

Shoumin Liu

Trinomials and exponential Diophantine equations

Master thesis, defended on May 7, 2008

Thesis advisor: Hendrik Lenstra



Mathematisch Instituut, Universiteit Leiden

Contents

0	Introduction	1
1	Cyclicity and discriminant	3
2	Minkowski's theorem	4
3	Cyclicity and extension over rational numbers with symmetric groups	5
4	Main theorem	7
5	Cyclicity and non-square discriminants for polynomials	8
6	Case of some trinomials and induced Diophantine equations	10
7	Application to Selmer's trinomial	13
7.1	A new version for the irreducibility of Selmer's trinomial . . .	13
7.2	Application	14

Abstract

Suppose A is an order of some number field K . In this thesis, we will present some results related to the Galois group and the discriminant under some special condition on A . We apply this to some $f \in \mathbb{Z}[x]$ with $\mathbb{Z}[x]/(f, f')$ cyclic. By studying the trinomial $f = x^n + ax^l + b$, we solve some exponential Diophantine equations. At last, Selmer's trinomial is used to illustrate our main theorem.

0 Introduction

Definition 0.1. Let K be a number field. Let \mathcal{O} be its ring of integers. An *order* of K is a subring $A \subset \mathcal{O}$ of finite index. The ring \mathcal{O} is the maximal order of K .

Definition 0.2. Let K be a field, and \overline{K} be its algebraic closure. Suppose $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in K[x]$, $a_n \neq 0$ and $\alpha_i, i = 1, 2, \dots, n$ be f 's roots in \overline{K} with multiplicities. Then the *discriminant* of f is $a_n^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2$, denoted as $\Delta(f)$.

In this thesis, let $\overline{\mathbb{Q}}$ be the algebraic closure of \mathbb{Q} in \mathbb{C} . Our main aim is to present the following theorem.

Theorem 0.3. (Main theorem) Suppose K is an extension over \mathbb{Q} of finite degree n . Let L , \mathcal{O} , Δ respectively be its normal closure in $\overline{\mathbb{Q}}$, its ring of integers, and its discriminant over \mathbb{Q} . Let A be an order of K , and $A^\dagger = \{x \in K \mid \text{Tr}(xA) \subset \mathbb{Z}\}$, where Tr is the trace from K to \mathbb{Q} . Suppose A^\dagger/A is a cyclic abelian group. Then we have the following conclusions.

- (1) $\text{Gal}(L/\mathbb{Q}) \simeq S_n$, where S_n is n -th symmetric group.
- (2) Suppose $\#(A^\dagger/A) = m^2d$, $m, d \in \mathbb{Z}$, and d square free. Then $|\Delta| = d$, and d is odd,
- (3) $\#(A^\dagger/A)$ is odd.

Using the theorem, we get a result for discriminants of some special polynomials in $\mathbb{Z}[x]$, which is as follows.

Theorem 0.4. Let f be a monic polynomial in $\mathbb{Z}[x]$. Suppose $\mathbb{Z}[x]/(f, f')$ is a cyclic abelian group, and $\deg f > 2$. Then $\mathbb{Z}[x]/(f, f')$ is finite, and $|\Delta(f)|$ is odd and not a square.

Inspired by [OSA] and [YAM], we study trinomial $f = x^n + ax^l + b$, and get the following conclusion.

Theorem 0.5. Suppose $f(x) = x^n + ax^l + b \in \mathbb{Z}[x]$, with $n > l > 0$, $n \geq 3$, and $ab \neq 0$. Then the abelian group $\mathbb{Z}[x]/(f, f')$ is cyclic if and only if both

- (1) and (2) hold:
- (1) $|b| = 1$ or $l \leq 2$,
- (2) $(al(n-l), nb) = 1$.

Using the above two theorems, we get results about certain exponential Diophantine equations.

Theorem 0.6. The equation

$$(X^X W^{X-1} + (1-X)^{X-1} Z^X)^2 = Y^4,$$

has no solution $X, Y, Z, W \in \mathbb{Z}$ with $X \geq 3$, $((X-1)Z, XW) = 1$.

Theorem 0.7. The equation

$$(\pm X^X V^{2(X-2)} + 4(X-2)^{X-2} Z^X)^2 = Y^4,$$

has no solution for $X, Y, Z, V \in \mathbb{Z}$ with $X \geq 3$, $(2(X-2)Z, XV) = 1$.

Theorem 0.8. The equation

$$((X+W)^{X+W} - (ZX)^X (\pm ZW)^W)^2 = Y^4,$$

has no solution for $X, Y, Z, W \in \mathbb{Z}$ with $X > 0$, $W > 0$, $(XWZ, X+W) = 1$.

Finally we will study Selmer's trinomials, which yield a good example of our main theorem. They have the following property.

Theorem 0.9. ([JPS]) For $n \in \mathbb{N}$ and $n \geq 2$, let α be a root of the polynomial $f_n = x^n - x - 1 \in \mathbb{Q}[x]$. Suppose L is the normal closure of $\mathbb{Q}(\alpha)$ in $\bar{\mathbb{Q}}$. Then $\text{Gal}(L/\mathbb{Q}) \simeq S_n$.

1 Cyclicity and discriminant

Definition 1.1. Let L/K be a finite separable field extension, let \mathcal{O}_K be a Dedekind domain with K as field of fractions, and let \mathcal{O}_L be the integral closure of \mathcal{O}_K in L . The fractional \mathcal{O}_L ideal

$$\mathfrak{C} = \{x \in L \mid \text{Tr}(x\mathcal{O}_L) \subset \mathcal{O}_K\}$$

is called Dedekind's complementary module, or the inverse different. Its inverse

$$\mathfrak{D}_{L/K} = \mathfrak{C}^{-1}$$

is called the different of L over K .

