参赛队员姓名：李颖

中学：南京外国语学校

省份：江苏省

国家/地区：中国

指导教师姓名：郭佩华

论文题目：On Finite Subgroups in the General Linear Groups over an algebraic number field

创新性申明

本参赛团队声明所提交的论文是在指导老师指导下进行的研究工作和取得的研究成果。尽本团队所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果。若有不实之处，本人愿意承担一切相关责任。

参赛队员：李颖　　指导老师：[illegible]

2020年09月09日

On Finite Subgroups in the General Linear Groups over an Algebraic Number Field

Li Ying

Abstract

As is well-known, there are only finitely many isomorphic classes of finite subgroups in a given general linear group over the field of rational numbers. This result can be generalized to any algebraic number field. While the case of field of rational numbers is relatively well-studied, we still do not know much for general algebraic number field cases. In this article, we discuss the finiteness of isomorphic classes of finite subgroups of general linear groups over an algebraic number field. We give a method to calculate a bound for the orders of the finite subgroups and to classify finite cyclic subgroups.

Keywords: General linear group, Algebraic number field, Cyclic group, Order

Contents

1 Introduction

For a given natural number n, it is well-known that, up to isomorphism, there are finitely many finite subgroups of $GL_n(\mathbb{Q})$. It is a result dating back to the era of Minkowski [3]. Decades later, Schur generalizes this result by replacing $\mathbb{Q}$ with any algebraic number field [5]. He used the character theory of finite groups to obtain this result.

Many works have been done on the classification of finite subgroups of $GL_n(\mathbb{Q})$. We have even thorough classification results when n is relatively small. See for example [1, 2]. However, for other algebraic number fields, we still do not have too many classification results.

The ultimate goal of our project is to determine, up to isomorphism, all finite subgroups of $\mathrm{GL}_n(K)$ for a given $n \in \mathbb{N}$ and for an algebraic number field K. In practice, we have obtained the following partial results that we shall present in the following parts of this article:

- In Section 2, we give a general method to classify finite cyclic subgroups of $GL_n(K)$.
- In Section 3, we propose another proof of Schur's result [5] in the case where the ring of integers is a principal ideal domain, without using character theory of finite groups.
- In Section 4, we give a general method to calculate an upper bound of finite subgroups of $GL_n(K)$.

The general results proposed in Section 2 and Section 4 can be applied directly to concrete examples. For example:

1. The order of any finite subgroup of $GL_2(\mathbb{Q}[\sqrt{-1}])$ divides 96 and finite cyclic subgroups of $GL_2(\mathbb{Q}[\sqrt{-1}])$ are exactly $C_1, C_2, C_3, C_4, C_6, C_8, C_{12}$, up to isomorphism.
2. The order of any finite subgroup of $GL_2(\mathbb{Q}[\sqrt{-2}])$ divides 48 and finite cyclic subgroups of $GL_2(\mathbb{Q}[\sqrt{-2}])$ are exactly $C_1, C_2, C_3, C_4, C_6, C_8$, up to isomorphism.
3. The order of any finite subgroup of $GL_3(\mathbb{Q}[\sqrt{-1}])$ divides 384 and finite cyclic subgroups of $GL_3(\mathbb{Q}[\sqrt{-1}])$ are exactly $C_1, C_2, C_3, C_4, C_6, C_8, C_{12}$, up to isomorphism.
4. .....

The above results are calculated explicitly in Section 2.3 and 4.3 .

The above results can help us classify finite subgroups in $GL_n(K)$ even if we do not know the thorough classificaition. For example, the symmetric group S_5 is *not* in $GL_2(\mathbb{Q}[\sqrt{-1}])$, since $|S_5|$ contains 5 as a factor whereas we prove that the order of any finite subgroup of $GL_2(\mathbb{Q}[\sqrt{-1}])$ divides 96. For similar reasons, we know that S_5 is *not* in $GL_2(\mathbb{Q}[\sqrt{-2}])$ or in $GL_3(\mathbb{Q}[\sqrt{-1}])$, either.

2 Finite Cyclic Subgroups of $GL_n(K)$

In this section, we are going to give a method to classify finite cyclic subgroups of $GL_n(K)$. By definition, classifying cyclic subgroups is equivalent to finding all possible orders of elements in $GL_n(K)$. We find that this problem is closely related to the irreducibility of cyclotomic polynomials in different fields. So we start with a brief introduction to cyclotomic polynomials.

2.1 Cyclotomic Polynomials

Let n be a natural number and $\mathbb{U}_n$ be the set of n-th primitive roots of unity in $\mathbb{C}$. In other words, $\mathbb{U}_n$ contains the complex numbers of the form $e^{\frac{2\pi ik}{n}}$ with k coprime with n. One may define a polynomial with complex coefficients in the following form:

$$\Phi_n(X) := \prod_{\zeta \in \mathbb{U}_n} (X - \zeta).$$

We call Φ_n the n-th cyclotomic polynomial. This polynomial is clearly of degree $\phi(n)$, where $\phi(n)$ denotes the Euler totient function. We list some properties of cyclotomic polynomials that we shall utilize afterwards.

Proposition 1 *Let $\Phi_n(X)$ denote the n-th cyclotomic polynomial.*

1. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
2. *For each n, Φ_n is a polynomial with* integer *coefficients.*
3. *Φ_n is irreducible in $\mathbb{Q}[X]$.*

Proof

1. Since $X^n - 1$ and $\prod_{d|n} \Phi_d(X)$ are both monic polynomials, we can prove the equation by showing that they have the same roots. The roots of $X^n - 1$ can be written as $e^{\frac{2\pi ik}{n}}$ where $k = 0, 1, \ldots, n-1$. Let d be the greatest common divisor of k and n, thus $\frac{k}{d}$ is coprime with $\frac{n}{d}$, i.e., $e^{\frac{2\pi ik}{n}}$ is a root of $\Phi_{\frac{n}{d}}(X)$. Therefore, $X^n - 1 = \prod_0^{n-1}(X - e^{\frac{2\pi ik}{n}}) = \prod_{d|n} \Phi_d(X)$.
2. First, we are going to prove that Φ_p is a polynomial with integer coefficients when p is a prime number. Since $X^p - 1 = \Phi_1(X)\Phi_p(X) = (X-1)\Phi_p(X)$, we can easily know that $\Phi_p(X) = \frac{X^p-1}{X-1} = 1 + X + X^2 + \cdots + X^{p-1}$, which shows that $\Phi_p(X)$ is a polynomial with integer coefficients. Here is a fact we are going to use later : when $f, g, h \in \mathbb{C}[X]$ are monic polynomials and $f = gh$, if $f, g \in \mathbb{Z}[X]$, then h is also a polynomial with integer coefficients. Hence, we assume by induction that for any $m < n$, $\Phi_m(X)$ is in $\mathbb{Z}[X]$. Since $X^n - 1 = \Phi_n(X) \prod_{d|n, d<n} \Phi_d(X)$, $\Phi_n(X)$ is a polynomial with integer coefficients because of the fact mentioned above.
3. This result is well-known and a standard proof can be found in, for example, the Theorem 4.2.6 of [7, p.94]

□

Corollary 2.1.1 *Let $\zeta_n \in \mathbb{U}_n$ be an n-th primitive root of unity. Then, $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n)$.*

Proof Since ζ_n is a root of Φ_n, which is irreducible in $\mathbb{Q}[X]$, Φ_n is the minimal polynomial of ζ_n over $\mathbb{Q}$. Then, we can know that $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \deg \Phi_n = \phi(n)$ by the basic knowledge of the field extension theory. □

2.2 Constraints for the order of an element

In this part, we shall give a constraint for the order of an element of $GL_n(K)$.

