THE TURÁN SIEVE AND SOME OF ITS APPLICATIONS

by

YU-RU LIU

A thesis submitted to the Department of Mathematics and Statistics in conformity with the requirements for the degree of Master of Science

Queen’s University
Kingston, Ontario, Canada
July, 1998

copyright © Yu-Ru Liu, 1998
The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author’s permission.

L’auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L’auteur conserve la propriété du droit d’auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-31225-9
Abstract

We introduce the Turán sieve and apply it to solve some normal order problems. We also apply the Turán sieve to probabilistic Galois theory problems in both the rational number and the function field cases. We estimate the number of polynomials of degree $n$ and height $\leq N$ whose Galois group is a proper subgroup of $S_n$. For the rational number field case, we get an estimate of $O(N^{n-1/3} \log N)$ and in the case of the function field over $\mathbb{F}_q$, we get $O((q^{n+1})^{n-1} N)$. 
Acknowledgements

The completion of this thesis marks the end of a period that started during my undergraduate years in Montreal where I was surrounded by a group of excellent number theorists. To Professors Chantal David and Hershy Kisilevsky, of Concordia University, thank you for providing me with the chance to work with you in the summer of 1997. It was a great experience and I learnt a lot from it. To all CICMA postdocs, Adrian, Andreas, Imin, Lisa and Yiannis, thank you for the time we spent together in your offices. I owe my development in number theory to all of you. To all of my friends at McGill University, thank you for accompanying me through my undergraduate years. The moments with you, both of joy and of sorrow, will always remain with me. Special thanks to Professor Henri Darmon, of McGill University. Your enthusiasm for number theory has opened my mind to a whole new world. Your open mind to all branches of mathematics has taught me the true meaning of humility. Moreover, your natural generosity with your time and knowledge sets a good example to all of your students. Thank you, Henri.

This thesis could not have been completed without the support of the Math department at Queen’s University. Especially, I want to thanks the number theory group here. To Professors Kani, Murty and Yui, thank you for providing such a stimulating environment for number theory students here. To all of my friends at Queen’s, thank you for your sincere help during my stay here. It is really a pleasure knowing all of you. Special thanks to David and Satya. Although I may forget some of the theorems that we proved in our modular forms course or class field theory lectures, I will never forget the pleasant moments we have spent together.

To my dear family, Mama, Baba and MeiMei-my little friend. Thank you for al-
lowing me the freedom to travel to different places, hence to broaden my mind, and thank you for always being concerned about me and sending me your blessings.

I will never know how to express my thanks to my supervisor, Professor M. Ram Murty. It is he who has taught me how to do research. It is he who has given me the confidence that I can do research. Also because of him, I have realized the importance of being strong and the true definition of 'the strong'.

The teacher who walks in the shadow of the temple, among his followers, gives not of his wisdom but rather his faith and his lovingness.

If he is indeed wise, he does not bid you enter the house of his wisdom, but rather leads you to the threshold of your own mind. (K. Gibran, The Prophet, On teaching)

Really, thank you, my guru.
Contents

1 The Turán Sieve and Normal Order Problems .................................................. 7
   1.1 Introduction. ................................................................................................. 7
   1.2 The Turán Sieve. ......................................................................................... 8
   1.3 The Turán sieve on normal order problems. .............................................. 11

2 Probabilistic Galois Theory in \( \mathbb{Q} \). ................................................................. 16
   2.1 Introduction. .................................................................................................. 16
   2.2 The Möbius function. ................................................................................... 18
      2.2.1 Definition of the Möbius function. ....................................................... 18
      2.2.2 The Möbius inversion formula. ............................................................. 18
   2.3 Monic irreducible polynomials in \( \mathbb{F}_p[x] \). .............................................. 20
   2.4 Two definitions of types and their relations. ............................................... 22
   2.5 Elementary group theory. .......................................................................... 23
   2.6 The Turán sieve on \( E_n(N) \). ................................................................... 25
      2.6.1 Lowering the level of the original question. ........................................ 25
      2.6.2 The Turán sieve on \( E_{r,n}(N) \). ......................................................... 26

3 The Galois Groups of Cubics and Trinomials ...................................................... 30
   3.1 Introduction. .................................................................................................. 30
Chapter 1

The Turán Sieve and Normal Order Problems

1.1 Introduction.

Let \( n \in \mathbb{N} \). We denote \( \nu(n) \) to be the number of distinct prime factors of \( n \). A celebrated theorem of Hardy and Ramanujan states that

\[
\nu(n) \sim \log \log n.
\]

In 1934, Paul Turán gave a very simple proof of the above theorem. He showed that

\[
\sum_{n \leq x} (\nu(n) - \log \log n)^2 = O(x \log \log x),
\]

from which the normal order of \( \nu(n) \) is easily deduced. The summation on the left hand side looks very much like the variance of the "random variable" \( \nu(n) \). Indeed, this similarity was amplified by Linnik when he developed the powerful large sieve method.
Unfortunately, even though many experts are aware that Turán’s original derivation of the Hardy-Ramanujan Theorem conceals in it, in seed form, an elementary sieve method, nowhere in the literature is the inherent sieve method in Turán’s derivation clearly exposed. The purpose of this chapter is to derive the “Turán sieve method” and indicate some of its application to normal order problems.

1.2 The Turán Sieve.

Let $S$ be a finite set and $I$ be an index set. For each $i \in I$, we use $\Omega(i)$ to denote some specified conditions and we define a set

$$S_i = \{ s \in S : s \text{satisfies } \Omega(i) \}.$$  

For each $s \in S$, we define

$$\pi_s(I) = \# \{ i \in I : s \text{satisfies } \Omega(i) \}.$$  

Since $S$ is a finite set, we can write

$$\frac{|S_i|}{|S|} = \delta_i + r_i,$$

where $r_i$ is chosen to be relatively small with respect to $\delta_i$.

We also assume that for different $i, j \in I$,

$$\frac{|S_i \cap S_j|}{|S|} = \delta_i \delta_j + r_{i,j},$$

where $r_{i,j}$ is chosen to be relatively small with respect to $\delta_i \delta_j$. In other words, we think of $\delta_i$ as an approximation for $\frac{|S_i|}{|S|}$ and $r_i$ as the “error”. We say $S_i$ and $S_j$ are quasi-independent.
Theorem 1.1 (The Turán sieve) Let \( \nu = \sum_{i \in I} \delta_i \). Then,

\[
\frac{1}{|S|} \sum_{s \in S} (\pi_s(I) - \nu)^2 = \sum_{i \in I} \delta_i(1 - \delta_i) + \sum_{i,j \in I} r_{i,j} - 2\nu \sum_{i \in I} r_i,
\]

where we use the convention that \( r_{i,i} = r_i \).

Before giving the proof of Theorem 1.1, we give a corollary.

Corollary 1.2

\[
\#\{s \in S : \pi_s(I) = 0\} \leq \frac{|S|}{\nu} + \frac{|S|}{\nu^2} \sum_{i,j \in I} |r_{i,j}| + \frac{2|S|}{\nu} \sum_{i \in I} |r_i|.
\]

Proof: Since \((1 - \delta_i) \leq 1\), by Theorem 1.1,

\[
\sum_{s \in S} (\pi_s(I) - \nu)^2 \leq |S| \nu + |S| \sum_{i,j \in I} |r_{i,j}| + 2|S| \sum_{i \in I} |r_i|.
\]

Noting that

\[
\nu^2 \#\{s \in S : \pi_s(I) = 0\} \leq \sum_{s \in S} (\pi_s(I) - \nu)^2,
\]

Corollary 1.2 follows.

Remark. For people who are familiar with some basic terminologies in statistics, the left hand side of the equation in Theorem 1.1, 

\[
\frac{1}{|S|} \sum_{s \in S} (\pi_s(I) - \nu)^2,
\]

can be interpreted in the following way: for each \( i \in I \), let \( X_i : S \rightarrow \{0, 1\} \) be a discrete random variable with the uniform distribution. We define

\[
X_i(s) = \begin{cases} 
1 & \text{if } s \in S_i, \\
0 & \text{if } s \notin S_i.
\end{cases}
\]
From the definition of $X_i$, $E(X_i) = \frac{|S_i|}{|S|} \sim \delta_i$.

Let $X = \sum_{i \in I} X_i$ be a discrete random variable with the uniform distribution. We have that

$$X(s) = \#\{i \in I : s \in \Omega(i)\} = \pi_s(I),$$

and

$$E(X) = \sum_{i \in I} E(X_i) \sim \sum_{i \in I} \delta(i) = \nu.$$

Hence,

$$\frac{1}{|S|} \sum_{s \in S} (\pi_s(I) - \nu)^2 = \sum_{s \in S} (X(s) - \nu)^2 P(s)$$

$$\sim \sum_{s \in S} (X(s) - E(X))^2 P(s)$$

$$= Var(X).$$
Proof of Theorem 1.1:

\[
\frac{1}{|S|} \sum_{s \in S} (\pi_s(I) - \nu)^2 = \frac{1}{|S|} \sum_{s \in S} (\pi_s(I))^2 - \frac{2\nu}{|S|} \sum_{s \in S} \pi_s(I) + \nu^2
\]

\[= S_1 - S_2 + \nu^2 \text{ (say)}\]

From the definition of \(\pi_s(I)\),

\[S_1 = \frac{1}{|S|} \sum_{s \in S} (\pi_s(I))^2 = \frac{1}{|S|} \sum_{s \in S} (\sum_{i \in s} 1)^2.\]

Interchanging the order of summation and rearranging terms gives:

\[S_1 = \frac{1}{|S|} \sum_{i,j \in I} \sum_{s_i \cap s_j} 1 = \sum_{i,j \in I} \frac{|S_i \cap S_j|}{|S|} + \sum_{i \in I} \frac{|S_i|}{|S|}.\]

By the definition of \(\delta_i, r_i\), and \(r_{i,j}\), one finds

\[S_1 = \sum_{i,j \in I} \delta_i \delta_j + \sum_{i,j \in I} r_{i,j} + \sum_{i \in I} \delta_i + \sum_{i \in I} r_i\]

\[= (\sum_{i \in I} \delta_i)^2 - \sum_{i \in I} \delta_i^2 + \sum_{i,j \in I} r_{i,j} + \sum_{i \in I} \delta_i. \tag{1.1}\]

Similarly, we can show that

\[S_2 = 2\nu \sum_{i \in I} \delta_i + 2\nu \sum_{i \in I} r_i. \tag{1.2}\]

Combining equation (1.1) and (1.2) yields

\[S_1 - S_2 + \nu^2 = (\sum_{i \in I} \delta_i - \nu)^2 + \sum_{i \in I} \delta_i (1 - \delta_i) + \sum_{i,j \in I} r_{i,j} - 2\nu \sum_{i \in I} r_i\]

\[= \sum_{i \in I} \delta_i (1 - \delta_i) + \sum_{i,j \in I} r_{i,j} - 2\nu \sum_{i \in I} r_i.\]

1.3 The Turán sieve on normal order problems.

The following propositions and corollaries can be found in [10].
Proposition 1.3 Let $P$ be the set of all primes and define $P_z = \prod_{p \leq z} p$. For $z \ll x^{1/2}$,

$$\# \{ n \in \mathbb{N} : n \leq x, \text{ such that } \gcd(n, P_z) = 1 \} \ll \frac{x}{\log \log x}.$$ 

Proof: Define $S = \{ n \in \mathbb{N} : n \leq x \}$ and $I = \{ p \in P : p \leq z \}$. For each $p \in I$, we define $\Omega(p)$ be the zero residue class (mod $p$). Hence,

$$S_p = \{ n \in S : n \equiv 0 \pmod{p} \},$$

and for each $n \in S$,

$$\pi_n(I) = \# \{ p \in I : n \equiv 0 \pmod{p} \}.$$

We have

$$\frac{|S_p|}{|S|} = \frac{1}{p} + O\left(\frac{1}{|x|}\right).$$

Choose $\delta_p = 1/p$. For different $p, q \in I$

$$\frac{|S_p \cap S_q|}{|S|} = \frac{1}{pq} + O\left(\frac{1}{|x|}\right).$$

The sets $S_p$ and $S_q$ are quasi-independent and we have $r_p, r_{p,q} = O\left(\frac{1}{|x|}\right)$. Also,

$$\nu = \sum_{p \leq z} \delta_p = \sum_{p \leq z} \frac{1}{p} = \log \log z + O(1).$$