Theorem 1.2. Let L be a finite extension of a number field K . Suppose \mathfrak{p}_L is a finite prime of L , and $\mathfrak{p}_K = \mathfrak{p}_L \cap K$. Let e be the ramification index of $\mathfrak{p}_L/\mathfrak{p}_K$. Then

$$\text{ord}_{\mathfrak{p}_L}(\mathfrak{D}_{L/K}) = e - 1 + u$$

with $u = 0$ if $\mathfrak{p}_L/\mathfrak{p}_K$ is tamely ramified and $u \geq 1$ if $\mathfrak{p}_L/\mathfrak{p}_K$ is wildly ramified, and we have $u \leq \text{ord}_{\mathfrak{p}_L}(e)$.

Proof. See [PSH2], page 36, Theorem 4.9. □

Corollary 1.3. Suppose K is a number field and each $p \mid \Delta_{K/\mathbb{Q}} = [\mathcal{O}_K : \mathfrak{D}_{K/\mathbb{Q}}]$ is tamely ramified. Then the abelian group $\mathcal{O}_K/\mathfrak{D}_{K/\mathbb{Q}}$ ($\mathfrak{D}_{K/\mathbb{Q}}$ is the different) has a square free exponent.

Proof. By the above theorem, it follows that $\mathfrak{D}_{K/\mathbb{Q}} = \prod \mathfrak{p}^{e_{\mathfrak{p}/p}-1}$, where \mathfrak{p} ranges over all finite ramifying primes of K over \mathbb{Q} and $\mathfrak{p} \cap \mathbb{Z} = p$, with $e_{\mathfrak{p}/p}$ as the ramification index of \mathfrak{p}/p . By Chinese Remainder Theorem, we get

$$\mathcal{O}_K/\mathfrak{D}_{K/\mathbb{Q}} \simeq \prod \mathcal{O}_K/\mathfrak{p}^{e_{\mathfrak{p}/p}-1},$$

where \mathfrak{p} ranges over all finite ramifying primes of K over \mathbb{Q} . Because $\mathfrak{p}^{e_{\mathfrak{p}/p}} \supset p\mathcal{O}_K$, easily we can check that the number $T = \prod p$, where p ranges over all finite ramified primes of \mathbb{Z} is an exponent of $\mathcal{O}_K/\mathfrak{D}_{K/\mathbb{Q}}$. □

Theorem 1.4. *Suppose K is an extension over \mathbb{Q} of finite degree. Let \mathcal{O} , Δ respectively be its ring of integers, its discriminant over \mathbb{Q} . Let $\mathcal{O}^\dagger = \{x \in K \mid \text{Tr}(x\mathcal{O}) \subset \mathbb{Z}\}$. If $\mathcal{O}^\dagger/\mathcal{O}$ is a cyclic abelian group, then $\#(\mathcal{O}^\dagger/\mathcal{O}) = |\Delta_{K/\mathbb{Q}}|$ is square free and odd.*

Proof. Suppose \mathfrak{p} is a nonzero prime ideal of \mathcal{O} , and wildly ramifying over \mathbb{Q} , with ramification index $e > 1$ and residue index f over the prime $p \in \mathbb{Z}$, and \mathfrak{D} is the different of \mathcal{O} . Because $\mathcal{O}^\dagger/\mathcal{O}$ is cyclic, \mathcal{O}/\mathfrak{D} is cyclic. By Theorem 1.2, we have a surjective morphism

$$\mathcal{O}/\mathfrak{D} \twoheadrightarrow \mathcal{O}/\mathfrak{p}^e$$

with the right side of cardinality $p^{ef} > p$ and annihilated by p , which contradicts that \mathcal{O}/\mathfrak{D} is cyclic. So all the ramifying primes of K over \mathbb{Q} are tame. So by Corollary 1.3, we can see that $\#(\mathcal{O}^\dagger/\mathcal{O}) = |\Delta_{K/\mathbb{Q}}|$ is square free.

By Stickelberger's discriminant relation, it is known that

$$\#(\mathcal{O}^\dagger/\mathcal{O}) \equiv 0, \text{ or } \pm 1 \pmod{4},$$

and is square free, thus we can see the number $\#(\mathcal{O}^\dagger/\mathcal{O}) = |\Delta_{K/\mathbb{Q}}|$ is odd. \square

2 Minkowski's theorem

Theorem 2.1. *(Minkowski) Let K be a number field over \mathbb{Q} of degree n , and let $\Delta_{K/\mathbb{Q}}$ be the discriminant of K over \mathbb{Q} . Suppose $|\Delta_{K/\mathbb{Q}}| = 1$. Then $K = \mathbb{Q}$.*

Proof. From [PSH] (corollary 5.10, Page 54) we know

$$|\Delta_{K/\mathbb{Q}}| \geq \left(\frac{\pi}{4}\right)^{2s} \frac{n^{2n}}{n!^2} \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{n!^2} = b_n.$$

In this inequality, s is the number of complex embeddings of K modulo complex conjugation. We observe that $b_{n+1}/b_n = \frac{\pi}{4}(1 + \frac{1}{n})^{2n} \geq \frac{\pi}{4} \cdot 4 = \pi$, so b_n strictly increases with n . We know $b_2 = \frac{\pi^2}{4} > 1$, so $K = \mathbb{Q}$ when $|\Delta_{K/\mathbb{Q}}| = 1$. \square

Theorem 2.2. *A rational prime p ramifies in the ring of integer \mathcal{O}_K of K if and only if it divides the discriminant $\Delta_{K/\mathbb{Q}}$.*

Proof. Using Theorem 1.2. \square

Definition 2.3. Suppose L, K are number fields, whose rings of integers are $\mathcal{O}_L, \mathcal{O}_K$ respectively, and L/K is Galois with $G = \text{Gal}(L/K)$. Let \mathfrak{p}_L be a maximal ideal in \mathcal{O}_L , and $\mathfrak{p}_K = \mathfrak{p}_L \cap \mathcal{O}_K$. The decomposition group $G_{\mathfrak{p}_L/\mathfrak{p}_K}$

consists of those elements $\sigma \in G$ such that $\sigma \mathfrak{p}_L = \mathfrak{p}_L$. To each $\sigma \in G_{\mathfrak{p}_L/\mathfrak{p}_K}$, we can associate an automorphism $\bar{\sigma}$ of $\mathcal{O}_L/\mathfrak{p}_L$ over $\mathcal{O}_K/\mathfrak{p}_K$, and the map given by

$$\sigma \rightarrow \bar{\sigma}$$

induces a morphism of $G_{\mathfrak{p}_L/\mathfrak{p}_K}$ to $\text{Gal}((\mathcal{O}_L/\mathfrak{p}_L)/(\mathcal{O}_K/\mathfrak{p}_K))$. The kernel of this morphism is called the inertia group of $\mathfrak{p}_L/\mathfrak{p}_K$, which is denoted as $I_{\mathfrak{p}_L/\mathfrak{p}_K}$.