To begin with, let ζ_n be an n-th primitive root of unity and let $\Phi_n(X)$ be the n-th cyclotomic polynomial. We know that $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$. $\Phi_n(X)$ may not be irreducible in K. It is natural to consider the irreducible decomposition of $\Phi_n(X)$ in $K[X]$. In fact, we have the following proposition:

Proposition 2 *Any irreducible factor of $\Phi_n(X)$ in $K[X]$ is of the same degree, namely, $[K[\zeta_n] : K]$.*

Proof Let $\Phi_n(X) = \Phi_{n1}(X) \dots \Phi_{nr}(X)$ be the irreducible decomposition. We may assume ζ_n^k is a root of $\Phi_{n1}(X)$, then $\Phi_{n1}(X)$ is the minimal polynomial of ζ_n^k over K. By the basic knowledge of the field extension theory, we can know that $[K[\zeta_n^k] : K] = \deg \Phi_{n1}$. It is obvious that $K[\zeta_n^k] \subset K[\zeta_n]$. Moreover, since k is coprime with n, let $a, b \in \mathbb{Z}$ make $ak + bn = 1$, and then $\zeta_n = \zeta_n^{ak+bn} = (\zeta_n^k)^a (\zeta_n^n)^b = (\zeta_n^k)^a \in K[\zeta_n^k]$. As a result of $K[\zeta_n^k] \supset K[\zeta_n]$, we can know that $K[\zeta_n^k] = K[\zeta_n]$. Therefore, $\deg \Phi_{n1}(X) = \dots = \deg \Phi_{nr}(X) = [K[\zeta_n^k] : K] = [K[\zeta_n] : K]$. □

In what follows, we shall denote

$$\phi_K(n) := [K[\zeta_n] : K].$$

Notice that $\phi_{\mathbb{Q}}(n) = \phi(n)$ is nothing but the Euler totient function.

Theorem 2.2.1 *Let K be an algebraic number field and n a natural number. Let $A \in GL_n(K)$ be an element of order d. Then d must be the least common multiple of some integers ℓ, not necessarily distinct, such that the sum of these $\phi_K(\ell)$ is less or equal to n.*

Proof Let μ_A be the minimal polynomial of A whose order is d. Then $\mu_A \mid X^d - 1$ and $\mu_A \nmid X^{d'} - 1$ for $1 \le d' < d$. By the property of cyclotomic polynomials, $X^d - 1 = \prod_{\ell | d} \Phi_\ell(X)$. If we write $\Phi_\ell(X)$ by its irreducible decomposition:

$$\Phi_\ell(X) = \Phi_{\ell 1}(X) \dots \Phi_{\ell r_\ell}(X),$$

thus the irreducible decomposition of $X^d - 1$ over $K[X]$ is

$$X^d - 1 = \prod_{\ell | d} \Phi_{\ell 1}(X) \dots \Phi_{\ell r_\ell}(X).$$

Therefore, $\mu_A \mid X^d - 1$ implies that μ_A is the product of some irreducible factors of $X^d - 1$, which is to say,

$$\mu_A(X) = \prod_{\text{some } \ell | d} \Phi_{\ell 1}(X) \dots \Phi_{\ell s_\ell}(X).$$

where $1 \le s_\ell \le r_\ell$. We claim that the least common multiple of these ℓ must be d. In fact, we assume by contradiction that the least common multiple of these integers ℓ is d' where $1 \le d' < d$, and then $\mu_A \mid X^{d'} - 1$, which contradicts the fact that $\mu_A \nmid X^{d'} - 1$ for any $1 \le d' < d$. By the discussion above, since $\deg \Phi_{\ell_i}(X) = \phi_K(\ell)$ for any $1 \le i \le s_\ell$, we can know that $\deg \mu_A = \sum s_\ell \phi_K(\ell)$ for some $\ell \mid d$ and the least common multiple of these

ℓ is d. On the other hand, by the Hamilton-Cayley theorem, $\mu_A \mid \chi_A$, so we can give that $\deg \mu_A \leq \deg \chi_A = n$, which can give a constraint

$$\sum s_\ell \phi_K(\ell) \leq n$$

for some $\ell \mid d$ and the least common multiple of ℓ is d. □

Corollary 2.2.1 *There are only finitely many possible orders of elements in $GL_n(K)$ for a given n and a given algebraic number field K.*

Proof Let d be the order of an element in $GL_n(K)$. Due to the fact that

$$[K[\zeta_\ell] : \mathbb{Q}] = [K[\zeta_\ell] : \mathbb{Q}[\zeta_\ell]] \cdot [\mathbb{Q}[\zeta_\ell] : \mathbb{Q}] = [K[\zeta_\ell] : K] \cdot [K : \mathbb{Q}],$$

we get this equation:

$$\phi_K(\ell) = [K[\zeta_\ell] : K] = \frac{[K[\zeta_\ell] : \mathbb{Q}[\zeta_\ell]] \cdot \phi(\ell)}{[K : \mathbb{Q}]}.$$

Specially, it means this inequation:

$$\phi_K(\ell) \geq \frac{\phi(\ell)}{[K : \mathbb{Q}]}.$$

Combined with the constraint in the theorem above, this inequation implies that

$$\sum s_\ell \phi(\ell) \leq n[K : \mathbb{Q}]$$

for some $\ell \mid d$ and the least common multiple of ℓ is d. As known, there are only finitely many natural numbers ℓ whose Euler totient function $\phi(\ell) \leq n[K : \mathbb{Q}]$. Therefore, as the least common multiple of some ℓ satisfying $\phi(\ell) \leq n[K : \mathbb{Q}]$, d has only finitely many possible values. □

2.3 Some Examples

In this section, we are going to classify finite cyclic subgroups for $GL_2(\mathbb{Q}[\sqrt{-1}])$, $GL_3(\mathbb{Q}[\sqrt{-1}])$, $GL_2(\mathbb{Q}[\sqrt{-2}])$ and $GL_3(\mathbb{Q}[\sqrt{-2}])$ by using the method mentioned above to show how the machinary works. For this purpose, we stretch a famous result from [7, p. 111: Corollary 4.5.4]:

Theorem 2.3.1 *Let $d > 1$ be a natural number and we define a set*

$$A_d = \left\{ \left(\frac{-1}{p}\right) p : \text{ for odd prime numbers } p \text{ dividing } d \right\} \cup \{-1 : \text{ if } 4|d\} \cup \{2 : \text{ if } 8|d\}.$$

Let m be a square-free integer. Let ζ_d denote a d-th primitive root of unity. Then $\sqrt{m} \in \mathbb{Q}[\zeta_d]$ if and only if m is a nontrivial product of distinct elements in A_d.

Example Let $K = \mathbb{Q}[\sqrt{-1}]$ and $n = 2$. Let d be the order of an element in $GL_2(\mathbb{Q}[\sqrt{-1}])$. Considering the equation we have shown above:

$$\phi_K(\ell) = \frac{[K[\zeta_\ell] : \mathbb{Q}[\zeta_\ell]] \cdot \phi(\ell)}{[K : \mathbb{Q}]},$$

since $[K : \mathbb{Q}] = 2$ in this occasion, we can show by Theorem 2.3.1 that

$$[K[\zeta_\ell] : \mathbb{Q}[\zeta_\ell]] = \begin{cases} 1 & \text{if } \sqrt{-1} \in \mathbb{Q}[\zeta_\ell], i.e., 4 \mid \ell \\ 2 & \text{if } \sqrt{-1} \notin \mathbb{Q}[\zeta_\ell], i.e., 4 \nmid \ell \end{cases}$$

which indicates that, in this case,

$$\phi_K(\ell) = \begin{cases} \phi(\ell) & \text{if } 4 \nmid \ell \\ \frac{1}{2}\phi(\ell) & \text{if } 4 \mid \ell \end{cases}$$

Thus, $\phi_K(\ell) \leq n = 2$ indicates that

$$\begin{cases} \phi(\ell) \leq 2 & \text{if } 4 \nmid \ell \\ \phi(\ell) \leq 4 & \text{if } 4 \mid \ell \end{cases}$$

Then, by calculation, we find that ℓ has seven possible values: $1, 2, 3, 4, 6, 8, 12$. Since d is the least common multiple of some ℓ, with the constraint

$$\sum s_\ell \phi_K(\ell) \leq n,$$

the possible values of d are $1, 2, 3, 4, 6, 8, 12$, which means that in $GL_2(\mathbb{Q}[\sqrt{-1}])$, there are seven kinds of finite cyclic subgroups whose orders are possibly $1, 2, 3, 4, 6, 8$ or 12. Next we show that these orders can indeed be obtained.