Note that

$$\# \{ n \leq x : \pi_n(I) = 0 \} = \# \{ n \leq x : \gcd(n, P_z) = 1 \}.$$

Applying corollary 1.2, we get

$$\# \{ n \leq x : \gcd(n, P_z) = 1 \} \ll \frac{x}{\log \log z} + \frac{z^2}{(\log \log z)^2} + \frac{2z}{\log \log z}.$$ 

Choosing $z \ll x^{1/2}$, the proposition follows.
Proposition 1.4 (Turán) Define $\nu(n)$ to be the number of distinct prime divisors of $n$. Then

$$
\sum_{n \leq x} (\nu(n) - \log \log x)^2 \ll x \log \log x.
$$

Proof: Set $z = \sqrt{x}$ and let $S$, $I$, $\Omega(p)$, $S_p$ and $\pi_n(I)$ be defined as in the proof of Proposition 1.3. Note that in this case,

$$
\nu = \sum_{p \leq \sqrt{x}} \frac{1}{p} = \log \log x + O(1).
$$

Applying Corollary 1.2, we get that

$$
\sum_{n \leq x} (\pi_n(I) - \log \log x)^2 \ll x \sum_{p \leq \sqrt{x}} \frac{1}{p} \left(1 - \frac{1}{p}\right) + x \sum_{p.q \leq \sqrt{x}} O\left(\frac{1}{x}\right) + 2x\nu \sum_{p \leq \sqrt{x}} O\left(\frac{1}{x}\right)
$$

$$
\ll x \log \log x.
$$

By definition,

$$
\pi_n(I) = \nu(n) + r(n),
$$

where $r(n) = 0$ or 1. Also,

$$
\sum_{n \leq x} (\pi_n(I) - \log \log x)^2 = \sum_{n \leq x} (\nu(n) + r(n) - \log \log x)^2
$$

$$
= \sum_{n \leq x} (\nu(n) - \log \log x)^2 + O\left(\sum_{n \leq x} \nu(n) + \sum_{n \leq x} \log \log x\right).
$$

(1.4)

Note that

$$
\sum_{n \leq x} \nu(n) = \sum_{p \leq x} \sum_{n \leq x \atop n \mid p} 1 = \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor = x \log \log x + O(x) \ll x \log \log x
$$

and

$$
\sum_{n \leq x} \log \log x \ll x \log \log x.
$$

By these observations and equation (1.3) and (1.4), Proposition 1.4 follows.
Corollary 1.5 Let $\delta > 0$, then

$$\# \{ n \in \mathbb{N} : n \leq x \text{ and } |\nu(n) - \log \log x| \geq (\log \log x)^{\frac{1}{2} + \delta} \} \text{ is } o(x).$$

Proof: Define $A_\delta = \{ n \in \mathbb{N} : n \leq x \text{ and } |\nu(x) - \log \log x| \geq (\log \log x)^{\frac{1}{2} + \delta} \}$ and let $N_\delta$ be its order. We have that

$$\sum_{n \in A_\delta} (\nu(n) - \log \log x)^2 \leq N_\delta (\log \log x)^{1 + 2\delta}.$$  

On the other hand, from Proposition 1.4, we have that

$$\sum_{n \leq x} (\nu(n) - \log \log x)^2 \ll x \log \log x.$$  

Hence,

$$N_\delta (\log \log x)^{1 + 2\delta} \leq x \log \log x,$$  

which implies that

$$N_\delta \ll \frac{x}{(\log \log x)^{2\delta}} = o(x).$$

Proposition 1.6 Fix $k \in \mathbb{N}$ and define $\pi_k(x) = \# \{ n \leq x : \nu(n) = k \}$. Then,

$$\pi_k(x) \ll \frac{x}{\log \log x}.$$  

Proof: In the proof of Proposition 1.4, we have shown that:

$$\sum_{n \leq x} (\nu(n) - k - \log \log x)^2 \ll x \log \log x.$$  

It implies that

$$\sum_{n \leq x, \nu(n) = k} (\nu(n) - k - \log \log x)^2 \ll x \log \log x,$$
i.e.,

\[ \pi_k(x)(\log \log x)^2 \ll x \log \log x. \]

Proposition 1.6 follows.

**Remark.** In the special case when \( k = 1, \nu(n) = 1 \) implies that \( n \) is a prime. Hence,

\[ \pi(x) = \#\{\text{primes } \leq x\} \ll \frac{x}{\log \log x}. \]

**Proposition 1.7** Define \( \nu_y(n) = \#\{p: \text{prime } : p|n \text{ and } p \leq y\} \). Then,

\[ \sum_{n \leq x} (\nu_y(n) - \log \log y)^2 \ll x \log \log x. \]

**Proof:** Replace \( I = \{p \in P : p \leq y\} \) in the proof of Proposition 1.3.
Chapter 2

Probabilistic Galois Theory in $\mathbb{Q}$.

2.1 Introduction.

Fix $n \in \mathbb{N}$ and let $F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$. We denote $\text{Gal}(F)$ to be the Galois group of the splitting field of $F$ over $\mathbb{Q}$. Since $F(x)$ is of degree $n$, $\text{Gal}(F)$ is a subgroup of $S_n$. The probabilistic Galois theory problem is to estimate the number of monic polynomials of degree $n$ whose Galois group is a proper subgroup of $S_n$.

We define the height of $F$, $H(F)$, to be

$$H(F) = \max\{1, |a_1|, |a_2|, \ldots, |a_n|\}.$$ 

Also, we denote

$$E_n(N) = \# \{F(x) \in \mathbb{Z}[x] : \deg(F) = n, F \text{ is monic, } H(F) \leq N \text{ and } \text{Gal}(F) \nsubseteq S_n\}.$$ 

In 1936, van der Waerden [15] gave an upper bound for $E_n(N)$. He proved that

$$E_n(N) \ll N^{\frac{n}{\log \log N}}$$

with $c = \frac{1}{6(n-2)}$. He also conjectured that

$$E_n(N) \ll N^{n-1}$$

16
for $n \geq 3$. 

In 1955, Knobloch [5] [6] improved the result of van der Waerden to

$$E_n(N) \ll N^{n-c}$$

with $c = \frac{1}{18n(n!)^3}$.

In 1973, using the technique of the large sieve in several variables, Gallagher [2] sharpened the result to

$$E_n(N) \ll N^{n-1/2} \log N.$$ 

In this chapter, using the Turán sieve, we prove that

$$E_n(N) \ll N^{n-1/3}(\log N)^2.$$ 

**Remark 1.** Though our result is weaker than Gallagher’s, our method of the Turán sieve is far simpler.

**Remark 2.** Let $F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ with $a_n = 0$. Then, $F(x)$ is a reducible polynomial, which implies that $\text{Gal}(F)$ is a proper subgroup of $S_n$. From this observation and the fact that the order of such polynomials is $N^{n-1}$, we get that

$$E_n(N) \gg N^{n-1}.$$ 

Hence, if the conjecture of van der Waerden is true, i.e.,

$$E_n(N) \ll N^{n-1},$$

the right order of $E_n(N)$ is $N^{n-1}$. 

17
2.2 The Möbius function.

2.2.1 Definition of the Möbius function.

Definition: The Möbius function $\mu : \mathbb{N} \rightarrow \{0, \pm 1\}$ is defined to be:

$$
\mu(n) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } n \text{ is not square-free} \\
(-1)^k & \text{if } n \text{ is square-free and } n = p_1 p_2 \cdots p_k, \text{ where } p_i \text{ are distinct primes.}
\end{cases}
$$

Proposition 2.1 If $n \in \mathbb{N}$, $n > 1$, then $\sum_{d|n} \mu(d) = 0$.

Proof: Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $p_i$ are distinct primes. Let $N = p_1 p_2 \cdots p_k$.

By definition of the Möbius function, we have that

$$
\sum_{d|n} \mu(d) = \sum_{d|N} \mu(d) = \sum_{r=0}^{k} (-1)^r \binom{k}{r} = (1 - 1)^k = 0.
$$

2.2.2 The Möbius inversion formula.

Proposition 2.2 Suppose $f$ and $g$ are two functions on $\mathbb{N}$. The following are equivalent:

1. $f(n) = \sum_{d|n} g(d)$.
2. $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$.
Proof:

(1) $\Rightarrow$ (2)

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) f(e)$$

$$= \sum_{d|n} \mu(d) \sum_{ht=e} g(h)$$

$$= \sum_{dht=n} \mu(d) g(h)$$

$$= \sum_{hf=n} g(h)\left(\sum_{d|f} \mu(d)\right) \text{ (note: if } f \neq 1, \sum_{d|f} \mu(d) = 0\right)$$

$$= \sum_{hf=n} g(h) \quad \text{ (if } f = 1)$$

$$= g(n)$$

(2) $\Rightarrow$ (1)

$$\sum_{d|n} g(d) = \sum_{dr=n} \sum_{et=d} \mu(e) f(t)$$

$$= \sum_{et=r=n} \mu(e) f(t)$$

$$= \sum_{th=n} f(t)\left(\sum_{e|h} \mu(e)\right) \text{ (note: if } h \neq 1, \sum_{e|h} \mu(e) = 0\right)$$

$$= \sum_{h=n} f(t) \quad \text{ (if } h = 1)$$

$$= f(n)$$
2.3 Monic irreducible polynomials in $\mathbb{F}_p[x]$. 

Let $\mathbb{F}_p$ be the finite field and let $\mathbb{F}_p[x]$ be the ring of polynomials in $x$ with coefficients in $\mathbb{F}_p$. It is a Euclidean domain, and hence is a unique factorization domain.

Let

$$A = \{ f(x) \in \mathbb{F}_p[x] : f(x) \text{ is monic} \}.$$

Consider $\sum_{f \in A} T^{\deg(f)}$. Applying the method used to prove the Euler product for the Riemann zeta-function, we can write

$$\sum_{f \in A} T^{\deg(f)} = \prod_{\substack{p \in A \\ p \text{ is irreducible}}} (1 + T^{\deg(p)} + T^{2\deg(p)} + \ldots)$$

$$= \prod_{\substack{p \in A \\ p \text{ is irreducible}}} (1 - T^{\deg(p)})^{-1}.$$

Let

$$N_d = \# \{ p \in A : p \text{ is irreducible and } \deg(p) = d \}.$$

By definition of $N_d$,

$$\prod_{\substack{p \in A \\ p \text{ is irreducible}}} (1 - T^{\deg(p)})^{-1} = \prod_{d=1}^{\infty} (1 - T^d)^{-N_d}.$$

For a fixed degree $n$, the number of polynomials in $A$ with degree $n$ is $p^n$. So, we have that

$$\sum_{f \in A} T^{\deg(f)} = \sum_{n=0}^{\infty} p^n T^n = \frac{1}{1 - pT}.$$

Combining the above equations, we obtain the following lemma.

Lemma 2.3

$$\frac{1}{1 - pT} = \prod_{d=1}^{\infty} (1 - T^d)^{-N_d}.$$
Lemma 2.4

\[ \frac{p^n}{n} = \sum_{de=n} \frac{N_d}{e}. \]

Proof: Taking logarithm on both sides of Lemma 2.3, we get that

\[ -\log(1 - pT) = -\sum_{d=1}^{\infty} N_d \log(1 - T^d). \]

Applying the identity \(-\log(1 - x) = \sum_{n=1}^{\infty} \frac{x^n}{n}\), we can write that

\[ -\log(1 - pT) = \sum_{n=1}^{\infty} \frac{p^n T^n}{n}. \]

and

\[ -\sum_{d=1}^{\infty} N_d \log(1 - T^d) = \sum_{d=1}^{\infty} N_d \sum_{e=1}^{\infty} \frac{T^{de}}{e} = \sum_{n=1}^{\infty} T^n \left( \sum_{de=n} \frac{N_d}{e} \right). \]

Comparing the coefficient of \(T^n\) in these two equations, the lemma follows.