Proposition 2.4. *If L/\mathbb{Q} is finite and Galois, then $\text{Gal}(L/\mathbb{Q})$ is generated by the collection of all inertia groups $I_{\mathfrak{p}/p}$ with \mathfrak{p} ranging over the set of finite primes of L .*

Proof. Let \mathcal{O}_L be the ring of integers of L . Let G be the subgroup of $\text{Gal}(L/\mathbb{Q})$ which is generated by the inertia groups of all finite \mathfrak{p} . Suppose $k = L^G$ and \mathcal{O}_k is the ring of integers of k . Let \mathfrak{p} be a nonzero prime ideal of \mathcal{O}_L , suppose $\mathfrak{p} \cap k = \mathfrak{p}_1$, and $\mathfrak{p} \cap L^{I_{\mathfrak{p}}} = \mathfrak{p}_2$, we can see that $k = L^G \subset L^{I_{\mathfrak{p}}}$ because $I_{\mathfrak{p}}$ is a subgroup of G . We have the equality $e_{\mathfrak{p}/\mathfrak{p}_2} = e_{\mathfrak{p}/\mathfrak{p}_1} = e_{\mathfrak{p}/\mathfrak{p}_2} e_{\mathfrak{p}_1/\mathfrak{p}_2} e_{\mathfrak{p}_1/p}$, thus $e_{\mathfrak{p}_1/p} = 1$. Therefore there is no ramification in \mathcal{O}_k/\mathbb{Z} . By Theorem 2.2, we get $|\Delta_{k/\mathbb{Q}}| = 1$. Finally by Theorem 2.1 we get $k = \mathbb{Q}$. Hence $G = \text{Gal}(L/\mathbb{Q})$. \square

3 Cyclicity and extension over rational numbers with symmetric groups

Theorem 3.1. *Suppose G is a subgroup of S_n . Suppose G is transitive and generated by a collection of 2-cycles. Then $G = S_n$.*

Proof. Define $[n] = \{1, 2, \dots, n\}$. For $i, j \in [n]$, we define $i \sim j$ if and only if the transposition $(ij) \in G$ or $i = j$. Easily we can check it is an equivalence relation. Suppose $H = \{\sigma \in G \mid \text{for all } i \in [n], \sigma i \sim i\}$. Thus H is a subgroup of G containing all transpositions in G , which implies $H = G$. So for all $\sigma \in G$, for all $i \in [n]$, one has $\sigma i \sim i$. Because G is transitive, we have for all $i, j \in [n]$, $i \sim j$, so $(ij) \in G$, which tells us $G = S_n$. \square

Theorem 3.2. *Let L be a finite field extension of a number field K , M the normal closure of L over K , and \mathfrak{p} a finite prime of K , we set $G = \text{Gal}(M/K)$ and $H = \text{Gal}(M/L) \subset G$, and let G act in natural way on the set Ω of left cosets of H in G . Suppose we are given integers e_i, f_i for $i = 1, 2, \dots, t$. Then the following two statements are equivalent.*

- (1) *the prime \mathfrak{p} has t distinct extensions $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_t$ to L with ramification indices $e(\mathfrak{q}_i/\mathfrak{p}) = e_i$ and residue class field degrees $f(\mathfrak{q}_i/\mathfrak{p}) = f_i$;*
- (2) *for every decomposition group $G_{\mathfrak{P}} \subset G$ of a prime \mathfrak{P} above \mathfrak{p} in M/K , there are t distinct $G_{\mathfrak{P}}$ -orbits $\Omega_i \subset \Omega$ of length $\#\Omega_i = e_i f_i$ such that under*

the action of the inertia group $I_{\mathfrak{P}} \subset G_{\mathfrak{P}}$ on Ω_i , there are f_i orbits of length e_i each.

Proof. Let \mathfrak{P} be a prime of M over \mathfrak{p} with restriction \mathfrak{q} to L , and write $\Omega_{\mathfrak{P}}$ for the $G_{\mathfrak{P}}$ -orbit of the coset $H \in \Omega$. The length of this orbit is $[G_{\mathfrak{P}} : G_{\mathfrak{P}} \cap H]$, and this is equal to $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p})$ since we have a tower of complete extensions

$$M_{\mathfrak{P}} \supset L_{\mathfrak{q}} \supset K_{\mathfrak{p}}$$

in which $\text{Gal}(M_{\mathfrak{P}}/K_{\mathfrak{p}}) = G_{\mathfrak{P}}$ contains a subgroup $H_{\mathfrak{P}} = H \cap G_{\mathfrak{P}}$ corresponding to $L_{\mathfrak{q}}$. An arbitrary $G_{\mathfrak{P}}$ -orbit in Ω , say of the residue class gH , can be written as

$$G_{\mathfrak{P}} \cdot gH = g \cdot G_{g^{-1}\mathfrak{P}}H = g \cdot \Omega_{g^{-1}\mathfrak{P}},$$

so the length of such an orbit equals $e(\mathfrak{q}'/\mathfrak{p})f(\mathfrak{q}'/\mathfrak{p})$ with \mathfrak{q}' the restriction of $g^{-1}\mathfrak{P}$ to L . We do obtain a bijection between \mathfrak{p} to L and $G_{\mathfrak{P}}$ -orbits in Ω :

$$g_1^{-1}\mathfrak{P} \cap L = g_2^{-1}\mathfrak{P} \cap L \iff \exists h \in H : hg_1^{-1}\mathfrak{P} = g_2^{-1}\mathfrak{P} \iff \exists h \in H : g_2hg_1^{-1} \in G_{\mathfrak{P}} \iff \exists h \in H : G_{\mathfrak{P}} \cdot g_2h = G_{\mathfrak{P}} \cdot g_1 \iff G_{\mathfrak{P}} \cdot g_2H = G_{\mathfrak{P}} \cdot g_1H.$$