In fact, we can exactly find possible elements of different orders to show their existence:

$d = 1$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$d = 2$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$d = 3$	$\begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$
$d = 4$	$\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$
$d = 6$	$\begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}$
$d = 8$	$\begin{pmatrix} 1 & i-1 \\ 1 & -1 \end{pmatrix}$
$d = 12$	$\begin{pmatrix} i & -3i \\ i & -2i \end{pmatrix}$

Using the same method, we can restrain the possible orders of elements of $GL_3(\mathbb{Q}[\sqrt{-1}])$ to be $1, 2, 3, 4, 6, 8, 12$. They are the same with those of $GL_2(\mathbb{Q}[\sqrt{-1}])$. To show the existence, if A is a 2×2 matrix in $GL_2(\mathbb{Q}[\sqrt{-1}])$ with order d, then

$$\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$$

would be a 3×3 matrix of order d in $GL_3(\mathbb{Q}[\sqrt{-1}])$.

Example Let $K = \mathbb{Q}[\sqrt{-2}]$ and d be the order of an element in $GL_2(\mathbb{Q}[\sqrt{-2}])$. According to the Theorem 4.3.1 above, we can get the following equation the same way we do in the preceding example:

$$[K[\zeta_\ell] : \mathbb{Q}[\zeta_\ell]] = \begin{cases} 1 & \text{if } \sqrt{-2} \in \mathbb{Q}[\zeta_\ell], i.e., 8 \mid \ell \\ 2 & \text{if } \sqrt{-2} \notin \mathbb{Q}[\zeta_\ell], i.e., 8 \nmid \ell \end{cases}$$

which indicates that, in this case,

$$\phi_K(\ell) = \begin{cases} \phi(\ell) & \text{if } 8 \nmid \ell \\ \frac{1}{2}\phi(\ell) & \text{if } 8 \mid \ell \end{cases}$$

We now use the result of the preceding section to classify finite cyclic subgroups of $GL_n(\mathbb{Q}[\sqrt{-2}])$ for $n = 2, 3$.

- When $n = 2$, $\phi_K(\ell) \leq 2$ indicates the following inequation:

$$\begin{cases} \phi(\ell) \leq 2 & \text{if } 8 \nmid \ell \\ \phi(\ell) \leq 4 & \text{if } 8 \mid \ell \end{cases}$$

  Then, by calculation,we find that ℓ has six possible values: $1, 2, 3, 4, 6, 8$. Since d is the least common multiple of some ℓ, with the constraint

$$\sum s_\ell \phi_K(\ell) \leq n,$$

  the possible values of d are $1, 2, 3, 4, 6, 8$, which means that in $GL_2(\mathbb{Q}[\sqrt{-2}])$, there are six kinds of finite cyclic subgroups whose orders are possibly $1, 2, 3, 4, 6$ or 8. We list possible matrices whose order is exactly among those possible values we find.

$d = 1$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$d = 2$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$d = 3$	$\begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$
$d = 4$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
$d = 6$	$\begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}$
$d = 8$	$\begin{pmatrix} -\sqrt{-2} & 1 \\ 1 & 0 \end{pmatrix}$

- When $n = 3$, like the occasion when $n = 2$, $\phi_K(\ell) \leq 3$ indicates the following inequation:

$$\begin{cases} \phi(\ell) \leq 3 & \text{if } 8 \nmid \ell \\ \phi(\ell) \leq 6 & \text{if } 8 \mid \ell \end{cases}$$

  Then, by calculation,we find that ℓ has six possible values:$1, 2, 3, 4, 6, 8$. Since d is the least common multiple of some ℓ, with the constraint

$$\sum s_\ell \phi_K(\ell) \leq n,$$

the possible values of d are $1, 2, 3, 4, 6, 8$, which means that in $GL_3(\mathbb{Q}[\sqrt{-2}])$, there are six kinds of finite cyclic subgroups whose orders are possibly $1, 2, 3, 4, 6$ or 8. If A is a 2×2 matrix in $GL_2(\mathbb{Q}[\sqrt{-2}])$ with order d, then

$$\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$$

would be a 3×3 matrix of order d in $GL_3(\mathbb{Q}[\sqrt{-2}])$.

3 Finite Subgroups of $GL_n(K)$

In this section, we are going to prove that there are only finitely many finite subgroups of $GL_n(K)$ for a given natural number $n > 0$ and an algerbraic number field K, whose ring of integers $\mathcal{O}_K$ is a principal ideal domain. First, we will show that any finite subgroup of $GL_n(K)$ is isomorphic to a subgroup of $GL_n(\mathcal{O}_K)$. Then after modulo a well-chosen prime element x in $\mathcal{O}_K$, we find any finite subgroup of $GL_n(\mathcal{O}_K)$ is isomorphic to a subgroup of $GL_n(\mathcal{O}_K/(x))$, while the latter, as a finite group, has only finitely many finite subgroups.

3.1 Free Modules over a Principal Ideal Domain

A general result on free modules over a principal ideal domain is that submodules of a free module of rank n is free and of rank no greater than n. We will give a proof of this result.

We begin by giving the definition of an A-module. It is a generalization over vector spaces over a field. But the properties of A-modules are more complicated.

Definition *Let A be a commutative ring. A module M over A is a set endowed with two operations:*

$$+ : M \times M \to M;$$
$$\cdot : A \times M \to M;$$

satisfying:

- *(+-axioms) $(M, +)$ is an abelian group;*
- *(·-axioms)*
  - $\forall \lambda, \mu \in A, x \in M, \lambda(\mu x) = (\lambda\mu)x$
  - $\forall x \in M, 1 \cdot x = x$
  - $\forall \lambda, \mu \in A, x \in M, (\lambda + \mu)x = \lambda x + \mu x$
  - $\forall \lambda \in A, x, y \in M, \lambda(x + y) = \lambda x + \lambda y$

Definition (Basis) *Let M be an A-module, $B \subset M$ is called a basis of M, if:*

- *$\forall x \in M$, $\exists x_1, \ldots, x_n \in B$,$\lambda_1, \ldots, \lambda_n \in A$, such that $x = \sum_1^n \lambda_i x_i$*

- *If $x_1, \ldots, x_n \in B$ are distinct and for $\lambda_1, \ldots, \lambda_n \in A$,*

$$\sum_{i=1}^{k} \lambda_i x_i = 0 \Longrightarrow \lambda_i = 0, \forall i.$$

The definition of basis of an A-module is similar to that of a vector space. The difference is that an A-module does not necessarily have a basis. If an A-module M admits a basis, then M is called *free*. A good example of a free A-module is:

$$A^n = \{(x_1, \ldots, x_n) : x \in A\}$$

where $\forall \lambda \in A$, $(x_1, \ldots, x_n) \in A^n$, $\lambda(x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n)$. Apparently, A^n is an A-module. There exits a basis of A^n, called the *canonical basis* of A^n, namely, $B := \{e_1, \ldots, e_n\}$, where e_i is an element in A^n whose i-th component is 1 and whose other components are 0. Therefore, we can draw the conclusion that A^n is a free A-module.

Definition *Let M, N be A-modules. $\phi : M \to N$ is called a homomorphism of A-modules (or A-linear map), if:*

- $\forall x \in M$, $\lambda \in A$, $\phi(\lambda x) = \lambda \phi(x)$
- $\forall x, y \in M$, $\phi(x + y) = \phi(x) + \phi(y)$

Furthermore, ϕ is an isomorphism ($\cong$) if it is bijective and homomorphic.

Let M be a free A-module with a basis B. Assume that the $\#B = n$, then clearly $M \cong A^n$ as A-modules.