Theorem 2.5

\[ N_n = \frac{1}{n} \sum_{d\mid n} \mu(d) p^{n/d}. \]

Proof: From Lemma 2.4, we obtain that

\[ p^n = \sum_{de=n} N_d \frac{n}{e} = \sum_{d\mid n} dN_d. \]

If we define \(f(n) = p^n\), \(g(d) = dN_d\), we get the relation that

\[ f(n) = \sum_{d\mid n} g(d). \]

Applying the Möbius inversion formula, we get that
\[ nN_n = g(n) \]
\[ = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right) \]
\[ = \sum_{d \mid n} \mu(d)p^{\frac{\lambda}{d}}. \]

It follows that

\[ N_n = \frac{1}{n} \sum_{d \mid n} \mu(d)p^{\frac{\lambda}{d}}. \]

**Corollary 2.6** Fix \( n \in \mathbb{N} \). There exists at least one monic irreducible polynomial in \( \mathbb{F}_p[x] \) which is of degree \( n \).

**Proof:** To prove this corollary, it suffices to show that \( N_n \) is positive. Consider the numbers \( p^n \) and \( \sum_{\substack{d \mid n \\ d \neq n}} p^{\frac{\lambda}{d}} \) in \( p \) base. The former is an \((n + 1)\) digit number, but the latter can only have at most \( n \) digits. Hence,

\[ p^n > \sum_{\substack{d \mid n \\ d \neq n}} p^{\frac{\lambda}{d}}. \]

It follows that

\[ N_n = \frac{1}{n} \sum_{d \mid n} \mu(d)p^{\frac{\lambda}{d}} \geq \frac{1}{n}(p^n - \sum_{\substack{d \mid n \\ d \neq n}} p^{\frac{\lambda}{d}}) > 0. \]

### 2.4 Two definitions of types and their relations.

**Definition:** Let \( F(x) \in \mathbb{Z}[x] \) is monic and of degree \( n \). For a prime \( p \), if the factorization of \( F(x) \) (mod \( p \)) is a product of \( r_1 \) linear factors, \( r_2 \) quadratic factors, \( r_3 \) cubic factors and etc, we say that \( F(x) \) has **mod \( p \) type** \( r = (r_1, r_2, r_3, \cdots) \).
Remark. Since \( F(x) \) has degree \( n \), \( \sum_k r_k k = n \).

**Definition:** Let \( \sigma \) be a permutation of \( S_n \). Up to the order, we can write \( \sigma \) as a product of disjoint cycles in a unique way. If \( \sigma \) has \( r_1 \) cycles of length 1, \( r_2 \) cycles of length 2 and etc, we say that \( \sigma \) has cycle type \( r = (r_1, r_2, \cdots) \).

**Remark 1.** Since \( \sigma \in S_n \), \( \sum_k r_k k = n \).

**Remark 2.** Two permutations of \( S_n \) are conjugate to each other if and only if they have the same cycle type. Hence, each cycle type can serve as a "label" for each conjugacy class.

Let \( F(x) \in \mathbb{Z}[x] \) be a monic polynomial of degree \( n \) and \( \text{Gal}(F) \) be its Galois group. We can view \( \text{Gal}(F) \) as a permutation group on the roots of \( F \) after choosing a labelling of the roots of \( F \). It is a subgroup of \( S_n \).

Considering \( \text{Gal}(F) \) to be a subgroup of \( S_n \), we can relate the mod \( p \) type of \( F(x) \) and the cycle type of permutations of \( \text{Gal}(F) \) in the following way:

**Theorem 2.7** Fix a monic polynomial \( F(x) \in \mathbb{Z}[x] \) which is of degree \( n \). Let \( r = (r_1, r_2, \cdots) \) be a type with \( \sum_k r_k k = n \). The following are equivalent: (This is essentially a consequence of the Chebotarev density theorem, see [1] and [3])

1. There exists a prime \( p \) such that \( F(x)(\text{mod } p) \) is of type \( r \).
2. There exists a permutation \( \sigma \in \text{Gal}(F) \subseteq S_n \) whose cycle type is \( r \).

2.5 Elementary group theory.

**Lemma 2.8** Suppose that \( G \) is a subgroup of a finite group \( H \). Let \( N(G) \) be the normalizer of \( G \) in \( H \), i.e. \( N(G) = \{ h \in H : hGh^{-1} = G \} \). Then, the number of
Conjugates of \( G \) in \( H \) is equal to \([H : N(G)]\).

**Proof:** Let \( S \) be the set of conjugates of \( G \) in \( H \), i.e., \( S = \{hGh^{-1}, \forall h \in H\} \). The group \( H \) acts transitively on \( S \) by conjugation.

\[
\alpha : H \times S \rightarrow S
\]

\[
h \cdot \tilde{G} \mapsto h\tilde{G}h^{-1}.
\]

Applying the counting formula for \( \alpha \), we get that

\[ |H| = |\text{Stab}(G)||\text{Orb}(G)|, \]

where \( \text{Stab}(G) \) is the stabilizer of \( G \) and \( \text{Orb}(G) \) is the orbit of \( G \), i.e.,

\[ \text{Stab}(G) = \{h \in H : hGh^{-1} = G\} \]

and

\[ \text{Orb}(G) = \{hGh^{-1}, \forall h \in H\}. \]

Notice that from the definition of \( \alpha \),

\[ \text{Stab}(G) = N(G). \]

and

\[ \text{Orb}(G) = \text{the conjugates of } G. \]

The lemma follows.

**Lemma 2.9** If \( G \) is a proper subgroup of a finite group \( H \), then the conjugates of \( G \) cannot cover the whole \( H \).
Proof: From Lemma 2.8,
\[
\#\{hGh^{-1}, \forall h \in H\} = [H : N(G)].
\]
Each conjugacy class contains the same number of elements with \(G\) and each one of them contains the identity element of \(H\). So,
\[
\#\{hgh^{-1}, h \in H, g \in G\} \leq [H : N(G)](|G| - 1) + 1
\]
\[\leq [H : G](|G| - 1) + 1 \text{ (since } G \subseteq N(G)\)
\[= |H| - [H : G] + 1
\[< |H| \text{ (since } G \nsubseteq H \text{ implies } [H : G] \geq 2\).
\]

Lemma 2.10 If \(G\) is a proper subgroup of \(H\), then there exists at least one conjugacy class \(C \subseteq H\) such that \(G \cap C = \emptyset\).

Proof: Suppose there is no such class. Then, by definition, the union of the conjugates of \(G\) is all of \(H\), contradicting Lemma 2.9.

2.6 The Turán sieve on \(E_n(N)\).

2.6.1 Lowering the level of the original question.

Consider a monic polynomial \(F(x) \in \mathbb{Z}[x]\) with degree \(n\). We supposed that the Galois group of \(F\), \(\text{Gal}(F)\), is a proper subgroup of \(S_n\). By Lemma 2.10, there exists \(\sigma \in S_n\) whose conjugacy class is disjoint from \(\text{Gal}(F)\). Suppose that \(\sigma\) is of cycle type \(r\). By Theorem 2.7, the factorization of \(F(x) \pmod{p}\) is not be of \(\text{mod } p\) type \(r\) for all primes \(p\). Hence, to obtain an upper bound for
\[
E_n(N) = \#\{F(x) \in \mathbb{Z}[x] : \deg(F) = n, F \text{ is monic, } H(F) \leq N \text{ and } \text{Gal}(F) \nsubseteq S_n\},
\]
it suffices to get an upper bound for

\[ E_{r,n}(N) = \#\{F(x) \in E_n(N) : F \text{ does not have mod } p \text{ type } r \text{ for all primes } p\}. \]

Summing \( E_{r,n}(N) \) over all possible types \( r \), we get an upper bound for \( E_n(N) \).

**Remark.** There is a uniform upper bound for \( E_{r,n}(N) \) for all types \( r \). Since the number of all types \( r \) is bounded (say, by the number of the conjugacy classes of \( S_n \)), the order of an upper bound for \( E_n(N) \) is equal to the one of \( E_{r,n}(N) \).

## 2.6.2 The Turán sieve on \( E_{r,n}(N) \).

Fix a type \( r = (r_1, r_2, \cdots) \) with \( \sum_k r_k k = n \). We want to estimate that

\[ E_{r,n}(N) = \#\{F(x) \in E_n(N) : F \text{ does not have mod } p \text{ type } r \text{ for all primes } p\}. \]

**Lemma 2.11** Fix a type \( r = (r_1, r_2, \cdots) \) with \( \sum_k r_k k = n \). There are \((\delta(r)p^n + O(p^{n-1}))\) many monic polynomials in \( \mathbb{F}_p[x] \) with degree \( n \) and of type \( r \), where \( \delta(r) = \prod_k \frac{1}{r_k!k^{r_k}} \). We denote the number of such polynomials by \( \omega(p) \).

**Proof:** We recall the definition of mod \( p \) type. Let \( F(x) \in \mathbb{Z}[x] \) be monic and be of degree \( n \). If \( F(x) \) has \( r_1 \) linear factors, \( r_2 \) quadratic factors and etc, we say that \( F(x) \) is of mod \( p \) type \( r = (r_1, r_2, \cdots) \). In Theorem 2.5, we counted the number of monic irreducible polynomials of degree \( k \) over \( \mathbb{F}_p \) is \( N_k \),

\[ N_k = \frac{1}{k} \sum_{d|k} \mu(d)p^{k/d} \sim \frac{p^k}{k}. \]

Hence, we have that

\[ \#\{\text{monic polynomials in } \mathbb{F}_p[x] \text{ with degree } n \text{ and of type } r\} \]
Lemma 2.12 Fix a type $r = (r_1, r_2, \ldots)$. There are

$$\left( \frac{(2N + 1)^n \omega(p)}{p^n} + O\left( \frac{N^{n-1}}{p^{n-1}} \omega(p) \right) \right)$$

many monic polynomials in $\mathbb{Z}[x]$ with height $\leq N$ which have mod $p$ type equal to $r$.

Proof: Fix a polynomial $x^n + u_1 x^{n-1} + \cdots + u_n$ in $\mathbb{F}_p[x]$. We consider the number of polynomials $x^n + a_1 x^{n-1} + \cdots + a_n$, $a_i \in \mathbb{Z}, |a_i| \leq N$ that satisfy $a_i \equiv u_i \pmod{p}$, which is equal to

$$\left( \frac{2N + 1}{p} + O(1) \right)^n = \left( \frac{2N + 1}{p} \right)^n + O\left( \left( \frac{N}{p} \right)^{n-1} \right).$$

Applying Lemma 2.11, the number of monic polynomials in $\mathbb{Z}[x]$ which are of degree $n$ and have mod $p$ type equal to $r$ is

$$\left( \frac{(2N + 1)^n}{p^n} + O\left( \left( \frac{N}{p} \right)^{n-1} \right) \right) \omega(p).$$

Theorem 2.13 Fix a type $r$, then

$$E_{r,n}(N) \ll N^{n-1/3} (\log N)^2.$$

Proof: The proof is an application of the Turán sieve.

Let $S = \{ s = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n, |a_i| \leq N \}$. For each $s \in S$, we define $F(s) =$
\[ x^n + a_1 x^{n-1} + \cdots + a_n. \] Let \( I = \{ p : p \text{ is a prime and } p \leq z \}. \) For each \( p \in I, \) we define \( \Omega(p) \) to be the condition that \( F(s) \pmod{p} \) is of type \( r. \) Hence,

\[ S_p = \{ s \in S : F(s) \pmod{p} \text{ is of type } r \} \]

and

\[ \pi_s(I) = \# \{ p \in I : F(s) \pmod{p} \text{ is of type } r \}. \]

From Lemma 2.12,

\[ |S_p| = (2N + 1)^n \frac{\omega(p)}{p^n} + O\left( \frac{N^{n-1}}{p^{n-1}} \right). \]

Since

\[ |S| = (2N + 1)^n, \]

we have that

\[ \frac{|S_p|}{|S|} = \frac{\omega(p)}{p^n} + O\left( \frac{\omega(p)}{p^{n-1}} \right). \]

We set \( \delta_p = \frac{\omega(p)}{p^n} \) and \( r_p = O\left( \frac{\omega(p)}{p^{n-1} N} \right). \) For different primes \( p, q, \) in \( I, \)

\[ \frac{|S_p \cap S_q|}{|S|} = \frac{\omega(p) \omega(q)}{p^n q^n} + O\left( \frac{\omega(p) \omega(q)}{p^{n-1} q^{n-1} N} \right), \]

i.e., \( S_p \) and \( S_q \) are quasi-independent. We also have that

\[ \nu = \sum_{p \leq z} \frac{\omega(p)}{p^n} \sim \delta(r) \frac{z}{\log z}. \]
Applying Corollary 1.2, we get that

$$E_{r,n}(N) = \# \{ F(x) \in \mathbb{Z}[x] : \text{deg}(F) = n, F : \text{monic}, H(F) \leq N, \text{Gal}(F) \subseteq S_n \text{ and } F(x) \pmod{p} \text{ is not of type } r \text{ for all primes } p \}$$

$$\leq \# \{ s \in S, \pi_s(P) = 0 \}$$

$$\leq \frac{|S|}{\nu} + \frac{|S|}{\nu^2} \sum_{p,q \leq z} |r_{p,q}| + \frac{2|S|}{\nu} \sum_{p \in \mathbb{P}} |r_p|$$

$$\ll \frac{N^n \log z}{z} + \frac{N^n (\log z)^2}{z^2} \sum_{p,q \in \mathbb{P}} \frac{pq}{N} + \frac{N^n \log z}{z} \sum_{p \leq z} \frac{p}{N} \quad \text{(note: } \omega(p) \leq p^n)$$

$$\ll \frac{N^n (\log z)^2}{z} \left( 1 + \frac{z^3}{N} \right).$$

Choosing $$z = N^{1/3}$$, we get that

$$E_{r,n}(N) \ll N^{n-1/3} (\log N)^2.$$ 

**Conclusion.** As we have mentioned in Section 2.6.1,

$$E_{r,n}(N) \ll N^{n-1/3} (\log N)^2$$

implies that

$$E_n(N) \ll N^{n-1/3} (\log N)^2.$$ 

In other words, the number of polynomials $$x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$$ with height $$\leq N$$ and whose Galois groups are proper subgroups of $$S_n$$ is $$\ll N^{n-1/3} (\log N)^2$$. Since there are $$(2N + 1)^n$$ many monic polynomials in $$\mathbb{Z}[x]$$ with height $$\leq N$$, we conclude that “almost all” monic polynomials of degree $$n$$ in $$\mathbb{Z}[x]$$ have Galois group equal to $$S_n$$. 

