{O}_L \) for all \( i \) via Jacobian Varieties of projective non-singular irreducible curve model \( C'_l \) of super elliptic curves \( y^l = f(x) \), where \( l \) is a large enough prime number which is relatively prime to degree of \( f(x) \) and \( (\pi) \).

In this section, we see an example through \( f(x) = x^3 - 2 \) over \( \mathbb{Q} \) with discriminant \( \Delta_f = -2^63^4 \). We assume that \( l \) is a large enough prime number. By easy calculation, \( y^l = x^3 - 2 \) has only one singular point \([1 : 0 : 0]\) in \( \mathbb{P}^2_{\mathbb{Q}} \) for

*email address: nanacanji@gmail.com

The subject classification codes by 2020 Mathematics Subject Classification is primary-11R29.
all large enough \( l \) and its genus \( g \) is larger than 0. For \( y^l = x^3 - 2 \), we can consider its non-singular projective irreducible model by resolving the singular point \([1 : 0 : 0]\) and we obtain a rational point as infinity point \( P_\infty \) (see Theorem 2.1 below). Hence we can consider Jacobian Variety \( J_f^l \) of \( y^l = x^3 - 2 \) for any large enough \( l \) over \( \mathbb{Q} \).

If a prime number \( p \geq 5 \) completely splits over \( K = \mathbb{Q}(\sqrt[3]{2}) \),

\[
(p) = p_1 p_2 p_3
\]

\((1.1)\)

\( f(x) \equiv (x - e_1)(x - e_2)(x - e_3) \pmod{p} \) for some \( e_i \in \mathbb{Z}, e_i \neq e_j \) (\( i \neq j \)), and \( p_i = p \mathcal{O}_K + (\sqrt[3]{2} - e_i) \mathcal{O}_K \) due to Dedekind-Kummer’s Theorem (see Theorem 3.2 below). Therefore, due to Theorem 2.1 below, Jacobian Variety \( J_f^l \) has a good reduction at \( p \) and has rational points \((\mathbb{Z}/l\mathbb{Z}) \oplus (\mathbb{Z}/l\mathbb{Z})\) over \( \mathbb{F}_p \) generated by \( P_1 - P_\infty \) and \( P_2 - P_\infty \), where \( P_1 \) is \([\alpha_i : 0 : 1]\) \((\alpha_i \equiv e_i \pmod{p})\) on \( y^l = x^3 - 2 \) over \( \mathbb{Q} \), \( P_\infty = [1 : 0 : 0] \), and \( P_1 - P_\infty \) is \( P_1 - P_\infty \pmod{p} \). Then, note that the following relations state:

\[
P_1 - P_\infty + P_2 - P_\infty + P_3 - P_\infty = 0
\]

\((1.2)\)

\[|p_1||p_2||p_3| = 1,\]

\((1.3)\)

where \([p_i]\) is class of \( p_i \) in ideal class group \( Cl(K) \) of \( K \). Therefore, if \([p_i]\) are not \( 1 \) in \( Cl(K) \), for any large enough prime number \( l \), we obtain surjective homomorphisms \( \varphi_I \) from a subgroup \( C(K)_p \) of \( Cl(K) \) generated by \([p_1]\) and \([p_2]\) to \((\mathbb{Z}/l\mathbb{Z}) \oplus (\mathbb{Z}/l\mathbb{Z})\) subgroup of rational points of \( J_f^l \pmod{p} \):

\[
\varphi_I : [p_1]^{n_1} [p_3]^{n_2} \mapsto n_1(P_1 - P_\infty) + n_2(P_2 - P_\infty).
\]

\((1.4)\)

This is well-defined because of relations (1.2) and (1.3) above, however, since \( Cl(K) \) is a finite group, this is inconsistent. Therefore, \([p_i] = 1 \) in \( Cl(K) \), in other words, \( p_i \) is a principal ideal in \( \mathcal{O}_K \).

## 2 Preparation for main Theorem

First, we consider a perfect field \( F \) because the following embedding Theorem 2.1 states over such any field and we use the Theorem over an algebraic field and a finite field. The following Theorem is used to embed roots of \( f(x) = x^d + a_1 x^{d-1} + a_2 x^{d-2} + \cdots + a_{d-1} x + a_d \) into Jacobian Variety’s \( l \)-torsion points \((\mathbb{Z}/l\mathbb{Z})^{d+2g+\epsilon}\), where \( g = (d-2)/2 \) and \( \epsilon = 1 \) if \( d \) is even, \( g = (d-1)/2 \) and \( \epsilon = 0 \) if \( d \) is odd. This Theorem plays important role of this paper.