It is well-known in linear algebra that any basis of a given vector space has the same cardinal. The same result holds for a free A-module. In fact, we are going to prove in the following paragraphs that $A^m \cong A^n$ if and only if $m = n$. Given this result, we define the *rank* of a free A-module as the cardinal of any of its bases.

Lemma 3.1.1 *Let $\phi : A^m \to A^n$ be a homomorphism of A-modules, and $\mathfrak{a}$ be an ideal of A. If $x = (x_1, \ldots, x_m)$ is in $\mathfrak{a}^m$, then $\phi(x) \in \mathfrak{a}^n$.*

Proof Let $\phi(x) = (\phi_1(x), \ldots, \phi_n(x))$. For any j, notice that $\phi_j(x) = \phi_j(\sum x_i e_i) = \sum x_i \phi_j(e_i) \in \mathfrak{a}$ since $x_i \in \mathfrak{a}, \forall i$. We conclude that $\phi(x) \in \mathfrak{a}^n$. □

Theorem 3.1.1 *Let A be a commutative ring. Then $A^m \cong A^n$ as A-modules if and only if $m = n$.*

Proof If $A^m \cong A^n$, there exists a map $\phi : A^m \to A^n$ which is an isomorphism of A-modules. Since A is a commutative ring, let $\mathfrak{m}$ be a maximal ideal of A. Then, we can define another map:

$$\psi : (A/\mathfrak{m})^m \to (A/\mathfrak{m})^n$$

as $(\bar{x}_1, \ldots, \bar{x}_m) \mapsto (\overline{\phi_1(x_1, \ldots, x_m)}, \ldots, \overline{\phi_n(x_1, \ldots, x_m)})$. We need to check:

- Well-definedness: Let $(\bar{x}_1, \ldots, \bar{x}_m) = (\bar{y}_1, \ldots, \bar{y}_m)$, then $x_i - y_i \in \mathfrak{m}, \forall i$. Therefore, by the lemma above, $\phi_j(x_i) - \phi_j(y_i) = \phi_j(x_i - y_i) \in \mathfrak{m}$, i.e., $\overline{\phi_j(x_i)} = \overline{\phi_j(y_i)}, \forall i, j$, which means that

$$(\overline{\phi_1(x_1, \ldots, x_m)}, \ldots, \overline{\phi_n(x_1, \ldots, x_m)}) = (\overline{\phi_1(y_1, \ldots, y_m)}, \ldots, \overline{\phi_n(y_1, \ldots, y_m)}).$$

- ψ is an $A/\mathfrak{m}$-linear map. It is direct from the fact that ϕ is an A-linear map.
- ψ is injective. In fact, let $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_m) \in \ker \psi$, then $\phi_j(x_1, \ldots, x_m) \in \mathfrak{m}, \forall j$. If ξ is the inverse map of ϕ, then $x_i = \xi_i(\phi(x)) \in \mathfrak{m}$ by the above lemma. Therefore, $\bar{x}_i \in \mathfrak{m}, \forall i$, i.e., $\bar{x} = 0$ in $(A/\mathfrak{m})^m$.
- ψ is surjective. This follows directly from the fact that ϕ is surjective.

Therefore, we construct an isomorphism of $A/\mathfrak{m}$-vectors spaces: $\psi : (A/\mathfrak{m})^m \cong (A/\mathfrak{m})^n$. Since any basis of a vector space has the same number of elements, we conclude that $m = n$. □
Then, we can deduce that if M is an $A-$module, B_1,B_2 be two bases such that $\#B_1 < +\infty$,$\#B_2 < +\infty$, then $\#B_1 = \#B_2$.

Definition *Let M be an $A-$module, $N \subset M$ is called a sub-module if N itself is an A-module.*

Specially, when $M = A$ is an A-module, the sub-module of M is the ideal of A.

Theorem 3.1.2 *Let $M \subset A^n$ is a sub-module, then M is a free $A-$module with rank $r \leq n$.*

Proof We argue by induction on n.

- $n = 1$.
  - If $M \cong \{0\}$, M is a free $A-$module with rank $r = 0$ where its basis is empty.
  - If $M \ncong \{0\}$, M is an ideal of A. Since A is a principal ideal domain, M:= $(m) = mA$ where $m \neq 0$. We can construct a map $\phi : A \to mA$ as $x \to mx$. Apparently, ϕ is a homomorphism. Let $x \in ker\phi$, $x = 0$ since $mx = 0$ and $m \neq 0$. Obviously, ϕ is surjective, then $M \cong A$ as $A-$modules and the rank of M is 1.
- Assume this theorem is true for all $k \leq n-1$. We shall prove that the theorem holds for n. Let M be a submodule of A^n. Let $A = \{(x, 0, \ldots, 0) : x \in A\} \subset A^n$ and $\Gamma := M \cap A$. By induction assumption, Γ is free of rank ≤ 1. We can construct a map $\psi : M \to A^{n-1}$ as $(x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n)$. Apparently, ψ is an homomorphism as A-modules. Since $\ker \psi = \{(x_1, \ldots, x_n) \in M : x_2, \ldots, x_n = 0\} = M \cap N$ where $N := \{(x, 0, \ldots, 0) : x \in A\} \cong A$, we can know that $M/M \cap N = M/\ker \psi \cong \mathrm{Im}\psi \subset A^{n-1}$. By induction assumption, $M/M \cap A$ is free of rank $\leq n-1$. Then, we need to prove that M is a free module. Let $\{\bar{e}_1, \ldots, \bar{e}_k\}$ be a basis of $M/M \cap A$ and $\{f_1, \ldots, f_p\}$ be a basis of $M \cap A$. May take $e_1 \in \bar{e}_1, \ldots, e_k \in \bar{e}_k$. We would like to show that $\{e_1, \ldots, e_k, f_1, \ldots, f_p\}$ forms a basis of M.
  - $\forall x \in M$, $x \in \bar{x} \in M/M \cap N$, $\bar{x} = n_1\bar{e}_1 + \cdots + n_k\bar{e}_k \in M/M \cap N$. Therefore, $\overline{x - (n_1e_1 + \cdots + n_ke_k)} = 0$, i.e., $x - (n_1e_1 + \cdots + n_ke_k) \in M \cap N$. Since $\{f_1, \ldots, f_p\}$ is a basis of $M \cap N$, there exists $m_1, \ldots, m_p$ such that $x - (n_1e_1 + \cdots + n_ke_k) = m_1f_1 + \cdots + m_pf_p$. Hence, $\{e_1, \ldots, e_k, f_1, \ldots, f_p\}$ spans M for $x = n_1e_1 + \cdots + n_ke_k + m_1f_1 + \cdots + m_pf_p$.

– While $n_1e_1 + \cdots + n_ke_k + m_1f_1 + \cdots + m_pf_p = 0$, i.e., in $M/M \cap N$,$n_1e_1 + \cdots + n_ke_k + 0 = 0$, $n_1 = \cdots = n_k = 0$ since $\{e_1, \ldots, e_k\}$ is a basis of $M/M \cap N$. Then, from $m_1f_1 + \cdots + m_pf_p = 0$ in $M \cap N$, we can know that $m_1 = \cdots = m_p = 0$.

Therefore, M is a free module of rank less or equal to n.

□

3.2 From $GL_n(K)$ to $GL_n(\mathcal{O}_K)$

Let K be an algebraic number field whose ring of integers $\mathcal{O}_K$ is a principal ideal domain. In this subsection, we are going to prove that any finite subgroup of $GL_n(K)$ is isomorphic to a subgroup of $GL_n(\mathcal{O}_K)$. (Therefore, to classify subgroups of $GL_n(K)$, it suffices to classify subgroups of $GL_n(\mathcal{O}_K)$).