29
Chapter 3

The Galois Groups of Cubics and Trinomials

3.1 Introduction.

In the previous chapter, using the Turán sieve, we proved that

\[ E_n(N) = \# \{ F(x) \in \mathbb{Z}[x] : \deg(F) = n, F \text{ is monic}, H(F) \leq N \text{ and } \text{Gal}(F) \subseteq S_n \} \leq N^{n-\frac{1}{2}}(\log N)^2. \]

It implies that almost all polynomials in \( \mathbb{Z}[x] \) of degree \( n \) have Galois group equal to \( S_n \). The most efficient upper bound for \( E_n(N) \) is given by Gallagher in 1973 [2]. Using the large sieve in several variables, he proved that

\[ E_n(N) \ll N^{n-\frac{1}{2}} \log N. \]

In the special case when \( n = 3 \), using the 'discriminant and quadratic form argument', Lefton [7] improved the result of Gallagher. She proved that

\[ E_3(N) \leq N^{2+\varepsilon}. \]
Moreover, she also gave an upper bound for trinomials in \( \mathbb{Z}[x] \) of the form

\[
f(x) = ax^n + bx^k + c
\]

whose Galois group is a subgroup of the alternating group \( A_n \). In this chapter, we are going to proceed as in [7]. Moreover, at the end of this chapter, we will provide another approach on the above two problems by using the Turán sieve to give a more analytical flavour of these theorems.

### 3.2 Preliminaries.

**Proposition 3.1** Let \( r \in \mathbb{N} \). Define

\[
d_r(n) = \#\{ \text{factorizations of } n \text{ into } r \text{ positive divisors, taking their orders into account.}\}
\]

Then for all \( \epsilon > 0 \),

\[
d_r(n) \ll n^\epsilon.
\]

**Proof:** Let \( d(n) \) denote the number of positive divisors of \( n \). Since

\[
d_{r+1}(n) \ll d(n)d_r(n), \forall r \geq 1,
\]

to prove this lemma, it suffices to show that

\[
d_2(n) = d(n) \ll n^\epsilon.
\]

Writing \( n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k} \), we have that

\[
d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).
\]
Hence, for all $\epsilon > 0$,

\[
\frac{d(n)}{n^\epsilon} = \prod_{i=1}^{k} \frac{\alpha_i + 1}{p_i^{\alpha_i \epsilon}} \leq \prod_{\substack{p \text{ prime} \, \frac{n+1}{p^\epsilon} \geq 1}} \frac{n+1}{p^{n^\epsilon}}.
\]

Since

\[
\frac{n+1}{p^{n^\epsilon}} \to 0 \quad \text{as} \quad p \to \infty \quad \text{or} \quad n \to \infty,
\]

there are only finitely many terms in the set \(\{\frac{n+1}{p^{n^\epsilon}}, n \in \mathbb{N}, p : \text{prime}\}\) which are $\geq 1$. It means that \(\prod_{\substack{p \text{ prime} \, \frac{n+1}{p^\epsilon} \geq 1}} \frac{n+1}{p^{n^\epsilon}}\) is bounded by a constant. So, we can conclude that

\[
d(n) \ll n^\epsilon,
\]

which implies that

\[
d_r(n) \ll n^\epsilon.
\]

**Remark.** By definition of $d_r(n)$, since 1 is a factor of every integer, we have that \(d(n) = d_2(n) \leq d_3(n) \leq d_4(n) \leq \cdots\).

**Proposition 3.2** [11] Let $K$ be a number field with $[K : \mathbb{Q}] = n$ and let $\mathcal{O}_K$ be its ring of integers. For $m \in \mathbb{N}$, define

\[
\pi_K(m) = \#\{i : i \text{ is an ideal of } \mathcal{O}_K \text{ and } N(i) = m\},
\]

where $N(i)$ denotes the 'norm' of $i$ in $\mathcal{O}_K$, i.e., the cardinality of $\mathcal{O}_K/i$. Then,

\[
\pi_K(m) \ll m^\epsilon.
\]
Proof: Notice that every ideal of norm $mn$ with $\gcd(m, n) = 1$ is a unique product of ideals with norm $m$ and $n$ respectively. Hence,

$$\pi_K(mn) = \pi_K(m)\pi_K(n), \text{ for } \gcd(m, n) = 1.$$ 

So, without loss of generality, we can assume $m = p^r$ for some prime $p$ and $r \in \mathbb{N}$. We prove that $\pi_K(m) = \pi_K(p^r) \ll (p^r)^t$. Since $\mathcal{O}_K$ is a Dedekind domain, up to the order, we can write the principal ideal generated by $p$ in $\mathcal{O}_K$, $p\mathcal{O}_K$, as a product of prime ideals in $\mathcal{O}_K$ in a unique way. Suppose that

$$p\mathcal{O}_K = p_1^{e_1}p_2^{e_2} \cdots p_s^{e_s},$$

where $p_i$ are distinct prime ideals in $\mathcal{O}_K$.

Give an ideal $i$ in $\mathcal{O}_K$ with $N(i) = p^r$ and let $p$ be a prime ideal which divides $i$. Using the properties of norm of ideals, we get that

$$p|i \Rightarrow N(p)|N(i).$$

$$\Rightarrow N(p) \text{ is a power of } p.$$ 
$$\Rightarrow p = p_i \text{ for some prime factor } p_i \text{ of } p\mathcal{O}_K.$$ 

Hence, we can write

$$i = p_1^{f_1}p_2^{f_2} \cdots p_s^{f_s},$$

which implies that

$$p^r = N(i) = N(p_1)^{f_1}N(p_2)^{f_2} \cdots N(p_s)^{f_s}.$$ 

For each $i, 1 \leq i \leq s$, $N(p_i)$ is a power of $p$. Hence, from the above equation, every ideal $i$ in $\mathcal{O}_K$ with $N(i) = p^r$ induces a factorization of $p^r$. If $j$ is another ideal in $\mathcal{O}_K$
which induces the same factorization of $p^r$, $j$ is equal to $i$. So,

$$
\pi_K(m) = \pi_K(p^r) \\
\leq d_s(p^r) \\
\leq d_n(p^r) \text{ (since } s \leq n) \\
\ll (p^r)^e.
$$

**Proposition 3.3** Let $d$ be a square-free integer, $d \geq 2$. Consider the real quadratic field $K = \mathbb{Q}(\sqrt{d})$ and let $\eta_K$ denotes its fundamental unit, $\eta_K > 1$. Then there exists a constant $c$ which does not depend on $K$ such that $\log \eta_K \geq c$ for all real quadratic fields $K$.

**Proof:** The proposition is a consequence of the construction of the fundamental unit. There are two cases for constructing the fundamental unit of a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ [9].

**Case(i):** $d \equiv 2, 3 \pmod{4}$. Consider $db^2 \pm 1$, where $b$ is a positive integer. Choose the smallest $b$ such that either $db^2 + 1$ or $db^2 - 1$ is a square of integers, say $a^2$, $a > 0$. Then $\eta_K = a + b\sqrt{d}$ is the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$. Since $a, b > 0$ and $d \geq 2$, we have that

$$
\log \eta_K \geq \log \sqrt{d} \geq \frac{1}{2} \log 2.
$$

**Case(ii):** $d \equiv 1 \pmod{4}$. Consider $db^2 \pm 4$, where $b$ is a positive integer. Choose the smallest $b$ such that either $db^2 + 4$ or $db^2 - 4$ is a square of integers, say $a^2$, $a > 0$. Then $\eta_K = \frac{1}{2}(a + b\sqrt{d})$ is the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$. Since $a, b > 0$ and $d \geq 5$, we have that

$$
\log \eta_K \geq \log \frac{\sqrt{5}}{2} \leq \frac{1}{4} \log 2.
$$

Choosing $c = \frac{1}{4} \log 2$, the proposition follows.
3.3 Integer solutions of quadratic forms.

Lemma 3.4 Fix a non-zero integer $d$ and a positive integer $m$. The number of integer solutions $(x, y)$ of $x^2 - dy^2 = m$ with $|x|, |y| \leq M$ is

$$\# \{(x, y) \in \mathbb{Z}^2 : x^2 - dy^2 = m\} \ll \begin{cases} m^\epsilon & \text{if } d < 0 \\ (mdM)\epsilon & \text{if } d > 0. \end{cases}$$

Proof: Without loss of generality, we can assume that $d$ is square-free. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Suppose we have a pair $(a, b) \in \mathbb{Z}^2$ such that $a^2 - db^2 = m$. Let $\alpha = a + b\sqrt{d} \in K$ and we denote $(\alpha)$ to be the principal ideal generated by $\alpha$. Then, the norm of $(\alpha)$, $N((\alpha))$, is

$$N((\alpha)) = a^2 - db^2 = m.$$ 

Hence, we observe that every integer solution of $x^2 - dy^2 = m$ induces a principal ideal $\mathfrak{a} = (\alpha)$ whose norm is equal to $m$.

Let $\epsilon > 0$. Applying Proposition 3.2, we have that

$$\# \{\mathfrak{a} : \mathfrak{a} \text{ is a principal ideal of } \mathcal{O}_K \text{ and } N(\mathfrak{a}) = m\} \ll m^\epsilon.$$ 

Now, to complete the proof of the lemma, we need to count the number of generators of $\mathfrak{a} = (\alpha)$ where $\alpha$ is of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ and $|a|, |b| \leq M$. We know that if two elements $\alpha, \beta$ of $\mathcal{O}_K$ generate the same ideal, then $\alpha = u\beta$ for some unit $u \in \mathcal{O}_K$.

We proceed the proof by considering three different cases according to the value of $d$.

Case (i): $d < 0$. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. There are at most six units of $\mathcal{O}_K$. So,

$$\# \{\mathfrak{a} : \mathfrak{a} \text{ is a principal ideal of } \mathcal{O}_K \text{ and } N(\mathfrak{a}) = m\} \ll m^\epsilon.$$
implies that
\[
\#\{(x, y) \in \mathbb{Z}^2 : x^2 - dy^2 = m \text{ with } |x|, |y| \leq M\} \ll m^\epsilon.
\]

**Case (ii):** \(d = 1\). We write that \(m = x^2 - y^2 = (x + y)(x - y)\), i.e., every integer solution \((x, y)\) of \(x^2 - y^2 = m\) induces a factorization of \(m\). Applying Proposition 3.1, we get that
\[
\#\{(x, y) \in \mathbb{Z}^2 : x^2 - dy^2 = m \text{ and } |x|, |y| \leq M\} \leq d(m) \ll m^\epsilon.
\]

**Case (iii):** \(d > 1\). Then \(K = \mathbb{Q}(\sqrt{d})\) is a real quadratic field and there are infinitely many units of \(\mathcal{O}_K\). We need to estimate how many elements \(\alpha\) in the form \(\alpha = a + b\sqrt{d}\) with \(|a|, |b| \leq M\) in \(\mathcal{O}_K\) will generate the same ideal. Consider \(\alpha = a + b\sqrt{d}, |a|, |b| \leq M\). We assume that \(N((\alpha)) = m\).