**Theorem 2.1.** We assume that a prime number \( l \) is relatively prime to an integer \( d \geq 3 \) and characteristic of a perfect field \( F \). For an irreducible polynomial \( f(x) = x^d + a_1 x^{d-1} + a_2 x^{d-2} + \cdots + a_{d-1} x + a_d \) over \( F \), by considering a projective plane curve \( y^l = f(x) \) and its non-singular irreducible projective model \( C_f^l \)
over $F$, we can embed all roots $e_1, e_2, \ldots, e_d$ of $f(x) = 0$ into $\hat{J}_f = J_f \otimes_F F$ ($J_f$ is Jacobian Variety of $C_f$ and $F$ is an algebraic closure of $F$) as $P_1 = P_\infty, P_2 = P_\infty, \ldots, P_d = P_\infty$, where $P_i$ are non-singular points of $C_f \otimes_F F$ corresponding to $[e_i : 0 : 1]$ of $y^l = f(x)$ and $P_\infty$ is a rational point of $C_f$ over $F$ corresponding to $[1 : 0 : 0]$. Furthermore, the subgroup of $\hat{J}_f$ generated by the image of $P_1 - P_\infty, P_2 - P_\infty, \ldots, P_d - P_\infty$ is $(\mathbb{Z}/l\mathbb{Z})^{2g + \varepsilon}$, where $g = (d - 2)/2$ and $\varepsilon = 1$ if $d$ is even, $g = (d - 1)/2$ and $\varepsilon = 0$ if $d$ is odd. We also assume that $l$ is large enough such that genus of $C_f$ is larger than $g + 1$.

* Note that $g$ is not equal to genus of $C_f$ in general.

Proof. Let $[X : Y : Z]$ be the homogeneous coordinate of $\mathbb{P}^2_F$, and consider the following homogeneous equation of the target projective plane curve:

$$Y^l = X^dZ^{l-d} + a_1X^{d-1}Z^{l-d+1} + \cdots + a_dXZ^{l-1} + a_dZ^l. \tag{2.1}$$

By considering the following form,

$$G(X, Y, Z) = Y^l - (X^dZ^{l-d} + a_1X^{d-1}Z^{l-d+1} + \cdots + a_dXZ^{l-1} + a_dZ^l) \tag{2.2}$$

a point in $\mathbb{P}^2_F$ satisfies $G = \partial G/\partial X = \partial G/\partial Y = \partial G/\partial Z = 0$ is just $[1 : 0 : 0]$ because of perfectness of $F$. Although a point $[1 : 0 : 0]$ is the only one singular point of $y^l = f(x)$ in projective plane $\mathbb{P}^2_F$ ($x = X/Z$ and $y = Y/Z$ in (2.1) above), we can resolve this singular point by repeating blow-up at $[1 : 0 : 0]$. Then please note that the inverse image of $[1 : 0 : 0]$ from projective singular curve $y^l = f(x)$ to $C_f$ consists of only one point because $(d, l) = 1$. Actually, the projective plane curve $y^l = f(x)$ is represented by the following equation near $[1 : 0 : 0]$ through $yz$ ($y = Y/X$ and $z = Z/X$ in (2.1) above) plane by considering homogeneous coordinate:

$$y^l = z^{l-d} + a_1z^{l-d+1} + a_2z^{l-d+2} + \cdots + a_{d-1}z^{l-1} + a_dz^l. \tag{2.3}$$

By putting $z = uy$, we can blow up at $(0, 0)$ of $yz$-plane:

$$y^l = u^{l-d} + a_1u^{l-d+1}y + \cdots + a_{d-1}u^{l-1}y^{d-1} + a_du^d. \tag{2.4}$$

Since $l > d$, divide (2.3) above by $y^{l-d}$:

$$y^d - u^{l-d} + a_1u^{l-d+1}y + \cdots - a_{d-1}u^{l-1}y^{d-1} - a_du^d = 0. \tag{2.5}$$