Let $G \subset GL_n(K)$ be a finite group. For any $g \in G$, $x \in K^n$, we have $gx \in K^n$. Regard $\mathcal{O}_K^n$ as a subset of K^n. We can define a subset Γ of K^n:

$$\Gamma := \{\sum_{i=1}^{m} g_i x_i : g_i \in G, x_i \in \mathcal{O}_K^n, m \in \mathbb{N}\}$$

We make the convention for the sum $\sum_{i=1}^{0} = 0$.

Apparently, we can know that Γ is an $\mathcal{O}_K$-module. Then, we are going to show that there exists $d \in \mathcal{O}_K$ such that $\mathcal{O}_K^n \subset \Gamma \subset \frac{1}{d}\mathcal{O}_K^n$. Furthermore, we can deduce that Γ is a free $\mathcal{O}_K$-module of rank n. In fact,

- $\forall x \in \mathcal{O}_K^n$, let $g_i := 1$, $x_i := x$ for any $i \in \mathbb{N}$, then $x = g_i x_i \in \Gamma$, which means $\mathcal{O}_K^n \subset \Gamma$.
- Since G is a finite subgroup of $GL_n(K)$, there are finite elements in G. For $\mathcal{O}_K^n$ is the ring of integers in K, K is the fraction field of $\mathcal{O}_K^n$. Let d be the least common multiple of the denominators of entries in G whose existence is guaranteed by the fact that $\mathcal{O}_K$ is a principal ideal domain and thus a unique factorization domain. $\forall x \in \Gamma$, $x = \sum_1^m g_i x_i$ where $g_i \in G$, $x_i \in \mathcal{O}_K^n$ and $m \in \mathbb{N}$. Since the entries of g_i are in $\frac{1}{d}\mathcal{O}_K$, we conclude that $x \in \frac{1}{d}\mathcal{O}_K^n$. That is to say, $\Gamma \subset \frac{1}{d}\mathcal{O}_K^n$.
- Since Γ is a sub-module of $\frac{1}{d}\mathcal{O}_K^n$, Γ is a free $\mathcal{O}_K$-module of rank less or equal to n. Since $\mathcal{O}_K^n$ is a sub-module of Γ, $\mathcal{O}_K^n$ is of rank n less or equal to the rank of Γ. Then, Γ is a free $\mathcal{O}_K$-module of rank n,

Therefore, there exists an $\mathcal{O}_K$-basis of Γ, namely, $e_1, \ldots, e_n$. Write every e_i in the coordinate form:

$$e_1 = [a_{11}, a_{21}, \ldots, a_{n1}]$$

$$\ldots$$

$$e_k = [a_{1k}, a_{2k}, \ldots, a_{nk}]$$

$$\ldots$$

$$e_n = [a_{1n}, a_{2n}, \ldots, a_{nn}]$$

with each entry an element in K. Then, we can define a matrix Q:

$$Q = \begin{bmatrix} a_{11}, a_{12}, \ldots, a_{1n} \\ \cdots \\ a_{k1}, a_{k2}, \ldots, a_{kn} \\ \cdots \\ a_{n1}, a_{n2}, \ldots, a_{nn} \end{bmatrix}$$

Apparently, $\{e_1, \ldots, e_n\}$ is a basis of K^n as $K-$vector space and every column of Q is linearly independent, so we can know that Q is in $GL_n(K)$. Then, we are going to show that for any $g \in G$, there exists $Q^{-1}gQ \in GL_n(K)$ so that we can deduce that G is isomorphic to a subgroup of $GL_n(\mathcal{O}_K)$.

Lemma 3.2.1 *For any $g \in G$, $Q^{-1}gQ$ is a map from $\mathcal{O}_K^n$ to $\mathcal{O}_K^n$ and is invertible.*

Proof Let $\{v_1, \ldots, v_n\}$ be the canonical basis of $\mathcal{O}_K^n$ and $\{e_1, \ldots, e_n\}$ be a basis of Γ. We can understand Q as a map from $\mathcal{O}_K^n$ to Γ: $\{v_1, \ldots, v_n\} \mapsto \{e_1, \ldots, e_n\}$.

- Surjectivity: $\forall x \in \Gamma, \exists s_1, \ldots, s_n \in \mathcal{O}_K$ such that $x = s_1e_1 + \cdots + s_ne_n = s_1Qv_1 + \cdots + s_nQv_n = Q(s_1v_1 + \cdots + s_nv_n)$
- Injectivity: Let $x = \lambda_1v_1 + \cdots + \lambda_nv_n$ be an element in $ker Q$.Then, $Qx = \lambda_1e_1 + \cdots + \lambda_ne_n = 0$. Since $e_1, \ldots, e_n$ is linearly independent, $\lambda_1 = \cdots = \lambda_n = 0$, i.e., $\ker Q = 0$.

Therefore, Q is bijective. Similarly, we can consider the matrix $g \in G$ as a map from Γ to Γ:$\{e_1, \ldots, e_n\} \mapsto \{ge_1, \ldots, ge_n\}$. Obviously, g is bijective since g is an invertible matrix whose inverse is also a map from Γ to Γ. Then, for any $x \in \mathcal{O}_K^n$, $Q^{-1}gQx$ is in $\mathcal{O}_K^n$, which means that $Q^{-1}gQ$ is a map from $\mathcal{O}_K^n$ to $\mathcal{O}_K^n$. Therefore, $Q^{-1}gQ$ is invertible since it is bijective. Then, $Q^{-1}gQ$ is in $GL_n(\mathcal{O}_K)$. □

We are ready to prove that G is isomorphic to a subgroup of $GL_n(\mathcal{O}_K)$. Define a map ϕ from G to $GL_n(\mathcal{O}_K)$: $g \mapsto Q^{-1}gQ$. We will prove that ϕ gives an isomorphism of G to a subgroup of $GL_n(\mathcal{O}_K)$:

- Homomorphism: $\phi(I) = Q^{-1}IQ = I$ and $\phi(AB) = Q^{-1}ABQ = Q^{-1}AQQ^{-1}BQ = \phi(A)\phi(B)$.
- Injectivity: Let x be in $\ker \phi$. From $\phi(x) = Q^{-1}xQ = I$, we can know that $I = QIQ^{-1} = QQ^{-1}xQQ^{-1} = x$, which is to say, $\ker \phi = 1$, i.e., ϕ is injective.

Hence, G is isomorphic to the image of ϕ as groups. Therefore, any finite subgroup of $GL_n(K)$ is isomorphic to a finite subgroup of $GL_n(\mathcal{O}_K)$.

3.3 Finite Subgroups of $GL_n(\mathcal{O}_K)$

In this subsection, we are going to prove that, up to isomorphism, there are only finitely many finite subgroups in $GL_n(\mathcal{O}_K)$.

First of all, we define a set of prime numbers

$$\mathcal{E} = \{p : p \text{ is a prime number and is the order of an element in } GL_n(K)\} \cup \{2\}.$$

This set, as we shall see soon, contains the prime numbers that do not have the properties we need. So we call the prime numbers in this set "*exceptions*".

By Corollary 2.2.1, we can see that in fact $\mathcal{E}$ is a finite set. This is an important fact that we will use continuously in what follows.

Now let $p \notin \mathcal{E}$ be a non-exceptional prime number and x be a prime factor of p in $\mathcal{O}_K$.