Let \(|\alpha|\) be the standard notation for the norm of \(\alpha\), i.e., \(|\alpha|^2 = (a + b\sqrt{d})(a - b\sqrt{d})\) and \(\overline{\alpha}\) be the conjugate of \(\alpha\) in \(K\), i.e., \(\overline{\alpha} = a - b\sqrt{d}\). Then,
\[
|\alpha| \leq M(1 + \sqrt{d})
\]
and
\[
|\overline{\alpha}| \leq M(1 + \sqrt{d}).
\]

Since \(|\alpha\overline{\alpha}| = N((\alpha)) = m \geq 1\), we deduce that
\[
\frac{1}{M(1 + \sqrt{d})} \leq |\alpha| \leq M(1 + \sqrt{d}).
\]

Taking logarithm on both sides, we get that
\[
|\log|\alpha|| \leq \log(M(1 + \sqrt{d})).
\]

Let \(\alpha = (\alpha)\) be a principal ideal of \(\mathcal{O}_K\) with \(N(\alpha) = m\). Suppose \(\alpha\) can be generated by another element of \(\mathcal{O}_K\), say \(\beta = a' + b'\sqrt{d}, a', b' \in \mathbb{Z}\). Since \((\alpha) = (\beta)\), we have
\[ \beta = \eta^i \alpha, \text{ where } \eta \text{ is the fundamental unit of } K, \eta > 1 \text{ and } i \in \mathbb{Z}. \]

Since \( N((\beta)) = m \), we have that

\[ |i \log \eta + \log |\alpha| | = \log |\beta| \leq \log(M(1 + \sqrt{d})), \]

which implies that

\[ \left| i + \frac{\log |\alpha|}{\log \eta} \right| \leq \frac{\log(M(1 + \sqrt{d}))}{\log \eta}. \]

Since \( \frac{1}{\log \eta} \) is bounded by a constant (by Proposition 3.3), the integer \( i \) belongs to an interval of length \( \ll \log(M(1 + \sqrt{d})) \ll (Md)^{\epsilon} \), i.e., for a fixed principal ideal \( \mathfrak{a} \)

\[ \# \{ \alpha \in K : \alpha = a + b\sqrt{d}, |a|, |b| \leq M \text{ and } (\alpha) = \mathfrak{a} \} \ll (Md)^{\epsilon}. \]

Combining this with the fact that

\[ \# \{ a : a \text{ is a principal ideal of } \mathcal{O}_K \text{ and } N(a) = m \} \ll m^{\epsilon}, \]

We get that

\[ \# \{ (x, y) \in \mathbb{Z}^2 : x^2 - dy^2 = m \text{ with } |x|, |y| \leq M \} \ll (Md^n)^{\epsilon}. \]

**Remark.** The same result of Lemma 3.4 holds if we replace \( M \) by \( M^i \).

**Lemma 3.5** Suppose \( Q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f \) is a quadratic form with coefficients in \( \mathbb{Z} \). We also assume that the absolute values of all coefficients of \( Q(x, y) \) are bounded by \( N \). Then,

\[ \# \{ (x, y) \in \mathbb{Z}^2 : Q(x, y) = 0 \text{ with } |x|, |y| \leq M \} \ll (MN)^{\epsilon}. \]

**Proof:** Setting

\[ D = b^2 - 4ac \ll N^2 \]
\[ x' = -Dy + 2ae - bd \ll N^2 M \]
\[ y' = 2ax + by + d \ll N^2 M \]
\[ m = -D(d^2 - 4af) + (2ae - bd)^2 \ll N^4, \]
we can transform \( Q(x, y) = 0 \) into \( Q'(x', y') = 0 \), where \( Q'(x', y') = x'^2 - Dy'^2 \).

Applying Lemma 3.4 and the preceding remark, the lemma follows.

### 3.4 The alternating group.

Let \( S_n \) be the symmetric group and we denote \( A_n \) to be the subgroup of \( S_n \) which consists of all even permutations. \( A_n \) is called the alternating group and \([S_n : A_n] = 2\).

Let \( F(x) \) be a monic polynomial in \( \mathbb{Q}[x] \) of degree \( n \). \( \text{Gal}(F) \) is the Galois group of \( F \). After choosing a labelling of the roots of \( F \), we can view \( \text{Gal}(F) \) as a subgroup of \( S_n \). We would like to know when \( \text{Gal}(F) \) is also a subgroup of \( A_n \).

**Lemma 3.6** [4] Let \( F(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in \mathbb{Q}[x] \), where all the \( \alpha_i \)'s are distinct. We denote \( G \) to be the Galois group of \( F \) and define that

\[
\Delta = \prod_{i<j} (\alpha_i - \alpha_j).
\]

Let \( \mathbb{Q}(\Delta) \) be the field adjointed \( \mathbb{Q} \) with \( \Delta \). We have that

\[
\mathbb{Q}(\Delta) = \text{Fix}(G \cap A_n),
\]

where \( \text{Fix}(G \cap A_n) \) is the subfield of \( K \) which consists of elements in \( K \) that are invariant under \( G \cap A_n \). In other word,

\[
\text{Fix}(G \cap A_n) = \{ \alpha \in K : \sigma(\alpha) = \alpha, \forall \sigma \in G \cap A_n \}.
\]

**Proof:** This lemma follows from Galois theory and the following observation: For \( \alpha \in G = \text{Gal}(F) \),

\[
\alpha(\Delta) = \begin{cases} 
\Delta & \text{if } \alpha \in A_n, \\
-\Delta & \text{if } \alpha \notin A_n.
\end{cases}
\]

38
Lemma 3.7 [4] Let $F(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in \mathbb{Q}[x]$, where all the $\alpha_i$'s are distinct. Consider the Galois group of $F$, $\text{Gal}(F)$. The following are equivalent:

(1) $G = \text{Gal}(F) \subseteq A_n$.

(2) $\delta = \Delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2$ is the square of an element in $\mathbb{Q}$.

Remark. We define the discriminant of $F$ to be $\delta$.

Proof:

(1) $\Rightarrow$ (2)

Suppose that $G \subseteq A_n$. By Lemma 3.6, we have that

$$\mathbb{Q}(\Delta) = \text{Fix}(G \cap A_n) = \text{Fix}(G),$$

i.e., $\Delta$ is invariant under all $\sigma \in G$. By the fundamental theorem of Galois theory, we have that $\text{Fix}(G) = \mathbb{Q}$, which implies that $\Delta$ is an element of $\mathbb{Q}$. In consequence, $\delta = \Delta^2$ is a square of an element of $\mathbb{Q}$.

(2) $\Rightarrow$ (1)

Suppose $\delta$ is a square of element in $\mathbb{Q}$, say $\delta = \alpha^2$, $\alpha \in \mathbb{Q}$. $\Delta^2 = \alpha^2$ implies that $\Delta = \pm \alpha \in \mathbb{Q}$. Since $\Delta \in \mathbb{Q}$, $\mathbb{Q}(\Delta) = \mathbb{Q} = \text{Fix}(G)$. From Lemma 3.6, we have that $\mathbb{Q}(\Delta) = \text{Fix}(G \cap A_n)$. Hence,

$$\text{Fix}(G) = \text{Fix}(G \cap A_n),$$

which implies that

$$G \subseteq A_n.$$

Remark. The results of the above two lemmas hold in any field whose characteristic is $\neq 2$. 

39
3.5 The Galois groups of cubics and trinomials

3.5.1 The Galois groups of cubics

Theorem 3.8 Let $N \in \mathbb{N}$. Define

$$E_3(N) = \# \{ F(x) = x^3 + bx^2 + cx + d \in \mathbb{Z}[x] : \text{Gal}(F) \subseteq S_3, H(F) \leq N \},$$

where $H(F) = \max\{|b|, |c|, |d|\}$. Then, for all $\epsilon > 0$,

$$E_3(N) \ll N^{2+\epsilon}.$$

Remark. Van der Waerden [15] and later Specht [14] showed that

$$\# \{ F(x) \in \mathbb{Z}[x] : \deg(F) = 3, H(F) \leq N \text{ and } F \text{ is reducible} \} \ll N^2.$$

Hence, without loss of generality, we can assume that the polynomials in $E_3(N)$ are all irreducible.

Proof: Given $F(x) = x^3 + bx^2 + cx + d \in E_3(N)$, the discriminant of $F$, $D_F$, is equal to

$$D_F = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd.$$

For $F(x) \in E_3(N)$, since $F(x)$ is irreducible, $\text{Gal}(F)$ is a transitive proper subgroup of $S_3$. It means that $\text{Gal}(F) = A_3$. Applying Lemma 3.7, we have that

$$D_F = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd = z^2$$

for some $z \in \mathbb{Z}$.

Write the above equation in the following way:

$$27(d)^2 + (4b^3 - 18bc)d + z^2 + (4c^3 - b^2c^2) = 0.$$
Fix $b$ and $c$, we can think the above equation as a quadratic form of $d$ and $z$. Applying Lemma 3.5, we obtain that

$$E_3(N) \ll N^{2+\varepsilon}.$$ 

**Remark.** In the same paper of the above theorem, using the same technique, Lefton[1] also proved that: for all $\varepsilon > 0$,

$$\# \{F(x) = x^4 + bx^2 + cx + d : H(f) \leq N, \text{Gal}(F) \subseteq A_4 \} \ll N^{2+\varepsilon}$$

and

$$\# \{F(x) = x^5 + bx^3 + cx + d : H(F) \leq N, \text{Gal}(F) \subseteq A_5 \} \ll N^{2+\varepsilon}.$$ 

### 3.5.2 The Galois groups of trinomials.

**Theorem 3.9** Choose $N \in \mathbb{N}$. Define

$$J_{k,n}(N) = \# \{f(x) = ax^n + bx^k + c \in \mathbb{Z}[x] : H(f) \leq N, \text{Gal}(f) \subseteq A_n \},$$

where $H(f) = \max\{|a|, |b|, |c|\}$. Then, for all $\varepsilon > 0$,

$$J_{k,n}(N) \ll N^{2+\varepsilon}.$$ 

**Proof:** Given $f(x) = ax^n + bx^k + c \in J_{k,n}(N)$, the discriminant $D_f$ of $f$ is equal to

$$D_f = \pm a^{n-k-1} c^{k-1} E^d,$$

where

$$\pm = (-1)^{\frac{n}{2}n(n-1)}, \quad d = \gcd(n,k), \quad n' = \frac{n}{d}, \quad k' = \frac{k}{d} \quad \text{and} \quad E = n' \cdot d^{k'} c^{n'-k'} + (-1)^{n'-1}(n - k)n'c^{k'}b^{n'}.$$ 

41
Since we have assumed $\text{Gal}(f) \subseteq A_n$, by Lemma 3.7, $D_f$ is a square of integers. There are two cases for $d = \gcd(n, k)$.

**Case (i):** $d$ is even. We define $F = a^{n - k - 2} c^{k - 2} E^d$. Since $d$ is even, $n$ and $k$ are both even, which implies that $F \in \mathbb{Z}[a, b, c]$. We have that

$$F^{-2}D_f = \pm ac.$$ 

Since both $D_f$ and $F^{-2}$ are squares of integers, so is $\pm ac$, say $\pm ac = z^2$ for some $z \in \mathbb{Z}$. We have that

$$(a + c)^2 - (a - c)^2 = \pm 4z^2.$$ 

If we fix the value of $(a + c)$ and think the above equation as a quadratic form for $(a - c)$ and $2z$, applying Lemma 3.5, we get that

$$J_{k, n}(N) \ll N^{2+\epsilon}.$$ 

**Case (ii):** $d$ is odd. We define $F = a^{(d-1)(n - k)} c^{(d-1)k} E^{d-1} \in \mathbb{Z}[a, b, c]$. Then,

$$F^{-2}D_f = \pm a^{n' - k' - 1} c^{k' - 1} E.$$ 

Since both $D_f$ and $F^{-2}$ are squares of integers, so is $\pm a^{n' - k' - 1} c^{k' - 1} E$. There are three subcases needed to be considered.