By repeating blowing up at $(0, 0)$ by putting $y = uy_1, y_1 = uy_2, \ldots, y_{m-1} = uy_m$, we can deduce the degree of $u^{l-d}$ and becomes smaller than $d$. Therefore we obtain the following equation by repeating blow-up at $(0, 0)$:

$$y^d_m - u^k + H(t, y). \tag{2.6}$$

where $k < d, (d, k) = 1$ and $H(u, y_m)$ is a higher term of $u$ and $y_m$. By repeating blow-up at $(0, 0)$ by putting $u = v_1y_m, v_1 = v_2y_m, \ldots$ this singular point
is resolved because of Euclidean Algorithm. The inverse image of \([1 : 0 : 0]\) to a non-singular curve model is a regular point and rational over \(F\). Hence we can assume that the inverse image of \([1 : 0 : 0]\) on \(y^l = f(x)\) to \(C^l_i\) is a rational and regular point. \(P_{\infty}\) denotes the inverse image of \([1 : 0 : 0]\) on \(y^l = f(x)\) to a non-singular model \(C^l_i\).

Next, we observe properties of \(P_i - P_{\infty}\) on \(J_f \otimes_F \overline{F}\). Since \(\text{div}(x - e_i) = LP_i - LP_{\infty}\) as a divisor of \(\overline{C^l_i} = C^l_j \otimes_F \overline{F}\); \(P_i - P_{\infty}\) is a \(l\)-torsion point on \(\overline{J_f} = J^l_j \otimes_F \overline{F}\). Furthermore, if \(P_i - P_{\infty} \sim P_j - P_{\infty}\), \(P_i - P_j = \text{div}(h)\) for some \(h \in K(\overline{C^l_i})\) of function filed of \(\overline{C^l_i}\). However this is impossible on \(\overline{C^l_i}\) if \(i \neq j\) because there is no element of \(\overline{C^l_i}\)'s function field such that order 1 at \(P_i\), order -1 at \(P_j\) and 0 at all other points. So we can embed all roots of \(f(x) = 0\) into \(\overline{J_f}\) injectively. Because of the following minimum relation and \(\text{div}(x - e_i) = LP_i - LP_{\infty}\),

\[
\text{div}(y) = P_1 + P_2 + \cdots + P_d - dP_{\infty} = P_1 - P_{\infty} + P_2 - P_{\infty} + \cdots + P_d - P_{\infty} \quad (2.7)
\]

the images of \(P_1 - P_{\infty}, P_2 - P_{\infty}, \ldots, P_d - P_{\infty}\) on \(\overline{J_f}(l)\) generate a subgroup \((\mathbb{Z}/l\mathbb{Z})^{d+e}\) of \(\overline{J_f}(l)\), where \(e = 1\) if \(d\) is even, 1 if \(d\) is odd. Actually, the image of any \(d - 1\) elements of \(P_1 - P_{\infty}, P_2 - P_{\infty}, \ldots, P_d - P_{\infty}\) are linearly independent over \(\mathbb{Z}/l\mathbb{Z}\).

\[\square\]

3 The main Theorem

**Theorem 3.1** (The main Theorem). We assume \(d \geq 3\). Let \(f(x) = x^d + a_1x^{d-1} + a_2x^{d-2} + \cdots + a_{d-1}x + a_d\) be an irreducible polynomial over an algebraic integer ring \(\mathcal{D}_K\), \(\theta\) be one of the roots of \(f(x) = 0\), \(L = K(\theta)\) and \(\mathcal{D}_K = K \cap \mathbb{Z}\), where \(K\) is a finite algebraic field \([K : \mathbb{Q}] < \infty\). If a principal prime ideal \((\pi)\) of \(\mathcal{D}_K\) is relatively prime to conductor \(\mathfrak{f} = \{\alpha \in \mathcal{D}_L\mid \text{a principal ideal } (\alpha) \text{ of } \mathcal{D}_L \subset \mathcal{D}_K(\theta)\}\) and splits completely over \(L\):

\[
(\pi)\mathcal{D}_L = \prod_{i=1}^{d} p_i, \quad (3.1)
\]

then \(p_i\) is a principal ideal for all \(i\).

**Proof.** We assume that \(l\) is a large enough prime number which is relatively prime to \(d\) and a principal prime ideal \((\pi)\). If a principal prime ideal \((\pi)\) is relatively prime to conductor \(\mathfrak{f}\) and completely splits over \(L = K(\theta)\),

\[
(\pi) = p_1p_2p_3\cdots p_d \quad (3.2)
\]