The inertia group $I_{\mathfrak{P}}$ of \mathfrak{P} is a normal subgroup of $G_{\mathfrak{P}}$, so all $I_{\mathfrak{P}}$ -orbits inside a single $G_{\mathfrak{P}}$ -orbit have the same length. Inside the orbit $\Omega_{\mathfrak{P}}$ this length is equal to the group index $[I_{\mathfrak{P}} : I_{\mathfrak{P}} \cap H] = [I_{\mathfrak{P}} : I_{\mathfrak{P}} \cap H_{\mathfrak{P}}] = [I_{\mathfrak{P}}H_{\mathfrak{P}} : I_{\mathfrak{P}}]$. In the extension $M_{\mathfrak{P}}/K_{\mathfrak{p}}$, this corresponds to a subextension $L_{\mathfrak{q}}/T_{\mathfrak{q}}$, with $T_{\mathfrak{q}}$ the inertia field of \mathfrak{q} in $L_{\mathfrak{q}}/K_{\mathfrak{p}}$. It follows that the length of the $I_{\mathfrak{P}}$ -orbits in $\Omega_{\mathfrak{P}}$ is $[L_{\mathfrak{q}} : T_{\mathfrak{q}}] = e(\mathfrak{q}/\mathfrak{p})$ as asserted. The identity $I_{\mathfrak{P}} \cdot gH = g \cdot I_{g^{-1}\mathfrak{P}}H$ now shows that the length of the $I_{\mathfrak{P}}$ -orbits in $G_{\mathfrak{P}}$ -orbit corresponding to a prime \mathfrak{q}' of L equals to $e(\mathfrak{q}'/\mathfrak{p})$. \square

Corollary 3.3. *Keep the notation in the above theorem. We suppose that $\{\mathfrak{q}/\mathfrak{p} | e(\mathfrak{q}/\mathfrak{p}) > 1\} = \{\mathfrak{q}'\}$, where \mathfrak{p} is any ramified finite prime of \mathcal{O}_K and \mathfrak{q}' is a finite prime of \mathcal{O}_L . If the unique \mathfrak{q}' that ramifies over \mathfrak{p} satisfies $e(\mathfrak{q}'/\mathfrak{p}) = 2$, $f(\mathfrak{q}'/\mathfrak{p}) = 1$, then $I_{\mathfrak{P}/\mathfrak{p}}$ acts as a 2-cycle, where \mathfrak{P} is a prime of \mathcal{O}_M and $\mathfrak{P} \cap L = \mathfrak{q}'$.*

Proof. Apply the above theorem. \square

Theorem 3.4. *Suppose K is an extension over \mathbb{Q} of finite degree n . Let L , \mathcal{O} , Δ respectively be its normal closure in $\overline{\mathbb{Q}}$, its ring of integers, its discriminant over \mathbb{Q} . Let $\mathcal{O}^\dagger = \{x \in K | \text{Tr}(x\mathcal{O}) \subset \mathbb{Z}\}$. If $\mathcal{O}^\dagger/\mathcal{O}$ is cyclic as an abelian group, then $\text{Gal}(L/\mathbb{Q}) \simeq S_n$.*

Proof. Thus by Theorem 1.4, it follows $\#(\mathcal{O}^\dagger/\mathcal{O})$ is square free, and we know that

$$\mathcal{O}^\dagger/\mathcal{O} \cong \mathcal{O}_K/\mathfrak{D}_{K/\mathbb{Q}} \cong \prod \mathcal{O}_K/\mathfrak{p}^{e_{\mathfrak{p}/p}-1+u_{\mathfrak{p}/p}},$$

where \mathfrak{p} ranges over all finite ramifying primes of K over \mathbb{Q} . Because $\mathcal{O}^\dagger/\mathcal{O}$ is cyclic, if a rational prime p has ramification in K , then there exists exactly

one prime in K that ramifies over p and it follows that $e(\mathfrak{p}/p) = 2$ and $f(\mathfrak{p}/p) = 1$ for all ramifying \mathfrak{p} over p . Because L is a normal closure of an extension of \mathbb{Q} of degree n , the group $\text{Gal}(L/\mathbb{Q})$ can be considered as a subgroup of S_n , and acts transitively on Ω (using $L, \mathbb{Q}[x]/(f_n), \mathbb{Q}$ to replace M, L, K in Theorem 3.1). By Theorem 2.4 we know $\text{Gal}(L/\mathbb{Q})$ is generated by all inertia groups. Using corollary 3.3, we know each inertia group is a 2-cycle or trivial. Finally through Theorem 3.1, the proof is concluded. \square

4 Main theorem

Theorem 4.1. (*Main theorem*) Suppose K is an extension over \mathbb{Q} of finite degree n . Let $L, \mathcal{O}, \Delta_{K/\mathbb{Q}}$ respectively be its normal closure in $\overline{\mathbb{Q}}$, its ring of integers, and its discriminant over \mathbb{Q} . Let A be an order of K , and $A^\dagger = \{x \in K \mid \text{Tr}(xA) \subset \mathbb{Z}\}$, where Tr is the trace from K to \mathbb{Q} . If A^\dagger/A is cyclic, we have the following conclusions

- (1) $\text{Gal}(L/\mathbb{Q}) \simeq S_n$,
- (2) Suppose $\#(A^\dagger/A) = m^2d$, $m, d \in \mathbb{Z}$, and d square free. Then $|\Delta_{K/\mathbb{Q}}| = d$, and d is odd,
- (3) $\#(A^\dagger/A)$ is odd.