**Case (ii-a):** $n$ is even and $k$ is odd. We have that $n'$ is even and $k'$ is odd. Since both $n' - k' - 1$ and $k' - 1$ are even, we have that $\pm E$ is a square of integers, say $z^2$. We obtain that

$$\pm n'^{n'} a^{k'} c^{n' - k'} = z^2 \pm (n - k)^{n' - k'} k^{k'} (b^{n' / 2})^2,$$ 

where $\pm = (-1)^{n' / 2}$. Fix $a$ and $c$, the above equation can be thought as a quadratic form in $z$ and $b^{n' / 2}$. Applying Lemma 3.7, we get that

$$J_{k, n}(N) \ll \sum_{|a|, |c| \leq N} N^\epsilon \ll N^{2+\epsilon}.$$ 

42
Case (ii-b) $n$ is odd and $k$ is even. We have that $n'$ is odd and $k'$ is even. So, $\pm cE$ is the square of an integer, say $z^2, z \in \mathbb{Z}$. We get that

$$\pm (n - k)^{n'} k'^{k'} b^n c = z^2 \mp n^{n'} c^{n' - k' + 1} (a^{k'}/2)^2,$$

where $\pm = (-1)^{(n-1)/2}$.

Fix $b$ and $c$, the above equation can be thought as a quadratic form of $z$ and $a^{k'}/2$. Applying Lemma 3.7, we get that

$$J_{k,n}(N) \ll N^{2+\epsilon}.$$

Case (ii-c) $n$ and $k$ are both odd. There is a one-to-one canonical correspondence between the set $\{f(x) = ax^n + bx^k + c \in \mathbb{Z}[x]\}$ and the set $\{g(x) = cx^n + bx^{n-k} + a\}$. Consider $f(x) = ax^n + bx^k + c \in J_{k,n}(N)$ and its correspondence $g(x) = cx^n + bx^{n-k} + a$. Applying the discriminant formula for trinomials, we get that $D_f = D_g$. Since both $n$ and $k$ are odd, we have $(n - k)$ is even, i.e., $g(x)$ is a polynomial belonging to Case (ii-b). Interchanging $a$ and $c$, $k$ and $(n - k)$ and applying Case (ii-b), the result follows.

### 3.6 The Turán sieve on special trinomials.

#### 3.6.1 The Turán sieve on $x^n + x + c$.

Consider the set $A = \{F(x) = x^n + x + c; |c| \leq N\}$. It is interesting to know that how often a polynomial in this special set is of Galois group contained in $A_n$. Applying the Turán sieve, we obtain that

**Theorem 3.10**

$$\#\{F(x) = x^n + x + c, |c| \leq N \text{ and } \text{Gal}(F) \subseteq A_n\} \ll N^{2/3}(\log N)^2.$$
Remark. In fact, in the case when \( n \geq 5 \), the number of the above set is finite: for a polynomial \( F(x) = x^n + x + c \in \mathbb{Z}[x] \), the discriminant of \( F \) is

\[
D_F = (-1)^{\frac{1}{2}(n-1)} (n^n c^{(n-1)} + (-1)^{(n-1)} (n - 1)^{(n-1)}) .
\]

Consider \( D_F \) as a \( (n - 1) \)-degree polynomial in \( c \), say \( D_F(c) \). Then,

\[
\text{Gal}(F) \subseteq A_n \iff D_F(c) \text{ is a square of some integer, say } y .
\]

\[\iff (c, y) \text{ is a rational point on the curve } y^2 = D_F(c) .\]

When \( n \geq 5 \), the genus of the curve \( y^2 = D_F(c) \) is \( \geq 2 \) [13]. By Faltings’ theorem, one obtain that the number of such \( c \) is finite.

Proof: We recall that the discriminant for \( F(x) = x^n + x + c \in \mathbb{Z}[x] \) is

\[
D_F = (-1)^{\frac{1}{2}(n-1)} (n^n c^{(n-1)} + (-1)^{(n-1)} (n - 1)^{(n-1)}) .
\]

Let \( S = \{ c \in \mathbb{Z} : |c| \leq N \} \). For each \( c \in S \), we assign that

\[
g(c) = (-1)^{\frac{1}{2}(n-1)} (n^n c^{(n-1)} + (-1)^{(n-1)} (n - 1)^{(n-1)}) .
\]

Let \( I = \{ p : p \text{ is prime and } p \leq t \} \). For each \( p \in I \), let \( \Omega(p) \) be the condition that \( g(c) \) is not a square mod \( p \). Hence,

\[S_p = \{ c \in S : g(c) \text{ is not a square mod } p \} .\]

and

\[
\pi_c(I) = \# \{ p \in I : g(c) \text{ is not a square mod } p \} .
\]

We need to apply a nontrivial theorem given by Deligne about smooth curves [8]: if \( C \) is a smooth curve which is of genus \( g \), then,

\[
\#C(\mathbb{F}_p) \leq p + 1 + (2g + 1) \sqrt{p} ,
\]
where $C(\mathbb{F}_p)$ is the set of $\mathbb{F}_p$-rational points. We also know that \cite{13}: Let $C_0$ be an affine curve,

$$C_0 : y^2 = a_0 x^d + a_1 x^{d-1} + \cdots + a_d,$$

where $\text{disc}(f) \neq 0$. There exists a smooth hyperelliptic curve $C \subseteq \mathbb{P}^{g+2}$, $g = \lfloor \frac{d-1}{2} \rfloor$, such that

$$C \cap \{X_0 \neq 0\} = C_0.$$

In fact,

$$\text{genus}(C) = \lfloor \frac{d-1}{2} \rfloor.$$

Applying the above facts, we have that

$$\sum_{x (\mod p)} \left( 1 + \left( \frac{g(x)}{p} \right) \right) = \#C(\mathbb{F}_p) \leq p + 1 + n\sqrt{p} = p + O(\sqrt{p}).$$

In fact, the number

$$\sum_{x (\mod p)} \frac{1}{2} \left( 1 + \left( \frac{g(x)}{p} \right) \right)$$

is equal to

$$\#\{x (\mod p) : g(x) \text{ is a square (mod p)}\}.$$

Hence,

$$\#\{x (\mod p) : g(x) \text{ is not a square (mod p)}\} = \frac{1}{2} p + O(\sqrt{p}).$$
We denote the above number to be $\omega(p)$.

So, we have that

$$|S_p| = \omega(p) \left( \frac{(2N + 1)}{p} + O(1) \right) = \frac{\omega(p)}{p} (2N + 1) + O(\omega(p)),$$

i.e.,

$$\frac{|S_p|}{|S|} = \frac{\omega(p)}{p} + O\left(\frac{\omega(p)}{N}\right).$$

We choose $\delta(p) = \frac{\omega(p)}{p}$ and $r_p = O\left(\frac{\omega(p)}{N}\right)$. For different $p, q \in I$,

$$|S_p \cap S_q| = \omega(p)\omega(q) \left( \frac{2N + 1}{pq} + O(1) \right) = \frac{\omega(p)\omega(q)}{pq} (2N + 1) + O(\omega(p)\omega(q)),$$

which implies that

$$\frac{|S_p \cap S_q|}{|S|} = \frac{\omega(p)\omega(q)}{pq} + O\left(\frac{\omega(p)\omega(q)}{N}\right).$$

Hence, $S_p$ and $S_q$ are quasi-independent. Also, we have that

$$\nu = \sum_{p \in P} \frac{\omega(p)}{p} \sim \frac{1}{2} \frac{t}{\log t}.$$ 

Applying Corollary 1.2, we get that

$$\# \{ F(x) = x^n + x + c \in \mathbb{Z}[x], |c| \leq N, \text{Gal}(F) \subseteq A_n \} = \# \{ c \in S : g(c) \text{ is a square} \} \leq \# \{ c \in S : \pi_c(P) = 0 \} \leq \frac{N(\log t)^2}{t} (1 + \frac{t^3}{N})$$

Now, choose $t = N^{1/3}$, we get that

$$\# \{ F(x) = x^n + x + c \in \mathbb{Z}[x] : |c| \leq N, \text{Gal}(F) \subseteq A_n \} \ll N^{2/3}(\log N)^2.$$
3.6.2 The Turán sieve on $ax^n + bx^k + c$ for $4|n, 2|k$.

We have seen in Section 3.5.2 that

$$\#\{f(x) = ax^n + bx^k + c \in \mathbb{Z}[x] : H(f) \leq N \text{ and } \operatorname{Gal}(f) \subseteq A_n\} \ll N^{2+\varepsilon}.$$ 

In the special case when $4|n, 2|k$, we can apply the Turán sieve to get an sharper upper bound.

**Lemma 3.11** For a fixed odd prime $p$, consider the set $A = \{(a, c) : (a, c) \in (\mathbb{Z}/p\mathbb{Z})^2\}$. There are $\frac{p^2 + 2p - 1}{2}$ elements of $A$ such that $ac$ is a square (mod $p$).

**Proof:** There are four cases for $(a, c) \in (\mathbb{Z}/p\mathbb{Z})^2$ to satisfy the condition that $ac$ is a square.

Case(i) $a = 0$. Since $0 \cdot c = 0$ is a square (mod $p$), $c$ can be any element of $\mathbb{Z}/p\mathbb{Z}$. In this case, we have $p$ many choices.

Case(ii) $a \neq 0$ and $c = 0$. We can choose $a$ to be any non-zero element of $\mathbb{Z}/p\mathbb{Z}$ and there are $(p - 1)$ many such choices.

Case(iii) if both $a$ and $c$ are non-zero and both are squares of some elements (mod $p$), $ac$ is a square (mod $p$). The number of such choices is $(\frac{p-1}{2})^2$.

Case(iv) if both $a$ and $c$ are non-zero and are not squares of some element (mod $p$), then $ac$ is a square (mod $p$). In this case, we have $(\frac{p-1}{2})^2$ many choices.

The total number of choices in above cases is $\frac{p^2 + 2p - 1}{2}$.

**Theorem 3.12** Let $n, k \in \mathbb{N}$, $4|n$ and $2|k$. Then,

$$\#\{f(x) = ax^n + bx^k + c \in \mathbb{Z}[x], \max\{|a|, |b|, |c|\} \leq N \text{ and } \operatorname{Gal}(f) \subseteq A_n\} \ll N^2(\log N)^2.$$ 

**Proof:** Given a trinomials $f(x) = ax^n + bx^k + c$, the discriminant of $f$, $D_f$, is

$$D_f = a^n c^{k-1} E^d,$$

47
where \( d = \gcd(n, k) \) and \( E \in \mathbb{Z}[a, b, c] \). If \( \text{Gal}(f) \subseteq A_n \), \( D_f \) is the square of an integer. Since \( d \) is even, \( ac \) is a square of some element of \( \mathbb{Z} \). Now, apply the Turán sieve.