\(f(x) \equiv (x - e_1)(x - e_2)(x - e_3)\cdots (x - e_d) \pmod{\pi}\) for some \(e_i \in \mathcal{D}_K\), \(e_i \neq e_j\) \((i \neq j)\), and \(p_i = (\pi)\mathcal{D}_L + (\theta - e_i)\mathcal{D}_L\) due to Dedekind-Kummer’s Theorem (see
Theorem 3.2 below). Therefore, due to Theorem 2.1, Jacobian Variety $J_f^I$ of an irreducible non-singular projective model of $y^i = f(x)$ has a good reduction at $(\pi)$ and has rational points $(\mathbb{Z}/l\mathbb{Z})^\oplus 2g+\varepsilon$ ($g = (d - 2)/2$ and $\varepsilon = 1$ if $d$ is even, $g = (d - 1)/2$ and $\varepsilon = 0$ if $d$ is odd). We also assume that $l$ is large enough such that genus of $C_f$ is larger than $g + 1$.) over $\mathcal{O}_K/(\pi)$ generated by $P_1 - P_\infty, P_2 - P_\infty, \ldots, P_d - P_\infty$, where $P_i \equiv [\alpha_i : 0 : 1] (\alpha_i \equiv e_i (\text{mod} (\pi)))$ on $y^i = f(x)$ over $\mathbb{Q}$, $P_\infty = [1 : 0 : 0]$, and $P_i - P_\infty$ is $P_i - P_\infty$ (mod $(\pi)$). Then, note that the following relations state:

$$\prod_{i=1}^{g} (P_i - P_\infty) = 0 \quad (3.3)$$

$$[p_1][p_2][p_3] \cdots [p_d] = 1, \quad (3.4)$$

where $[p_i]$ is class of $p_i$ in ideal class group $Cl(L)$ of $L$. Therefore, if $[p_i] \not\equiv 1$ in $Cl(L)$, for any large enough prime number $l$, we obtain surjective homomorphisms $\varphi_l$ from a subgroup $Cl(L)_l$ of $C(L)$ generated by $[p_1], [p_2], \ldots, [p_d]$ to $(\mathbb{Z}/l\mathbb{Z})^\oplus 2g+\varepsilon$ subgroup of rational points of $J_f^I$ (mod $(\pi)$):

$$\varphi_l : [p_1]^{n_1}[p_2]^{n_2} \cdots [p_d]^{n_d} \mapsto n_1(P_1 - P_\infty) + n_2(P_2 - P_\infty) + \cdots + n_d(P_d - P_\infty). \quad (3.5)$$

This is well-defined because of relations (3.3) and (3.4) above. However, since ideal class group $Cl(L)$ is a finite group, this is inconsistent. Therefore, $[p_i] = 1$ in $Cl(L)$, in other words, $p_i$ is a principal ideal in $\mathcal{O}_L$.

We must write the following important and useful Theorem here.

**Theorem 3.2 (Dedekind-Kummer).** Let $K$ be an algebraic field ($[K : \mathbb{Q}] < \infty$) and $\theta$ be an algebraic integer such that $L = K(\theta)$ and $\theta \in \mathcal{O}_L$. Furthermore, let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of $\theta$ over $K$, $\mathcal{O}_L$ and $\mathcal{O}_K$ be algebraic integer rings of $L$ and $K$ respectively, and $\overline{f}(x)$ denotes $f(x) \text{ (mod } p)$. Then, for a prime ideal $p$ of $\mathcal{O}_K$ which is relatively prime to conductor $\mathfrak{f} = \{ \alpha \in \mathcal{O}_L | \alpha \text{ a principal ideal } \}$ of $\mathcal{O}_L \subset \mathcal{O}_K[\theta]$}, we have the following decomposition

$$p\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i} \quad (3.6)$$

where $\mathfrak{P}_i = p\mathcal{O}_L + f_i(\theta)\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$, $f(x) \equiv \prod_{i=1}^{g} \overline{f}_i(x)^{e_i} \text{ (mod } p)$ is irreducible decomposition of $f(x) \text{ (mod } p)$, and $f_i(x)$ is a pull back of $\overline{f}_i(x)$ to $\mathcal{O}_K[x]$.

**Proof.** See [2] (8.3) Proposition. \qed
References

[1] Shinji Ishida, A reciprocity law of finite Galois extension fields defined by odd
degree irreducible polynomials over algebraic integer ring, [arXiv:2012.04503]
[math.GM]

[2] Jürgen Neukirch, Algebraic Number Theory, Springer, New York (1999).

[3] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer, New York
(1985).

[4] Takashi Ono, An Introduction to Algebraic Number Theory, University Se-
ries in Mathematics (1990).

[5] William Fulton, Algebraic Curves: An Introduction to Algebraic Geometry,
Addison-Wesley Publishing Company (1969)