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

Ying Li

269 South Third Ring Road, Xiushui Road, Shengze Town, Wujiang District, Suzhou City, Jiangsu Province, China
E-mail: liying_louisechina@163.com

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 multiplicative bound for the orders of finite subgroups and to classify finite cyclic subgroups.

1. Introduction
For a given positive integer \( n \), 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 generalized this result by replacing \( \mathbb{Q} \) with any algebraic number field [5]. He used the character theory of finite groups to obtain this result.[4]

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 [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 \( GL_n(K) \) for a given positive integer \( n \) and for an algebraic number field \( K \). In practice, we have obtained the following partial results:

- 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] when the ring of integers in \( K \) is a principal ideal domain, without using the character theory of finite groups.
- In Section 4, we give a general method to calculate a multiplicative bound of finite subgroups of \( GL_n(K) \).

The general results proposed in Section 2 and 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 precisely \( C_1, C_2, C_3, C_4, C_6, C_8, C_{12} \), 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 precisely \( C_1, C_2, C_3, C_4, C_6, C_8, C_{12} \), 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 precisely \( C_1, C_2, C_3, C_4, C_6, C_8, C_{12} \), up to isomorphism.

The above results are calculated explicitly in Sections 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 classification. For example, the symmetric group $S_3$ is not in $GL_2(\mathbb{Q}[\sqrt{-3}])$, since $|S_3|$ contains 5 as a factor whereas we prove that the order of any finite subgroup of $GL_2(\mathbb{Q}[\sqrt{-3}])$ divides 96. For similar reasons, we know that $S_3$ is not in $GL_2(\mathbb{Q}[\sqrt{-2}])$ or in $GL_3(\mathbb{Q}[\sqrt{-3}])$, 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 positive integer and $\mathbb{U}_n$ be the set of primitive $n$-th roots of unity in $\mathbb{C}$. In other words, $\mathbb{U}_n$ consists of 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 $\Phi_n$ 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.

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

1. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
2. For each $n$, $\Phi_n$ is a polynomial with integer coefficients.
3. $\Phi_n$ 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 $k = 0, 1, \cdots, n - 1$. 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 $\Phi_d(X)$. Therefore, $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

2. First, we are going to prove that $\Phi_p$ is a polynomial with integer coefficients when $p$ is a prime number. Since $X^{p-1} - 1 = \Phi_1(X)\Phi_p(X) = (X - 1)\Phi_p(X)$, we can easily know that $\Phi_p(X) = \frac{X^{p-1} - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{p-1}$, 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 $X^n - 1 = \prod_{d|n, d<n} \Phi_d(X)$, $\Phi_n(X)$ 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]

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

Proof: Since $\zeta_n$ is a root of $\Phi_n$, which is irreducible in $\mathbb{Q}[X]$, $\Phi_n$ is the minimal polynomial of $\zeta_n$ 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.

Property of the order of an element in $GL_n(K)$

In this part, we shall give a property of the order of an element of $GL_n(K)$. To begin with, let $\zeta_n$ be a primitive $n$-th root of unity and $\Phi_n(X)$ 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:

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

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

In what follows, we shall denote

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

Notice that $\phi_K(n) = \phi(n)$ is nothing but the Euler totient function.

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

Proof: Let $\mu_A \in K[X]$ be the minimal polynomial of $A$ with order $d$. Then $\mu_A \mid (X^d - 1)$ and $\mu_A \not\mid (X^d - 1)$ for every $1 \leq d' < d$. By the property of cyclotomic polynomials, $X^d - 1 = \prod_{\ell \mid d} \Phi_\ell(X)$. If we write $\Phi_\ell(X)$ by its irreducible decomposition:

$$\phi_\ell(X) = \Phi_{\ell,1}(X) \cdot \cdots \cdot \Phi_{\ell,r_\ell}(X),$$

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

$$X^d - 1 = \prod_{\ell \mid d} \Phi_{\ell,1}(X) \cdot \cdots \cdot \Phi_{\ell,r_\ell}(X).$$

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

$$\mu_A = \prod_{\ell \mid d \text{ some } \ell} \Phi_{\ell,1}(X) \cdot \cdots \cdot \Phi_{\ell,s_\ell}(X),$$

where $1 \leq s_\ell \leq r_\ell$. We claim that the least common multiple of these $\ell$ must be $d$. In fact, we assume by contradiction that the least common multiple of these $\ell$ is $d'$ where $1 \leq d' < d$, and then $\mu_A \mid (X^{d'} - 1)$, which contradicts the fact that $\mu_A \not\mid (X^{d'} - 1)$ for any $1 \leq d' < d$. By the discussion above, since $\deg \Phi_{\ell,1}(X) = \phi_K(\ell)$ for any $1 \leq \ell < s_\ell$, 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 $\ell$ is $d$. On the other hand, by the Hamilton-Cayley theorem, $\mu_A \mid \chi_A$, so we can get the inequality 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 these $\ell$ is $d$.