Let \( S = \{ s = (a, b, c) \in \mathbb{Z}^3 : \max\{|a|, |b|, |c|\} \leq N \} \) and \( I = \{ p : p \text{ is a prime and } 3 \leq p \leq z \} \). For each \( p \in I \), we define \( \Omega(p) \) to be the condition that \( ac \) is not a square \( \pmod{p} \). We have that

\[
S_p = \{ s = (a, b, c) \in S : ac \text{ is not a square } \pmod{p} \}.
\]

and

\[
\pi_s(I) = \# \{ p \in I : ac \text{ is not a square } \pmod{p} \}.
\]

From Lemma 3.11, there are \( (p^2 - \frac{p^2 + 2p - 1}{2}) = \frac{p^2 - 2p + 1}{2} \) many pairs \( (a, c) \in (\mathbb{Z}/p\mathbb{Z})^2 \) such that \( ac \) is not a square. Let \( \omega(p) \) be this number. We have that

\[
|S_p| = \omega(p) \left( \frac{2N + 1}{p} \right)^2 (2N + 1) + O(1)
\]

and

\[
\frac{|S_p|}{|S|} = \frac{\omega(p)}{p^2} + O\left( \frac{\omega(p)}{N^3} \right).
\]

We set \( \delta_p = \frac{\omega(p)}{p^2} \) and \( r_p = O\left( \frac{\omega(p)}{N^3} \right) \). For different \( p, q \in I \),

\[
\frac{|S_p \cap S_q|}{|S|} = \frac{\omega(p)\omega(q)}{p^2q^2} + O\left( \frac{\omega(p)\omega(q)}{N^3} \right).
\]

We have that

\[
\nu = \sum_{p \in I} \frac{\omega(p)}{p^2} \sim \frac{1}{2} \frac{z}{\log z}.
\]

Applying Corollary 1.2, we get that

\[
\# \{ f(x) = ax^n + bx^k + c \in \mathbb{Z}[x] : H(f) \leq N \text{ and } \text{Gal}(f) \subseteq A_n \}
\]
\[ \leq \# \{ s = (a, b, c) \in S : \pi_s(I) = 0 \} \]
\[ \ll \frac{|S|}{\nu} + \frac{|S|}{\nu^2} \sum_{p, q \leq z} |\tau_{p, q}| + \frac{2|S|}{\nu} \sum_{p \leq z} |\tau_p| \]
\[ \ll \frac{N^3 (\log z)^2}{z} (1 + \frac{z^3}{N^3}) \text{(note: } \omega(p) \leq p^2 \leq z^2). \]

Choosing \( z = N \), we get that

\[ \# \{ f(x) = ax^n + bx^k + c \in \mathbb{Z}[x] : H(f) \leq N \text{ and } \text{Gal}(f) \subseteq A_n \} \ll N^2 (\log N)^2. \]
Chapter 4

Probabilistic Galois Theory in the Function Field Case

4.1 Introduction.

In Chapter 2, we consider the probabilistic Galois theory problem in \( \mathbb{Q} \). We estimate

\[
E_n(N) = \#\{F(x) \in \mathbb{Z}[x] : \deg(F) = n, F \text{ is monic}, H(F) \leq N \text{ and } \text{Gal}(F) \subsetneq S_n\}.
\]

We obtain that

\[
E_n(N) \ll N^{n-1/3}(\log N)^2.
\]

In this chapter, we consider the function field version of the probabilistic Galois theory problem: for a fixed \( n \in \mathbb{N} \), let \( F(x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t) \in \mathbb{F}_q[t, x] \). We denote \( \text{Gal}(F) \) to be the Galois group of the splitting field of \( F \) over \( \mathbb{F}_q(t) \). Since \( F(x) \) is of degree \( n \), \( \text{Gal}(F) \) is a subgroup of \( S_n \). We want to estimate the number of monic polynomials of degree \( n \) whose Galois group is a proper subgroup of \( S_n \).

We define the height of \( F \), \( H(F) \), to be

\[
H(F) = \max\{ \deg(a_1(t)), \deg(a_2(t)), \ldots, \deg(a_n(t)) \}.
\]
Also, we denote that
\[ P_n(N) = \# \{ F(x) = x^n + a_1(t)x^{n-1} + a_2(t)x^{n-2} + \cdots + a_n(t) \in \mathbb{F}_q[t, x], \]
\[ H(F) \leq N \text{ and } \text{Gal}(F) \subseteq S_n \} \]

Applying the Turán sieve, we obtain that
\[ P_n(N) \ll (q^{N+1})^{(n-1)} N. \]

### 4.2 Monic irreducible polynomials in \( F_v[x] \).

Fix a monic irreducible polynomial \( v(t) \in \mathbb{F}_p[t] \). Let \( n_v \) denote the degree of \( v(t) \).

We define \( F_v \) to be \( \mathbb{F}_q[t]/(v(t)) \), a finite field with \( q^{n_v} \) elements. Let \( F_v[x] \) be the ring of polynomials in \( x \) with coefficients in \( F_v \). It is a Euclidean domain, and hence is a unique factorization domain.

Given \( F(x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t) \in \mathbb{F}_q[t, x] \), we denote
\[ F(x)(\text{mod } v(t)) = x^n + u_1(t)x^{n-1} + \cdots + u_n(t), \]
where \( a_i(t) \equiv u_i(t)(\text{mod } v(t)) \) and \( \deg(u_i(t)) < \deg(v(t)) \). Since \( F_v[x] \) is a unique factorization domain, we can factor \( F(x)(\text{mod } v(t)) \) as a product of monic irreducible polynomials.

We have analogues of Theorem 2.5 and Corollary 2.6.

**Theorem 4.1** Let \( N_k \) be the number of monic irreducible polynomials in \( F_v[x] \) which is of degree \( k \), then
\[ N_k = \frac{1}{k} \sum_{d|k} \mu(d)(q^{n_v})^{\frac{k}{d}}. \]

**Corollary 4.2** Fix a monic irreducible polynomial \( v(t) \in \mathbb{F}_q[x] \). For all \( n \in \mathbb{N} \), there exists at least one monic irreducible polynomial in \( F_v[x] \) with degree \( n \).
4.3 Definitions of mod $v(t)$ type and its relation to cycle type

Definition: Let $F(x) \in \mathbb{F}_q[t, x]$ is monic and of degree $n$. For an irreducible polynomial $v(t)$, if the factorization of $F(x) (\text{mod } v(t))$ is a product of $r_1$ linear factors, $r_2$ quadratic factors, $r_3$ cubic factors and etc, we say that $F(x)$ has mod $v(t)$ type $r = (r_1, r_2, r_3, \cdots)$.

Remark. Since $F(x)$ has degree $n$, $\sum_k r_k k = n$.

As in the case of $\mathbb{Q}$, the mod $v(t)$ type and cycle type are closely related.

Theorem 4.3 Fix a monic irreducible polynomial $F(x) \in \mathbb{F}_q[t, x]$ of degree $n$ and a type $r = (r_1, r_2, \cdots)$, $\sum r_k k = n$. The following are equivalent: (see [1], [3] and [12])

1. There exists a irreducible polynomial $v(t)$ such that $F(x) \pmod{v(t)}$ is of type $r$.

2. There exists a permutation $\sigma \in \text{Gal}(F) \subseteq S_n$ whose cycle type is $r$.

4.4 Reducible polynomials in $\mathbb{F}_q[t, x]$.

Before we start the function field version of the probabilistic Galois theory problem, we estimate first the number of reducible polynomials in $\mathbb{F}_q[t, x]$. More precisely, we find an upper bound for

$$R_n(N) = \# \{ F(x) = x^n + a_1(t)x^{n-1} + a_2(t)x^{n-2} + \cdots + a_n(t) \in \mathbb{F}_q[t, x], \quad H(F) \leq N \text{ and } F \text{ is reducible} \}$$. 
Theorem 4.4

\[ R_n(N) \ll (q^{N+1})(n-1)N. \]

**Proof:** The proof is an application of the Turán sieve.

Let \( S = \{ s = (a_1(t), a_2(t), \ldots, a_n(t)) \in (\mathbb{F}_q[t])^n, \deg(a_i(t)) \leq N \} \). For each \( s \in S \), we define \( F(s) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t) \in \mathbb{F}_q[t] \). Let \( I = \{ v(t) \in \mathbb{F}_q[t] : v(t) \) is monic, irreducible and \( \deg(v) = n_v \leq z \} \). For each \( v(t) \in I \), we define \( \Omega(v) \) to be the condition that \( F(s) \pmod{v(t)} \) is irreducible. Hence,

\[ S_v = \{ s \in S : F(s) \pmod{v(t)} \text{ is irreducible} \} \]

and

\[ \pi_s(I) = \# \{ v(t) \in I : F(s) \pmod{v(t)} \text{ is irreducible} \}. \]

Let \( \omega(v) \) denote the number of monic irreducible polynomials of degree \( n \) in \( F_v[x] \). We observe that for a fixed monic polynomial \( f(x) \) in \( F_v[x] \), there are \( q^{(N-n_v+1)n} \) many \( s \in S \) such that \( F(s) \equiv f(x) \pmod{v(t)} \). Hence, we have that

\[ |S_v| = q^{(N-n_v+1)n}\omega(v) \]

and

\[ \frac{|S_v|}{|S|} = \frac{\omega(v)}{q^n}. \]

For all \( v(t) \in I \), we set \( \delta_v = \frac{\omega(v)}{q^n} \) and \( \tau_v \) is 0. Moreover, for different \( v(t), w(t) \in I \), \( S_v \) and \( S_w \) are quasi-independent with \( \tau_{v,w} = 0 \). By Theorem 4.1, \( \omega(v) \sim \frac{q^{n_v}n}{n} \), hence, we have that

\[ \nu = \sum_{v \in I} \frac{1}{n} \sim \frac{1}{n} \frac{q^z}{nz}. \]

53
Applying Corollary 1.2, we get

\[ R_n(N) = \# \{ F(x) \in \mathbb{F}_q[t, x] : \deg(F) = n, F : \text{monic}, H(F) \leq N, \text{Gal}(F) \subsetneq S_n \text{ and } F(x) \text{ is reducible} \} \]

\[ = \# \{ s \in S, \pi_s(I) = 0 \} \]

\[ \leq \frac{|S|}{\nu} \quad (\text{note: all } r_{pq} \text{ and } r_p \text{ are 0}) \]

\[ \ll \frac{q^{(N+1)n}N}{q^N} \]

\[ = q^{(N+1)n-N}N. \]

Choosing \( z = N \), the theorem follows.

4.5 The Turán sieve on \( P_n(N) \).

In this section, we prove that

\[ P_n(N) = \# \{ F(x) = x^n + a_1(t)x^{n-1} + a_2(t)x^{n-2} + \cdots + a_n(t) \in \mathbb{F}_q[t, x], \]

\[ H(F) \leq N \text{ and } \text{Gal}(F) \subsetneq S_n \} \]

\[ \ll (q^{N+1})^{n-1}N. \]

Remark. We notice the fact that not all polynomials in \( \mathbb{F}_q[t, x] \) are separable. However, the number of such polynomials is negligible in the following sense: give \( F(x) \in \mathbb{F}_q[t, x] \) of degree \( n \). By Theorem 4.4, to prove the above statement, without loss of generality, we can assume that \( F(x) \) is irreducible. Moreover, for an irreducible polynomial \( F(x) \in \mathbb{F}_q[t, x] \), \( F(x) \) is inseparable if and only if \( F(x) = G(x^p) \) for some polynomial \( G \). Hence, if \( p \nmid n \), \( F(x) \) is always separable. Otherwise, the number of inseparable polynomials is at most \( (q^{N+1})^{n-1} \), which is negligible in our cases. Hence, without loss of generality, we can assume all polynomials \( F(x) \) in the correspondence.
set of $P_n(N)$ are separable, hence $\text{Gal}(F)$ always exist.

By the same argument in Section 2.6.1, to obtain an upper bound for

$$P_n(N) = \#\{F(x) \in \mathbb{F}_q[t, x] : \deg(F) = n, F \text{ is monic}, H(F) \leq N \text{ and } \text{Gal}(F) \subseteq S_n\},$$

it suffices to get an upper bound for

$$P_{r,n}(N) = \#\{F(x) \in E_n(N) : F \text{ does not have mod } v(t) \text{ type } r$$

for all irreducible polynomials $v(t) \in \mathbb{F}_q[t]$.}

We have analogues of Lemma 2.11 and Lemma 2.12.

**Lemma 4.5** Fix a type $r = (r_1, r_2, \cdots)$ with $\sum \beta_k = n$. There are $(\delta(r)(q^{n_0})^n + O((q^{n_0})^{n-1})$ many monic polynomials in $F_q[x]$ with degree $n$ and of type $r$, where

$$\delta(r) = \prod_{k} \frac{1}{r_k!k^{r_k}}.$$ We denote the number of such polynomials by $\omega(v)$.

**Lemma 4.6** Fix a type $r = (r_1, r_2, \cdots)$. There are

$$(q^{N-n_0+1})^n \omega(v)$$

many monic polynomials in $\mathbb{F}_q[t, x]$ with height $\leq N$, which have mod $v(t)$ type equal to $r$.