Proof. Because A^\dagger/A is cyclic, and $A \subset \mathcal{O} \subset \mathcal{O}^\dagger \subset A^\dagger$, then $\mathcal{O}^\dagger/\mathcal{O}$ is cyclic. By Theorem 3.4, we get (1) is true. By duality, we have

$$\mathcal{O}/A \simeq A^\dagger/\mathcal{O}^\dagger.$$

By Theorem 1.4, we can see (2) is true.

Suppose $\#(A^\dagger/A)$ is even. Because $\#(A^\dagger/A) = \#(\mathcal{O}/A)^2 |\Delta_{K/\mathbb{Q}}|$, the number $\#(\mathcal{O}/A)$ is even. Let $A' = A + 2\mathcal{O}$ which has index 2 in \mathcal{O} . Suppose $\mathfrak{f} = \{x \in K \mid x\mathcal{O} \subset A'\}$ is the conductor of A' . Then we have inclusions

$$\mathfrak{f} \subset A' \subset \mathcal{O} \subset \mathcal{O}^\dagger \subset A'^\dagger.$$

Because \mathfrak{f} is the kernel of the natural surjective morphism

$$A' \twoheadrightarrow \text{Hom}(\mathcal{O}/A', \mathcal{O}/A') \simeq \mathbb{F}_2,$$

then we have

$$2\mathcal{O} \subset \mathfrak{f}, A'/\mathfrak{f} \simeq \mathbb{F}_2, \mathfrak{N}(\mathfrak{f}) = 4.$$

Suppose $(2) = \mathfrak{f}\mathfrak{g}$, where \mathfrak{g} is an ideal of \mathcal{O} . By (2), we know 2 is unramified in \mathcal{O} . Therefore we have $(\mathfrak{f}, \mathfrak{g}) = 1$. So we get

$$A'/2\mathcal{O} \subset \mathcal{O}/2\mathcal{O} \cong \mathcal{O}/\mathfrak{f} \times \mathcal{O}/\mathfrak{g}$$

Suppose $\beta \in \mathcal{O}$ and

$$\beta \equiv 1 \pmod{\mathfrak{f}}, \beta \equiv 0 \pmod{\mathfrak{g}}.$$

At the same time we can get

$$\overline{A'} = A'/2\mathcal{O} \cong \mathbb{F}_2 \times \mathcal{O}/\mathfrak{g}$$

We can see that $\overline{A'} \cdot \overline{\beta} = \{0, \overline{\beta}\}$. Suppose

$$\text{Tr} : \mathcal{O}/2\mathcal{O} \longrightarrow \mathbb{F}_2$$

which is the natural morphism induced by trace from K to \mathbb{Q} . Then $\text{Tr}(\overline{\beta}) = 0$. Therefore it follows that $\text{Tr}_{K/\mathbb{Q}}(A'\beta) \subset 2\mathbb{Z}$. Thus $\frac{\beta}{2} \in A'^{\dagger}$ and $\frac{\beta}{2} \notin \mathcal{O}$. Hence we have $\mathcal{O} \subset \mathcal{O} + \mathbb{Z}\frac{\beta}{2} \subset A'^{\dagger}$ and $\beta \in A'$. We can see that $A' \subset \mathcal{O} \subset \mathcal{O} + \mathbb{Z}\frac{\beta}{2}$, and $(\mathcal{O} + \mathbb{Z}\frac{\beta}{2})/A'$ is cyclic of order 4, which contradicts that it is annihilated by 2. Hence $\#(A'^{\dagger}/A)$ is odd. \square

Corollary 4.2. *Let $f \in \mathbb{Z}[x]$ be irreducible, and of degree $n > 1$. Suppose $\mathbb{Z}[x]/(f, f')$ is cyclic, and $\#(\mathbb{Z}[x]/(f, f')) = m^2d$, where $m, d \in \mathbb{N}$, and d is square free. Let $K = \mathbb{Q}(\alpha)$, where α is a root of f , and L be the normal closure of K . Then*

(1) $\text{Gal}(L/\mathbb{Q}) = S_n$

(2) $|\Delta_{K/\mathbb{Q}}| = d$, and d is odd.

(3) m is odd. In particular, $\#(\mathbb{Z}[x]/(f, f'))$ is odd and not a square.

Proof. It is known that $\mathbb{Z}[\alpha]^{\dagger} = \frac{1}{f'(\alpha)}\mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha]^{\dagger}/\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(f, f')$ which is cyclic. Then by the above theorem and Minkowski's Theorem, we obtain the corollary. \square

5 Cyclicity and non-square discriminants for polynomials

Theorem 5.1. *Let f be a monic polynomial in $\mathbb{Z}[x]$. Suppose $\mathbb{Z}[x]/(f, f')$ is a cyclic abelian group, and $\deg f > 2$. Then $\mathbb{Z}[x]/(f, f')$ is finite, and $|\Delta(f)|$ is odd and not a square.*

Proof. If $\mathbb{Z}[x]/(f, f')$ is infinite, then under an isomorphism φ , we have $\mathbb{Z}[x]/(f, f') \simeq \mathbb{Z}$. Suppose $\varphi(x) = a \in \mathbb{Z}$. Then $(x - a)^2 | f$. So we can construct a natural surjective morphism $\mathbb{Z}[x]/(f, f') \twoheadrightarrow \mathbb{F}_2[x]/((x - a)^2)$. But the right side is not cyclic, so we can conclude that $\mathbb{Z}[x]/(f, f')$ is finite.