Lemma 3.3.1 *$\mathcal{O}_K/(x)$ is a finite field.*

Proof $\mathcal{O}_K/(x)$ is a field since x is a prime element in $\mathcal{O}_K$. We can define a map ϕ:

$$\phi : \mathbb{Z} \hookrightarrow \mathcal{O}_K \longrightarrow \mathcal{O}_K/(x).$$

Clearly, since $\ker\phi = p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker\phi \cong Im\phi \subset \mathcal{O}_K/(x)$. Therefore, $\mathcal{O}_K/(x)$ is an extension of $\mathbb{F}_p$. As a well-known fact, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of finite rank $[K:\mathbb{Q}]$ (c.f. [4, p.45]). Then, let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. For any $x \in \mathcal{O}_K$, we can write x as $\sum_1^n \lambda_i e_i$ where $\lambda_i \in \mathbb{Z}$. Hence, $\bar{x} = \sum_1^n \overline{\lambda_i e_i} \in \mathcal{O}_K/(x)$ where $\bar{\lambda}_i \in \mathbb{Z}/\mathbb{Z} \cap (x) = \mathbb{Z}/p\mathbb{Z}$. So $\mathcal{O}_K/(x)$ can be spanned by $\{\bar{e}_1, \ldots, \bar{e}_n\}$ as the vector space of $\mathbb{Z}/p\mathbb{Z}$. The dimension of $\mathcal{O}_K/(x)$ is no bigger than n over $\mathbb{F}_p$, which implies that $\mathcal{O}_K/(x)$ is a finite field. □

Now, we can define a group homomorphism:

$$\tau_x : GL_n(\mathcal{O}_K) \to GL_n(\mathcal{O}_K/(x))$$

by modulo x for each entry. This homomorphism has the following interesting property:

Proposition 3 *For $g \in \ker\tau_x$ and $l \in \mathbb{N}$ such that $p \nmid l$, if $g^l = 1$, then $g = 1$.*

Proof For $g \in \ker\tau_x$, $\tau_x(g) = [1]$, which means that $g = 1 + h$ where p divides all entries of h. It suffices to prove the proposition for l a prime number. In fact, for $l \geq 2$, $l = p_1 \ldots p_r$, g' is defined to be $g^{p_1 \cdots p_{r-1}}$. Then, $g' \equiv 1^{p_1 \cdots p_{r-1}} = 1 \bmod x$. Since $g'^{p_r} = g^l \equiv 1 \bmod x$, we can know that $g' = 1$ if we assume the proposition for l a prime number is true. By induction on r, $g = 1$.

Now we assume that l is a prime number not equal to p. May assume by contradiction that $h \neq 0$. We can write h as xdh' where $d \in \mathcal{O}_K$ and $h' \in M_n(\mathcal{O}_K)$ such that the greatest common divisor of entries of h' is 1.

$$\begin{aligned} g^l &= (1+h)^l \\ &= (1+xdh')^l \\ &= (xdh')^l + \binom{l}{l-1}(xdh')^{l-1} + \cdots + lxdh' + 1 \end{aligned}$$

By $g^l = 1$, we can know that $(xdh')^l + \binom{l}{l-1}(xdh')^{l-1} + \cdots + lxdh' = 0$. Since $\mathcal{O}_K$ is a domain,

$$(xd)^{l-1}h'^n + \binom{l}{l-1}(xd)^{l-2}h'^{l-1} + \cdots + lh' = 0.$$

Then, from the fact that x divides $(xd)^{l-1}h'^n + \binom{l}{l-1}(xd)^{l-2}h'^{l-1} + \cdots + \binom{l}{2}xdh'^2$, we conclude that $x|lh'$, and therefore, $x|l$ in $\mathcal{O}_K$ since the greatest common divisor of entries of h is 1. Because x divides p and l, p are not coprime in $\mathcal{O}_K$, we know that l, p are not coprime in $\mathbb{Z}$ according to Bézout's theorem. Therefore, $l = p$, which is contradictory to our assumption of l. Hence, $h = 0$. □

Theorem 3.3.1 *For any finite subgroup $G \subset GL_n(\mathcal{O}_K)$, τ_x gives an isomorphism of G to a subgroup of $GL_n(\mathcal{O}_K/(x))$.*

Proof We define a map ϕ: $G \longrightarrow GL_n(\mathcal{O}_K/(x))$ by modulo x for each entry. We are going to show that ϕ gives an isomorphism from G to the image of ϕ. Apparently, ϕ is a group homomorphism. It suffices to show ϕ is injective. In fact, since $\ker\phi = \ker\tau_x \cap G$. For any $g \in \ker\phi$, $g \in G$, then there exists $m \in \mathbb{N}$ such that $g^m = 1$ since G is a finite subgroup. From our choice of p, p does not divide m. Therefore, by the preceding proposition, $g = 1$. This proves the injectivity of ϕ. Hence, ϕ gives an isomorphism from G to the image of ϕ. □

From this theorem, we conclude that any finite subgroup of $GL_n(\mathcal{O}_K)$ is isomorphic to a subgroup of $GL_n(\mathcal{O}_K/(x))$, whereas the latter, being a finite group since $\mathcal{O}_K/(x)$ is a finite field, has only finitely many subgroups. Taking account of the result of Section 3.2, we have finally proven the following theorem:

Theorem 3.3.2 *Let n be a natural number and K be an algebraic number field whose ring of integers is a principal ideal domain. Then there are finitely many finite subgroups of $GL_n(K)$, up to isomorphism.*

4 A Bound for the Order of Finite Subgroups of $GL_n(K)$

The preceding section shows that there are only finitely many finite subgroups of $GL_n(K)$. It is thus interesting to give an upper bound for the order of subgroups of $GL_n(K)$ for a given n and a given algebraic number field K. In this section, we are going to present a general method to calculate an upper bound and apply it to special cases.

4.1 Preliminaries

We present some tools and theorems that will be used in calculating the upper bound.

Lemma 4.1.1 *Let $\mathbb{F}_q$ be a finite field with q elements and n be a natural number. Then there are $q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\dots(q-1)$ elements in the group $GL_n(\mathbb{F}_q)$.*

Proof A matrix is invertible if and only if its rows are linearly independent. For the first row, the only constraint is that it cannot be $(0,\dots,0)$, so there are q^n-1 choices of the first row. Assume the first k rows are chosen, and to make sure the $(k+1)$-th row is linearly independent of the first k rows, it should not lie in the k-dimensional subspace spanned by the first k rows. So there are $q^n - q^k$ choices of the $(k+1)$-th row. In total, there are $(q^n-1)(q^n-q)\dots(q^n-q^{n-1}) = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\dots(q-1)$ choices of invertible matrices. □

Lemma 4.1.2 *Let ℓ be a prime number, then $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ is a cyclic group.*

Proof Since $|(\mathbb{Z}/\ell^2\mathbb{Z})^\times| = \ell(\ell-1)$, it suffices to find an element of order $\ell(\ell-1)$ in $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. First notice that $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is cyclic since $\mathbb{Z}/\ell\mathbb{Z}$ is a field. We can find an integer x' such that the order of x' modulo ℓ is $\ell-1$. The order of x' modulo ℓ^2 is thus $d(\ell-1)$ in $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ for some $d \geq 1$. Then $x := x'^d$ is of order $\ell-1$ modulo ℓ^2. Then, we find that $y = 1+\ell$ is of order ℓ modulo ℓ^2 by noticing the following congruence equation:

$$(1+\ell)^k \equiv 1 + k\ell \bmod \ell^2.$$

Finally, since ℓ and $\ell-1$ are coprime, xy is of order $\ell(\ell-1)$ modulo ℓ^2. In other word, $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ is a cyclic group. □

Theorem 4.1.1 (Dirichlet's arithmetic progression) *Let m, n be two coprime integers and $m > 0$. Then there are infinitly many prime numbers of the form $mk + n$ for $k \in \mathbb{N}$.*

For a proof of this result, we refer the readers to Serre's textbook [6, pp. 61-76].

Theorem 4.1.2 (Chinese remainder theorem) *Let m, n be coprime integers and a, b be any given integers. Then there exists $x \in \mathbb{Z}$ such that*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

Such x is unique modulo mn.