**Theorem 4.7** Fix a type $r$, then

$$P_{r,n}(N) \ll q^{(N+1)n-N} N.$$ 

**Proof:** The proof is an application of the Turán sieve.

Let $S = \{s = (a_1(t), a_2(t), \cdots, a_n(t)) \in (\mathbb{F}_q[t])^n, \deg(a_i) \leq N\}$. For each $s \in S$, we define $F(s) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t) \in \mathbb{F}_q[t, x]$. Also, we choose $I = \{v(t) \in \cdots$
\( E_q[t] : v(t) \) is monic, irreducible and \( \text{deg}(v) = n_v \leq z \). For each \( v(t) \in I \), we define \( \Omega(v) \) to be the condition that \( F(s) \pmod{v(t)} \) is of type \( r \). Hence,

\[
S_v = \{ s \in S : F(s) \pmod{v(t)} \text{ is of type } r \}
\]

and

\[
\pi_s(I) = \# \{ v(t) \in I : F(s) \pmod{v(t)} \text{ is of type } r \}.
\]

From Lemma 4.6,

\[
|S_v| = q^{(N-n_v+1)n} \omega(v).
\]

Since

\[
|S| = q^{(N+1)n},
\]

we have

\[
\frac{|S_v|}{|S|} = \frac{\omega(v)}{q^{n_v n}}.
\]

We set \( \delta_v = \frac{\omega(v)}{q^{n_v n}} \) and \( \tau_v \) is 0. For different \( v(t) \), \( w(t) \), in \( I \),

\[
\frac{|S_v \cap S_w|}{|S|} = \frac{\omega(v)\omega(w)}{q^{n_v n}q^{n_w n}},
\]

i.e., \( S_p \) and \( S_q \) are quasi-independent with \( \tau_{v,w} = 0 \). We also have that

\[
\nu = \sum_{v \in \mathcal{P}} \frac{\omega(v)}{q^{n_v n}} \sim \sum_{v \in \mathcal{P}} \delta(r) \sim \delta(r) \frac{q^z}{z}.
\]
Applying Corollary 1.2, we get that

\[ P_{r,n}(N) = \#\{F(x) \in \mathbb{F}_q[t, x]: \deg(F) = n, F: \text{monic}, H(F) \leq N, \text{Gal}(F) \nsubseteq S_n \text{ and } F(x) \pmod{v(t)} \text{ is not of type } r \text{ for all irreducible polynomials } v(t) \in \mathbb{F}_q[t]\} \]

\[ = \#\{s \in S, \pi_s(P) = 0\} \]

\[ \leq \frac{|S|}{\nu} \quad \text{(note: all } \tau_{pq} \text{ and } r_p \text{ are 0)} \]

\[ \ll \frac{q^{(N+1)n}N}{q^N} \]

\[ = q^{(N+1)n-N}N. \]

**Conclusion.** For different types \( r \),

\[ P_{r,n}(N) \ll (q^{(N+1)})^{n-1} N \]

implies that

\[ P_n(N) \ll (q^{(N+1)})^{n-1} N. \]

In other words, the number of polynomials \( x^n + a_1(t)x^{n-1} + a_2(t)x^{n-2} \cdots + a_n(t) \in \mathbb{F}_q[t, x] \) with height \( \leq N \) and having Galois groups to be proper subgroups of \( S_n \) is \( \ll (q^{(N+1)})^{n-1} N. \) Since there are \( q^{(N+1)n} \) many monic polynomials in \( \mathbb{F}_q[t, x] \) with height bounded by \( N \), we conclude that "almost all" of monic polynomials in \( \mathbb{F}_q[t, x] \) of degree \( n \) have Galois group equal to \( S_n. \)
Chapter 5

Further Applications of the Turán Sieve

5.1 Introduction.

In the previous four chapters, we have introduced the Turán sieve and applied it to solve the probabilistic Galois theory problems in the cases of \( \mathbb{Q} \) and the function field. From the similarities of these two cases, it seems very likely that we can give a more generalized version of the probabilistic Galois theory problem. Unfortunately, due to the limitation of time, we are not able to proceed on this problem further in the thesis. This chapter is meant for stating these further developments and giving a brief discussion on each one of them.
5.2 Probabilistic Galois theory in $\mathbb{F}_q(t)$.

In Chapter 2 and Chapter 4 we considered the following two quantities respectively:

$$E_n(N) = \# \{ F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x], \quad H(F) \leq N \text{ and } \text{Gal}(F) \subsetneq S_n \}$$

and

$$P_n(N) = \# \{ F(x) = x^n + a_1(x) x^{n-1} + a_2(x) x^{n-2} + \cdots + a_n(x) \in \mathbb{F}_q[t, x], \quad H(F) \leq N \text{ and } \text{Gal}(F) \subsetneq S_n \}. $$

We proved that

$$E_n(N) \ll N^{n-1/3}(\log N)^2$$

and

$$P_n(N) \ll (q^{n+1})^{n-1}N.$$

Given $F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ with $H(F) \leq N$, if we assume $a_n = 0$, $\text{Gal}(F)$ is a proper subgroup of $S_n$. Since the order of such elements is $N^{n-1}$, we have

$$E_n(N) \gg N^{n-1}.$$  

By the same argument, we can show that

$$P_n(N) \gg (q^{n+1})^{n-1}.$$  

In 1936, van der Waerden [15] conjectured that

$$E_n(N) \ll N^{n-1}.$$  

From the above observation, it is tempting to make the following conjecture.
Conjecture 5.1

\[ P_n(N) \ll (q^{N+1})^{n-1}. \]

Remark. In fact, this would follow from a suitable large sieve inequality in the function field case. We hope to deal with this question in further research.

5.3 Probabilistic Galois theory in the number field.

5.3.1 Probabilistic Galois theory in the quadratic field.

Let \( D \) be a non-zero, square-free integer. We denote by \( K = \mathbb{Q}(\sqrt{D}) \) the quadratic field over \( \mathbb{Q} \) and let \( \mathcal{O}_K \) be its ring of integers. For an element \( a \in \mathcal{O}_K \), there exist \( b, c \in \mathbb{Z} \) such that [9]

\[
a = \begin{cases} 
  b + c\sqrt{D} & \text{if } D \equiv 2, 3 \pmod{4}, \\
  \frac{1}{2}(b + c\sqrt{D}) & \text{if } D \equiv 1 \pmod{4}.
\end{cases}
\]

For each \( a \in \mathcal{O}_K \), we define the height of \( a \), \( h(a) \), to be

\[ h(a) = \max\{|b|, |c|\}. \]

Given a monic polynomial \( F(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathcal{O}_K[x] \), we define the height of \( F \), \( H(F) \), to be

\[ H(F) = \max\{h(a_1), h(a_2), \ldots, h(a_n)\}. \]

Let

\[ G_n(N) = \#\{F(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathcal{O}_K[x], H(F) \leq N \text{ and } \text{Gal}(F) \not\subseteq S_n\}. \]
The probabilistic Galois theory problem in the quadratic field \( K = \mathbb{Q}(\sqrt{D}) \) is to estimate the order of \( G_n(N) \). In fact, following the same arguments in Chapter 2, we can prove that

\[
G_n(N) \ll N^{2n-1/3} (\log N)^2,
\]

which implies that almost all monic polynomials of degree \( n \) in \( \mathcal{O}_K[x] \) are of Galois group \( S_n \).

5.3.2 Probabilistic Galois theory in the number field.

Let \( K \) be a number field and let \( \mathcal{O}_K \) be its ring of integer. If \([K : \mathbb{Q}] = n\), \( \mathcal{O}_K \) is a free abelian group of rank \( n \) [9]. Let \( \{e_1, e_2, \ldots, e_n\} \) be an integral basis of \( \mathcal{O}_K \). Then, for each \( a \in \mathcal{O}_K \), we can write

\[
a = c_1e_1 + c_2e_2 + \cdots + c_ne_n,
\]

where \( c_i \in \mathbb{Z} \) for all \( i \). We define the height of \( a \), \( h(a) \), to be

\[
h(a) = \max\{|c_1|, |c_2|, \cdots, |c_n|\}.
\]

Thus \( h \) depends on the choice of an integral basis.

Given a monic polynomial \( F(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathcal{O}_K[x] \), we define the height of \( F \), \( H(F) \), to be

\[
H(F) = \max\{h(a_1), h(a_2), \cdots, h(a_n)\}.
\]

Let

\[
G_n(N) = \#\{F(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathcal{O}_K[x], H(F) \leq N \text{ and } \text{Gal}(F) \subsetneq S_n\}.
\]

The probabilistic Galois theory problem in the number field \( K \) is to estimate the order of \( G_n(N) \).
Remark. Given $F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathcal{O}_k[x]$ with $H(F) \leq N$, if we assume $a_n = 0$, $\text{Gal}(F)$ is a proper subgroup of $S_n$. Since the order of such elements is $(N^n)^{n-1}$, we have that

$$G_n(N) \gg (N^n)^{n-1}.$$ 

Following the argument of Van der Waerden about $E_n(N)$, we make an analogous conjecture.

Conjecture 5.2

$$G_n(N) \ll (N^n)^{n-1}.$$ 

5.4 Probabilistic Galois theory for Dedekind domains.

The notation of Dedekind domain is an important tool in modern number theory.

Definition: A Dedekind domain is an integral domain $R$ such that

1. $R$ is Noetherian.
2. Every non-zero prime ideal is a maximal ideal.
3. $R$ is integrally closed in its field of fractions $K$,

$$K = \{\alpha/\beta; \alpha, \beta \in R, \beta \neq 0\},$$

which means that: for $\alpha/\beta \in K$, if there exist a monic polynomial $f(x) \in R[x]$ such that $f(\alpha/\beta) = 0$, then $\alpha/\beta \in R$.

Theorem 5.1 Every ideal in a Dedekind domain $R$ is uniquely representable as a product of prime ideals. [9]
So far, we have considered the probabilistic Galois theory problem in $\mathbb{Q}, \mathbb{F}_q(t)$ and the number field $K$. The corresponding rings of integers are $\mathbb{Z}, \mathbb{F}_q[t]$ and $\mathcal{O}_K$ respectively - all of them are Dedekind domains. From this observation, we can generalize probabilistic Galois theory as follows: fix $n \in \mathbb{N}$. Let $R$ be a Dedekind domain and $K$ be its field of fractions. Suppose that there exists a function $\phi$ from $R$ to $\mathbb{N}$. For each $F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$, we define the height of $F$, $H(F)$, to be

$$H(F) = \max\{\phi(a_1), \phi(a_2), \cdots, \phi(a_n)\}.$$

We will assume that the set of elements of a given height is finite. The probabilistic Galois theory problem is to estimate the order of $V_n(N)$, where

$$V_n(N) = \#\{F(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x], H(F) \leq N \text{ and } \text{Gal}(F) \subseteq S_n\}.$$

**Remark.** In the special case when $R = \mathbb{Z}$, one may take the function $\phi$ to be the absolute value function and in the case of the function field, $\phi$ to be the degree function.

Let $C(N)$ be the number of $a \in R$ with the property that $\phi(a) \leq N$. Following the argument of Van der Waerden, we could ask the following question.

**Question.** Estimate $V_n(N)$, can we expect

$$V_n(N) \ll (C(N))^{n-1},$$

for “reasonable” $\phi$? To define “reasonable” is also part of the question.

## 5.5 Probabilistic Galois theory for subgroup of $S_n$.

To conclude this chapter, hence the whole thesis, we would like to give a more generalized version of the probabilistic Galois theory problem.
Let $n \in \mathbb{N}$ and $R$ be a Dedekind domain. Let $\phi$ be a function from $R$ to $\mathbb{N}$. In the previous section, we propose a problem about the order of $V_n(N)$, where

$$V_n(N) = \#\{F(x) = x^n + a_1x^{n-1} + \cdots + a_n \in R[x], \ H(F) \leq N \text{ and } \text{Gal}(F) \subsetneq S_n\}.$$ 

More generally, if we replace $S_n$ be any subgroup $G$ of $S_n$, we can ask that if we can estimate the order of the following set:

$$\{F(x) = x^n + a_1x^{n-1} + \cdots + a_n \in R[x], \ H(F) \leq N \text{ and } \text{Gal}(F) \subseteq G\}.$$ 

To answer such a question, first, we need to get criteria to decide if $\text{Gal}(F)$ is a subgroup of $S_n$. In the case when $G = A_n$, the discriminant of $F$ gives a criterion for $\text{Gal}(F)$ to be contained in $A_n$. (For more details on it, see Chapter 3.) In general, one may associate $G$ the Lagrange resolvent of $F$, denoted $R_G(F)$. It is a monic polynomial of degree $[S_n : G]$ whose coefficients are polynomial functions with coefficients in the prime ring (i.e., $\mathbb{Z}$ if $\text{char } R = 0$ and $\mathbb{F}_p$ if $\text{char } R = p$) of the coefficients of $F$. Furthermore, $R_G(F)$ has a root if and only if $\text{Gal}(F)$ is contained in a conjugate of $G$. It is certainly an interesting question worthy of further research.
Bibliography