If f is irreducible, then by corollary 4.2, the theorem is correct. Suppose f is not irreducible, then there exists a nonconstant polynomial $g \in \mathbb{Z}[x]$,

monic and irreducible, such that $f = gh$, with $h \in \mathbb{Z}[x]$ and $\deg h > 0$. Thus we see that $\mathbb{Z}[x]/(f, f') \twoheadrightarrow \mathbb{Z}[x]/(g, g')$, which implies that $\mathbb{Z}[x]/(g, g')$ is cyclic. Suppose p is a prime number in \mathbb{Z} and $p | (\Delta(g), \Delta(h))$. Suppose $\bar{g}, \bar{h} \in \mathbb{F}_p[x]$ and

$$\begin{aligned}\bar{g} &= (g \bmod p); \\ \bar{h} &= (h \bmod p).\end{aligned}$$

Therefore there exist nonconstant $G, H \in \mathbb{F}_p[x]$ such that $G^2 | \bar{g}, H^2 | \bar{h}$. Thus we can find a surjective morphism

$$\mathbb{Z}[x]/(f, f') \twoheadrightarrow \mathbb{F}_p[x]/(GH),$$

and the right side is not cyclic, a contradiction. Hence $(\Delta(h), \Delta(g)) = 1$. We have

$$\Delta(f) = \Delta(h)\Delta(g)R(g, h)^2,$$

where $R(g, h)$ is the resultant of g and h . If $f = \prod_{i=1}^t g_i$, and $g_i \in \mathbb{Z}[x]$ monic and irreducible, then by induction, we will get

$$\Delta(f) = \left(\prod_{i=1}^t \Delta(g_i) \right) \cdot m^2$$

and $m \in \mathbb{N}$, with

$$(\Delta(g_i), \Delta(g_j)) = 1, \quad 1 \leq i \neq j \leq t.$$

If $|\Delta(f)|$ is a square, by corollary 4.2, we can see each g_i is linear and monic. Because $\deg f > 2$, which means f has at least 3 linear factors, we suppose they are $x - a, x - b$, and $x - c \in \mathbb{Z}[x]$. Without loss of generality, we can suppose

$$a \equiv b \pmod{2},$$

so in $\mathbb{F}_2[x]$, $(x - a)^2 | f$ and $(x - a)^2 | f'$, then there is a morphism

$$\mathbb{Z}[x]/(f, f') \twoheadrightarrow \mathbb{F}_2[x]/((x - a)^2).$$

This is a contradiction because the right side is not cyclic. Finally we can say that $\Delta(f)$ is not a square.

If $2 | \Delta(f)$, then f is not separable in $\mathbb{F}_2[x]$, we can use the above method to get a contradiction. So $\Delta(f)$ is odd. \square

6 Case of some trinomials and induced Diophantine equations

For the polynomial $f(x) = x^n + ax^l + b \in \mathbb{Z}[x]$, with $n > l > 0$, $n \geq 3$, and $ab \neq 0$, we give a criterion to judge whether $R = \mathbb{Z}[x]/(f, f')$ is cyclic.

Here we suppose that $\mathbb{Z}_{(n)} = \mathbb{Z}[1/n]$, where $0 \neq n \in \mathbb{Z}$.

When $|b| \neq 1$ and $l \geq 3$, if prime $p|b$, we will have a morphism $R \rightarrow \mathbb{F}_p[x]/(x^2)$ as abelian group, with the right side is not cyclic. So we separate the rest of trinomials of this form into 3 cases.

Case 1 : $l = 1$. Now we have

$$f = x^n + ax + b, f' = nx^{n-1} + a.$$

(1) If there exists a prime $p|(a, n)$, it follows that $R \rightarrow \mathbb{F}_p[x]/(x^n + b)$, and the right side is not cyclic. So $(a, n) = 1$.

(2) If there exists a prime $p|(a, b)$, because $(a, n) = 1$, we will see a morphism

$$R \rightarrow \mathbb{F}_p[x]/(x^n, nx^{n-1}) = \mathbb{F}_p[x]/(x^{n-1})$$

with the right side is not cyclic. So $(a, b) = 1$.

(3) If there exists a prime $p|(n-1, b)$, then there is a morphism $R \rightarrow \mathbb{F}_p[x]/(\overline{f}, \overline{f}')$. Because $n\overline{f} = x\overline{f}'$ in $\mathbb{F}_p[x]$, and $p \nmid n$, then $\mathbb{F}_p[x]/(\overline{f}, \overline{f}') = \mathbb{F}_p[x]/(\overline{f}')$, which is not cyclic. So $(n-1, b) = 1$.

So (1), (2), (3) is equivalent to that $(a(n-1), bn) = 1$.

Conversely, suppose $(a(n-1), bn) = 1$. Because $nf - xf' = a(n-1)x + bn$, then we have

$$R \simeq \mathbb{Z}[x]/(f, f', a(n-1)x + bn) \simeq \mathbb{Z}_{(a(n-1))}/(f(-bn/a(n-1)), f'(-bn/a(n-1)))$$

with $x = \frac{-bn}{a(n-1)}$. We get the right side is a cyclic abelian group, because $(f(-bn/a(n-1)), f'(-bn/a(n-1)))$ is not trivial in $\mathbb{Z}_{(a(n-1))}$ as a result of $n \left(\frac{-bn}{a(n-1)} \right)^{n-1} \neq a$.

Case 2: $l = 2$, then

$$f = x^n + ax^2 + b, f' = nx^{n-1} + 2ax.$$

(1) If $2|n$, we get a morphism $R \rightarrow \mathbb{F}_2[x]/(\overline{f})$

(2) If $2|b$, then we get another morphism $R \rightarrow \mathbb{F}_2[x]/(x^2)$ Both (1) and (2) contradict the fact that R is cyclic, so b, n are odd.

(3) Suppose there exists a $p|(a, n)$, then there is a surjective morphism $R \rightarrow \mathbb{F}_p[x]/(\overline{f})$, with the right side not cyclic, so $(a, n) = 1$.