Proof Chinese remainder theorem is equivalent to saying that the ring homomorphism

$$\begin{array}{rccc} \Phi: & \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & x & \mapsto & (x \bmod m, x \bmod n) \end{array}$$

is bijective. Since both sides have mn elements, it suffices to show that Φ is injective. In fact, let $x \in \ker \Phi$, then $m|x, n|x$. But m, n are coprime, this implies that $mn|x$, i.e. $x = 0$ in $\mathbb{Z}/mn\mathbb{Z}$. □

4.2 General Method to Calculate the Upper Bound

Let $G \subset GL_n(K)$ be a finite group. Let $p > 2$ be a prime number and $x \in \mathcal{O}_K$ be a prime factor of p in $\mathcal{O}_K$. Since the characteristic of $\mathcal{O}_K/(x)$ is p, $\mathcal{O}_K/(x)$ is isomorphic to $\mathbb{F}_{p^r}$ for some $r \geq 1$. To make the notation pithy, we write $\mathbb{F}_{p^r}$ as $\mathbb{F}_q$. Aside from finitely many exceptional prime numbers p, G can be viewed as a subgroup of $GL_n(\mathcal{O}_K/(x))$, i.e., $GL_n(\mathbb{F}_q)$. (Corollary 2.2.1 and Theorem 3.3.1)

Let $\ell \geq 2$ be a fixed prime number, $\nu_\ell(|G|)$ is defined to be the power of ℓ of $|G|$. Then by the theorem of Lagrange, $\nu_\ell(|G|)$ is less or equal to $\nu_\ell(|GL_n(\mathbb{F}_q)|)$. Therefore, finding the minimum of $\nu_\ell(|GL_n(\mathbb{F}_q)|)$ suffices to calculate the maximum of $\nu_\ell(|G|)$. Since

$$|GL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\dots(q-1),$$

By Fermat's little theorem, $p^{\ell-1} - 1 \equiv 0$ by modulo ℓ, so ℓ is certainly a factor of $|GL_n(\mathbb{F}_q)|$ as n becomes large. However, we don't know clearly the power of ℓ and we want it to be as small as possible. Then, we consider what the power of ℓ^2 is in $|GL_n(\mathbb{F}_q)|$. As we know from Lemma 4.1.2 above, $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ is a cyclic group, which is to say, there exists an $x \in \mathbb{Z}$ such that $Ord_{\ell^2}(x) = \ell(\ell-1)$. Then, we define x in this way and as long as $p \equiv x$ by modulo ℓ^2, p satisfies $Ord_{\ell^2}(p) = \ell(\ell-1)$. According to Dirichlet's arithmetic progression, there are infinitely many prime numbers in $\{k\ell^2 + x\}$, while there are only finitely many exceptions which p can not be chosen from, then we can find a prime number $p = k\ell^2 + x$ such that $Ord_{\ell^2}(p) = \ell(\ell-1)$.

Then, we can find a way to calculate $\nu_\ell(p^k-1)$ for any $k \le n$. Moreover, we demand that $\ell > 2$ in this following case and we will consider $\ell = 2$ later. By a direct expansion, we find

$$\nu_\ell(p^k-1) = \begin{cases} 1+\nu_\ell(k) & \text{if } \ell-1 | k \\ 0 & \text{if } \ell-1 \nmid k \end{cases}$$

As a result, we can calculate $\nu_\ell(GL_n(\mathbb{F}_q))$ by the equation above. Let m be the greatest common divisor of r and $\ell-1$, then we can know that $\frac{\ell-1}{m} \mid k$ since $\ell-1 \mid rk$. So let $k = d\frac{\ell-1}{m}$.

$$\begin{aligned}
\nu_\ell(GL_n(\mathbb{F}_{p^r})) &= \sum_{k=1}^{n} \nu_\ell(p^r k - 1) \\
&= \sum_{d=1}^{\lfloor \frac{mn}{\ell-1} \rfloor} \nu_\ell(p^{rd\frac{\ell-1}{m}} - 1) \\
&= \lfloor \frac{mn}{\ell-1} \rfloor + \sum_{d=1}^{\lfloor \frac{mn}{\ell-1} \rfloor} \nu_\ell(rd\frac{\ell-1}{m}) \\
&= \lfloor \frac{mn}{\ell-1} \rfloor + \sum_{d=1}^{\lfloor \frac{mn}{\ell-1} \rfloor} \nu_\ell(rd) \\
&= \lfloor \frac{mn}{\ell-1} \rfloor (1+\nu_\ell(r)) + \sum_{d=1}^{\lfloor \frac{mn}{\ell-1} \rfloor} \nu_\ell(d) \\
&= \lfloor \frac{mn}{\ell-1} \rfloor (1+\nu_\ell(r)) + \nu_\ell(\lfloor \frac{mn}{\ell-1} \rfloor !)
\end{aligned}$$

Now we consider the situation that $\ell = 2$. In this case, $p = 2^e x + 1$ for $e \in \mathbb{Z}$ and x is not an even number. Then, we know that $p^k = (2^e x+1)^k = 1 + k2^e x + \binom{k}{2}(2^e x)^2 + \ldots + (2^e x)^k$. We classify the possible values of e into two parts:

- When $e > 1$, $\nu_\ell(p^k - 1) = \nu_\ell(k) + e$. To make e as small as possible, we consider $e = 2$, which means $p \equiv 5$ by modulo 8. Therefore, $\sum_{k=1}^{n} \nu_2(p^{rk}-1) = \sum_{k=1}^{n}(2+\nu_2(rk)) = n(2+\nu_2(r)) + \nu_2(n!)$.
- When $e = 1$, i.e., $p \equiv 3$ by modulo 4, we can know that $\nu_2(p^k-1) = \nu_2(2kx + 2k(k-1)x^2) = \nu_2(2kx(1+(k-1)x)) = \nu_2(k)+1+\nu_2(1+(k-1)x)$. To avoid possible explosion of $\nu_2(1+(k-1)x)$ as k varies, we can take p as small as we can. Take $p = 3$ when 3 is not in the exceptions, then $\nu_2(3^k-1) = 1+2\nu_2(k)$. Therefore, we can get the minimum possible value of $GL_n(\mathbb{F}_{p^r})$:

$$\sum_{k=1}^{n} \nu_2(3^{rk}-1) = \sum_{k=1}^{n}(1+2\nu_2(rk)) = n(1+2\nu_2(r)) + 2\nu_2(n!).$$

4.3 Some Examples

In this subsection, we will give three examples to show how sharp the upper bound we calculated above is.

Example Let $K = \mathbb{Q}[\sqrt{-1}]$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$. Let p be a prime number in $\mathbb{Z}$. As we know, if p is a prime element in $\mathcal{O}_K$, then $p \equiv 3$ by modulo 4; if p is not a prime element in $\mathcal{O}_K$, then $p \equiv 1$ by modulo 4 or $p = 2$. Since there is $\nu_\ell(r)$ in the calculation of $|GL_n(\mathbb{F}_q)|$, we want the value of r as small as possible. We hope that $r = 1$, i.e., $\mathbb{Z}[\sqrt{-1}]/(x) \cong \mathbb{F}_p$ where x is a prime element in $\mathbb{Z}[\sqrt{-1}]$ that divides p. When can this happen?

Claim If x is a prime factor of p where $p \equiv 1 \bmod 4$ or $p = 2$ in $\mathbb{Z}[\sqrt{-1}]$, then $\mathbb{Z}[\sqrt{-1}]/(x) \cong \mathbb{F}_p$.

Proof We are going to show that for any element $y \in \mathbb{Z}[\sqrt{-1}]$, there exists $k \in \mathbb{Z}[\sqrt{-1}]$ such that $y = kx + a$ where $a = 0, \ldots, p-1$. In fact, let $e = g + hi$, $x = c + di$ with c coprime with d and $y = M + Ni$. Let $y = M + Ni = ex + s = (g + hi)(c + di) + s = gc - hd + (gd + hc)i + s$ where $s \in \mathbb{Z}$. Since c is coprime with d, we can find suitable g, h such that $gd + hc = N$. However, we do not know whether $s = 0, 1, \ldots, p-1$. Then, we make s equal $a + mp$ where $m \in \mathbb{Z}$ and $a = 0, 1, \ldots, p-1$. Since $p = x\bar{x}$, we know that $M + Ni = (g + hi)(c + di) + a + mx\bar{x} = x(g + hi + m\bar{x}) + a$. Thus, we represent $M + Ni$ as $kx + a$ for some $k \in \mathbb{Z}[\sqrt{-1}]$ and $a \in \{0, 1, \ldots, p-1\}$. Therefore, we prove that $\mathbb{Z}[\sqrt{-1}]/(x)$ has exactly p elements and it is thus isomorphic to $\mathbb{F}_p$. □

We now use the result of the preceding section to give upper bounds of finite subgroups of $GL_n(\mathbb{Q}[\sqrt{-1}]$ for $n = 2, 3$. In what follows, let G be a finite subgroup of $GL_n(\mathbb{Q}[\sqrt{-1}]$.