(4) If there exists a prime $p|(a, b)$, we can see that $R \rightarrow \mathbb{F}_p[x]/(x^{n-1})$. But $\mathbb{F}_p[x]/(x^{n-1})$ is not cyclic for $n \geq 3$. So it tells us that $(a, b) = 1$.

(5) By the argument similar to (3) of case 1, for $n\bar{f} = 2x\bar{f}'$ in $\mathbb{F}_p[x]$, we get $(n-2, b) = 1$.

Easily we can say (1), (2), (3), (4), (5) are equivalent to $(2a(n-2), nb) = 1$. Conversely, If $(2a(n-2), nb) = 1$, by

$$nf - xf' = (n-2)ax^2 + nb, f' = 2ax + nx^{n-1},$$

We can construct a natural surjective morphism

$\mathbb{Z}_{(2(n-2)a)} \twoheadrightarrow R$ with $x = \frac{-n}{2a} \left(\frac{-nb}{(n-2)a} \right)^{\frac{n-1}{2}}$. By an argument similar to case 1, it follows that R is cyclic.

Case 3: $b = \pm 1$, then

$$f = x^n + ax^l + b, f' = nx^{n-1} + alx^{l-1}.$$

(1) If there exists a prime $p|(al, n)$, then there is a surjective morphism $R \rightarrow \mathbb{F}_p[x]/(\bar{f})$, which contradicts to R is cyclic. So $(al, n) = 1$.

(2) By (1), we can see $(n-l, n) = 1$. We can see that (1) and (2) are equivalent to $(l(n-l)a, nb) = 1$.

Conversely, we suppose $(l(n-l)a, nb) = 1$. Because $f = x^n + ax^l + b$ and $b \in R^*$, then $x \in R^*$. Because $nf - xf' = a(n-l)x^l + bn = 0 \in R$ and $(l(n-l)a, nb) = 1$, then we get $a(n-l), n \in R^*$. Using the universal property of $\mathbb{Z}_{((n-1)a)}$, we get a morphism $\varphi: \mathbb{Z}_{((n-1)a)} \rightarrow R$. Suppose R_0 is the image of φ . Easily we find that $x^l = \frac{-bn}{a(n-1)} \in R_0$. For $(n, l) = 1$, therefore there exist $t, s \in \mathbb{Z}$, such that $tn + sl = 1$. So

$$x = x^{tn}x^{sl} = (-ax^l - b)^t(x^l)^s$$

which implies $x \in R_0$, and it follows that $R_0 = R$. Easily we can check that $\text{Ker}\varphi$ is not trivial, so we get R is cyclic.

We generalize the above cases to get the following theorem.

Theorem 6.1. *Suppose $f(x) = x^n + ax^l + b \in \mathbb{Z}[x]$, with $n > l > 0$, $n \geq 3$, and $ab \neq 0$. The abelian group $\mathbb{Z}[x]/(f, f')$ is cyclic if and only if both (1) and (2) hold:*

- (1) $|b| = 1$ or $l \leq 2$,
- (2) $(al(n-l), nb) = 1$.

The following is a theorem about the discriminant of the trinomial in [SWAN].

Theorem 6.2. *Let $n > l > 0$, $d = (n, l)$, and $n = n_1d$, $l = l_1d$. Then*

$$\Delta(x^n + ax^l + b) = (-1)^{n(n-1)/2} b^{l-1} [n^{n_1} b^{n_1-l_1} + (-1)^{n_1+1} (n-l)^{n_1-l_1} l^{l_1} a^{n_1}]^d.$$

Using Theorem 5.3 and Theorem 6.1, we get three theorems of three diophantine equations for the above 3 cases.

Theorem 6.3. *The equation*

$$(X^X W^{X-1} + (1-X)^{X-1} Z^X)^2 = Y^4,$$

has no solution $X, Y, Z, W \in \mathbb{Z}$ with $X \geq 3$, $((X-1)Z, XW) = 1$.

Proof. By Theorem 6.2, it follows that

$$|\Delta(f)| = |n^n b^{n-1} + (-1)^{n+1} (n-1)^{n-1} a^n|,$$

where $f = x^n + ax + b \in \mathbb{Z}[x]$, and $n > 3$, $ab \neq 0$. When $(a(n-1), nb) = 1$, by Theorem 5.1 and Theorem 6.1, we get that $|\Delta(f)|$ is not a square. Then we replace n, a, b by X, Z, W respectively, and the proof is concluded. \square

Theorem 6.4. *The equation*

$$(\pm X^X V^{2(X-2)} + 4(X-2)^{X-2} Z^X)^2 = Y^4,$$

has no solution for $X, Y, Z, V \in \mathbb{Z}$ with $X \geq 3$, $(2(X-2)Z, XV) = 1$.

Proof. By Theorem 6.2, it follows that

$$|\Delta(f)| = |b[n^n b^{n-2} + (-1)^{n+1} \cdot 4(n-2)^{n-2} a^n]|,$$

where $f = x^n + ax^2 + b \in \mathbb{Z}[x]$, and $n > 3$, $ab \neq 0$. When $(2a(n-2), nb) = 1$, by Theorem 5.1 and Theorem 6.1, we get that $|\Delta(f)|$ is not a square. Then we replace n, a, b by X, Z, V^2 (or $-V^2$) respectively, and the proof is concluded. \square

Theorem 6.5. *For equation*

$$((X+W)^{X+W} - (ZX)^X (\pm ZW)^W)^2 = Y^4,$$

has no solution for $X, Y, Z, W \in \mathbb{Z}$ with $X > 0$, $W > 0$, $(XWZ, X+W) = 1$.