- When $n = 2$. We take a prime number $p \equiv 1 \bmod 4$ which is not an exception. In this case, $r = m = 1$ in the formula of $\nu_\ell(GL_n(\mathbb{F}_{p^r})$. For $\ell > 3$, we find that $\lfloor \frac{mn}{\ell - 1} \rfloor = 0$, and thus
$$\nu_\ell(|G|) \leq \nu_\ell(GL_n(\mathbb{F}_{p^r})) = \lfloor \frac{mn}{\ell - 1} \rfloor (1 + \nu_\ell(r)) + \nu_\ell(\lfloor \frac{mn}{\ell - 1} \rfloor !) = 0.$$
For $\ell = 3$, we find
$$\nu_\ell(|G|) \leq \nu_\ell(GL_n(\mathbb{F}_{p^r}) = \lfloor \frac{mn}{\ell - 1} \rfloor (1 + \nu_\ell(r)) + \nu_\ell(\lfloor \frac{mn}{\ell - 1} \rfloor !) = 1 \times (1 + 0) + 0 = 1.$$
For $\ell = 2$, by taking a prime number $p \equiv 5 \bmod 8$ which is not an exception and by utilizing the formula of the preceding part, we find
$$\nu_2(|G|) \leq n(2 + \nu_2(r)) + \nu_2(n!) = 2 \times 2 + 1 = 5.$$
Taking account of all the calculations above, we conclude that $|G|$ divides $2^5 \times 3^1 = 96$.

- When $n = 3$, we also take a prime number $p \equiv 1 \bmod 4$ which is not an exception. In this case, $r = m = 1$ in the formula of $\nu_\ell(GL_n(\mathbb{F}_{p^r})$. For $\ell > 3$, we find that $\lfloor \frac{mn}{\ell - 1} \rfloor = 0$, and thus
$$\nu_\ell(|G|) \leq \nu_\ell(GL_n(\mathbb{F}_{p^r})) = \lfloor \frac{mn}{\ell - 1} \rfloor (1 + \nu_\ell(r)) + \nu_\ell(\lfloor \frac{mn}{\ell - 1} \rfloor !) = 0.$$
For $\ell = 3$, we find that
$$\nu_\ell(|G|) \leq \nu_\ell(GL_n(\mathbb{F}_{p^r}) = \lfloor \frac{mn}{\ell - 1} \rfloor (1 + \nu_\ell(r)) + \nu_\ell(\lfloor \frac{mn}{\ell - 1} \rfloor !) = 1 \times (1 + 0) + 0 = 1.$$
For $\ell = 2$, by taking a prime number $p \equiv 5 \bmod 8$ which is not an exception and by utilizing the formula of the preceding part, we find
$$\nu_2(|G|) \leq n(2 + \nu_2(r)) + \nu_2(n!) = 3 \times 2 + 1 = 7.$$
Taking account of all the calculations above, we conclude that $|G|$ divides $2^7 \times 3^1 = 384$.

Example Let $K = \mathbb{Q}[\sqrt{-2}]$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. Let p be a prime number in $\mathbb{Z}$. As we know, if p is not a prime element in $\mathbb{Z}[\sqrt{-2}]$, i.e., p can be written as $a^2 + 2b^2$, then $p \equiv 1, 3$ by modulo 8.

We now use the result of the preceding section to give upper bounds of finite subgroups of $GL_n(\mathbb{Q}[\sqrt{-2}])$ for $n = 2$. Let G be a finite subgroup of $GL_n(\mathbb{Q}[\sqrt{-1}])$. Let $x \in \mathbb{Z}$ such that $Ord_{\ell^2} x = \ell(\ell - 1)$. We take a prime number $p \equiv 1, 3$ by modulo 8 and $p \equiv x$ by modulo ℓ^2 which is not an exception. In this case, $r = m = 1$ in the formula of $\nu_\ell(GL_n(\mathbb{F}_{p^r})$. For $\ell > 3$, we find that $\lfloor \frac{mn}{\ell-1} \rfloor = 0$, and thus

$$\nu_\ell(|G|) \leq \nu_\ell(GL_n(\mathbb{F}_{p^r})) = \lfloor \frac{mn}{\ell - 1} \rfloor (1 + \nu_\ell(r)) + \nu_\ell(\lfloor \frac{mn}{\ell - 1} \rfloor !) = 0.$$

For $\ell = 3$, we find

$$\nu_\ell(|G|) \leq \nu_\ell(GL_n(\mathbb{F}_{p^r})) = \lfloor \frac{mn}{\ell - 1} \rfloor (1 + \nu_\ell(r)) + \nu_\ell(\lfloor \frac{mn}{\ell - 1} \rfloor !) = 1 \times (1 + 0) + 0 = 1.$$

For $\ell = 2$, since $p \equiv 1, 3$ by modulo 8, we take $p \equiv 3$ by modulo 4 in this case. To avoid possible explosion of $\nu_2(1 + (k-1)x)$ as k varies, we can take p as small as we can. Since p is not among the exceptions which are orders of elements in $GL_2(\mathbb{Q}[\sqrt{-2}])$, while the elements in $GL_2(\mathbb{Q}[\sqrt{-2}])$ has only six possible orders: $1, 2, 3, 4, 6, 8$, we can take $p = 11$ in this case. By the formula above, we find that $\nu_2(11^k - 1) = \nu_2(k) + 1 + \nu_2(5k - 4)$. Hence,

$$\nu_\ell(|G|) \leq \nu_\ell(GL_n(\mathbb{F}_{11})) = \sum_{k=1}^{n} (1 + \nu_\ell(k) + \nu_\ell(5k - 4)) = n + \nu_2(n!) + \sum_{k=1}^{n} \nu_2(5k - 4) = 4.$$

Taking account of all the calculations above, we conclude that $|G|$ divides $2^4 \times 3^1 = 48$.

References

[1] P. M. Gudivok, A. A. Kiri]yuk, V. P. Rud'ko, and A. I. Tsitkin, *Finite Subgroups of the Group $GL(n, \mathbb{Z})$*, Translated from Kibernetika, No. 6, pp. 71-82, November-December, 1982. Original ar- ticle submitted June 30, 1982.

[2] G. Mackiw, *Finite Groups of 2×2 Integere Matrices*, Mathmatics Magazines, Vol. 69, No. 05, Dec. 1996.

[3] H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, J.Crelle 101 (1887), 196–202 (= Ges.Abh., Band I, n.VI)

[4] Jürgen Neukirch, *Algebraic Number Theory*, 1999, Springer-Verlag Berlin Heidelberg.

[5] I. Schur, *Uber eine Klasse von endlichen Gruppen linearer Substitutionen*, Sitz. Preuss. Akad. Wiss. Berlin (1905), 77–91 (= Ges.Abh., Band I, n. 6).

[6] J.P. Serre, *A Course in Arithmetic*, 1996, Springer.

[7] S. H. Weinstraub, *Galois Theory*, 2009, Spring-Verlag New York.

Acknowledgments

I would like to express my full appreciation to all my maths teachers, who have helped develop my interest in mathematics since I was young. Especially, I shall give my sincerest acknowledgment to my present school math teacher Ms. Guo Peihua, as my instructor of this research. She encouraged me a lot in my process of studying and gave useful suggestions. Moreover, I would like to pay gratitude to my families and friends who have supported me in many ways. Last but not least, I wish to thank the committee of Yau Awards for providing such a valuable opportunity for me to learn more and discover something in the area of mathematics.