Proof. By Theorem 6.2, it follows that

$$|\Delta(f)| = |(\pm 1)^{n-l} n^n + (-1)^{n+1} (n-l)^{n-l} l^l a^n|,$$

where $f = x^n + ax^2 \pm 1 \in \mathbb{Z}[x]$, and $n > 3$, $a \neq 0$. When $(la(n-l), n) = 1$, by Theorem 5.1 and Theorem 6.1, we get that $|\Delta(f)|$ is not a square. Then we replace n, a, l by $X+W, Z, W$ respectively, and the proof is concluded. \square

7 Application to Selmer's trinomial

7.1 A new version for the irreducibility of Selmer's trinomial

Theorem 7.1. (*[SEL]*) Let $n \in \mathbb{N}$ and $n \geq 2$, then $f_n = x^n - x - 1$ is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose $f(x) \in \mathbb{Z}[x]$ is monic with nonzero constant term and $\{x_i\}_{i=1}^{\deg f}$ are its roots with multiplicities, we define

$$S(f) = \sum \left(x_i - \frac{1}{x_i} \right) \quad (7.1)$$

As a symmetric function of the roots, S is rational, and an integer if the constant term of $f \in \mathbb{Z}[x]$ is 1 or -1 . In the latter case, if $f = gh$, and $g, h \in \mathbb{Z}[x]$, then $S(f) = S(g) + S(h)$, and $S(g), S(h) \in \mathbb{Z}$, since a rational factor of f must also have a constant term ± 1 (*Gauss Lemma*). Suppose $n \geq 3$, and we write f_n as the following :

$$f_n = \prod_{i=1}^n (x - x_i) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

and $a_{n-1} = 0$, $a_1 = -1$, $a_0 = -1$,

$$\begin{aligned} S(f_n) &= \sum \left(x_i - \frac{1}{x_i} \right) = \sum x_i - \sum \frac{1}{x_i} \\ &= -a_{n-1} - \sum \frac{x_1 \dots x_{i-1} x_{i+1} \dots x_n}{x_1 \dots x_n} = 0 + \frac{a_1}{a_0} = 1. \end{aligned}$$

Suppose x_i is any root of f_n , then we get

$$x_i + 1 = x_i^n, \quad \bar{x}_i + 1 = \bar{x}_i^n. \quad (7.2)$$

Thus

$$(x_i + 1)(\bar{x}_i + 1) = x_i^n \bar{x}_i^n,$$

which implies

$$x_i + 1 + \bar{x}_i = x_i^n \bar{x}_i^n - x_i \bar{x}_i \begin{cases} \geq 0, & |x_i| \geq 1 \\ \leq 0, & |x_i| \leq 1 \end{cases},$$

so $(x_i + 1 + \bar{x}_i)(1 - \frac{1}{x_i \bar{x}_i}) \geq 0$, which implies that

$$x_i - x_i^{-1} + \bar{x}_i - \bar{x}_i^{-1} = (x_i + \bar{x}_i) \left(1 - \frac{1}{x_i \bar{x}_i} \right) \geq \frac{1}{x_i \bar{x}_i} - 1.$$

Thus for any factor g of f_n :

$$S(g) = \sum \left(x_i - \frac{1}{x_i} \right) \geq \frac{1}{2} \sum \left(\frac{1}{|x_i^2|} - 1 \right) \quad (7.3)$$

The sum is over all roots of g . On the other hand, the product of the modulus over the same roots must give unity: $\prod \frac{1}{|x_i^2|} = 1$. The geometric mean of all $|x_i^{-2}|$ is consequently equal to 1. Since this is always at most the arithmetic mean (again with the equality only for all $|x_i| = 1$), it follows for the sum in (1.3) that $S(g) \geq 0$. Consequently any factorization of f_n must yield the integer partition $1 = 0 + 1$. The equality

$$1 = |x| = |x + 1| = |x^n|$$

only happens when $x = e^{\pm 2\pi i/3}$, which says that f_n is reducible can occur only for the factor $g = x^2 + x + 1$ or $\frac{f_n}{g} = x^2 + x + 1$. Easily we can see that $x^2 + x + 1$ is not a factor for f_n , and this concludes our proof. \square

7.2 Application

Theorem 7.2. ([JPS]) For $n \in \mathbb{N}$ and $n \geq 2$, let S_n be n -th symmetric group and α be a root of the polynomial $f_n = x^n - x - 1 \in \mathbb{Q}[x]$. Suppose L is the normal closure of $\mathbb{Q}(\alpha)$ in $\bar{\mathbb{Q}}$. Then

- (1) the group $\text{Gal}(L/\mathbb{Q}) \simeq S_n$;
- (2) the cardinality of $\mathbb{Z}[\alpha]^\dagger/\mathbb{Z}[\alpha]$ is $n^n - (1 - n)^{n-1}$, and $n^n - (1 - n)^{n-1}$ is not a square.

Proof. It is known that $\mathbb{Z}[\alpha]^\dagger = \frac{1}{f_n'(\alpha)}\mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha]^\dagger/\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f_n, f_n')$ which is a cyclic abelian group by Theorem 6.1 and has cardinality $n^n - (1 - n)^{n-1}$ by Theorem 6.2. So by our main theorem we conclude our proof. \square

References

- [JNK] Jürgen Neukirch, Algebraic Number Theory, 1992 Springer-Verlag Berlin, Heidelberg, New York.
- [OSA] Hiroyuki Osada, The Galois Groups of Polynomials $X^n + aX^l + b$, Journal of Number Theory, volume 23, 1987.
- [SEL] Ernst S. Selmer, On the Irreducibility of Certain Trinomials, Math. Scand. 4(1956), 287–302.

- [JPS] Jeans-Pierre Serre, Topics in Galois Theory, 1992 by Jones and Bartlett publisher.
- [PSH] Peter Stevenhagen, *Number Rings*, <http://www.math.leidenuniv.nl/~wpalenst/ant/ant.pdf>
- [PSH2] Peter Stevenhagen, *Local fields* <http://websites.math.leidenuniv.nl/algebra/localfields.pdf>
- [SWAN] Richard G. Swan, Factorization of Polynomials over finite fields, Pacific Journal of Mathematics Volume 12, Number 3(1962), 1099-1106.
- [YAM] K.Yamamura, On unramified Galois extension of real quadratic number fields, Osaka J.Math. 23 (1986), 471-478.