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

Proof: Let $d$ be the order of an element in $GL_n(K)$. According to Telescopic extension theorem,

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

We get this equation:

$$\phi_K(\ell) = [K[\zeta]: K] = \frac{[K[\zeta]: \mathbb{Q}[\zeta]] \cdot \phi(\ell)}{[K: \mathbb{Q}]}.$$
In particular, it implies this equality:

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

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

$$\sum \phi_K(\ell) \leq n[\mathbb{Q} : \mathbb{Q}]$$

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

Some examples

In this section, we are going to classify finite cyclic subgroups for $GL_2(\mathbb{Q}[\sqrt{-1}])$, $GL_2(\mathbb{Q}[\sqrt{-3}])$, and $GL_2(\mathbb{Q}[\sqrt{-2}])$ by using the method mentioned above to show how the mechanism works. For this purpose, we stretch a famous result from [7]:

2.1.6. Theorem. Let $d > 1$ be a positive integer and we denote

$$A'_d = \{\left(\frac{-1}{p}\right) : p \text{ is an odd prime number dividing } d\},$$

where $\left(\frac{-1}{p}\right)$ is the Legendre symbol. Then, we define

$$A_d = \begin{cases} A'_d \cup \{-1\} & \text{if } d \equiv 4 \text{ mod } 8; \\ A'_d \cup \{-1, 2\} & \text{if } d \equiv 0 \text{ mod } 8; \\ A'_d & \text{otherwise}. \end{cases}$$

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

2.1.7. 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:

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

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

$$[K[\zeta_d] : \mathbb{Q}[\zeta_d]] = \begin{cases} 1 & \text{if } \sqrt{-1} \in \mathbb{Q}[\zeta_d]; \\ 2 & \text{if } \sqrt{-1} \notin \mathbb{Q}[\zeta_d]; \end{cases}$$

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 when $4 \nmid \ell$, $\phi(\ell) \leq 2$, and when $4 \mid \ell, \phi(\ell) \leq 4$.

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

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

The possible values of $d$ are 1, 2, 3, 4, 6, 8, and 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 are obtainable.

In fact, we can indeed find possible elements of those different orders to show their existence.
Table 1. Restrict the possible orders of elements

| $d$ | Matrix |
|-----|--------|
| 1   | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ |
| 2   | $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ |
| 3   | $\begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$ |
| 4   | $\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -1 \end{pmatrix}$ |
| 6   | $\begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}$ |
| 8   | $\begin{pmatrix} 1 & \sqrt{-1} - 1 \\ \sqrt{-1} & -1 \end{pmatrix}$ |
| 12  | $\begin{pmatrix} \sqrt{-1} & -3\sqrt{-1} \\ \sqrt{-1} & -2\sqrt{-1} \end{pmatrix}$ |

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

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

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

2.1.8. Example. Let $K = \mathbb{Q}[\sqrt{-2}]$ and $d$ be the order of an element in $GL_n(\mathbb{Q}[\sqrt{-2}])$. By 2.3.1 Theorem above, we can get the following equation:

$$[K[\zeta_d]: \mathbb{Q}[\zeta_d]] = \begin{cases} 1 & \text{if } \sqrt{-2} \in \mathbb{Q}[\zeta_d]; \\ 2 & \text{if } \sqrt{-2} \not\in \mathbb{Q}[\zeta_d]; \end{cases}$$

which indicates that, in this case,

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

As shown in Table 2, 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 that when $8 \nmid \ell$, $\phi(\ell) \leq 2$, and when $8 \mid \ell$, $\phi(\ell) \leq 4$. Then, by calculation, we find that $\ell$ has six possible values: 1, 2, 3, 4, 6, 8. Since $d$ is the least common multiple of some $\ell$, with the constraint

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

the possible values of $d$ are 1, 2, 3, 4, 6, and 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 orders are exactly those possible values we find.
2.1.9. Table 2. The possible values and matrices

| \( d \) | Matrix          |
|-------|----------------|
| 1     | \[
| \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
| \] |
| 2     | \[
| \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}
| \] |
| 3     | \[
| \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}
| \] |
| 4     | \[
| \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}
| \] |
| 6     | \[
| \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}
| \] |
| 8     | \[
| \begin{pmatrix} \sqrt{-2} & 1 \\ 1 & 0 \end{pmatrix}
| \] |

When \( n = 3 \), like the case when \( n = 2 \), \( \phi_K(\ell) \leq 3 \) indicates that when \( 8 \nmid \ell \), \( \phi(\ell) \leq 3 \), and when \( 8 \mid \ell \), \( \phi(\ell) \leq 6 \). Then, by calculation, we find that \( \ell \) has six possible values: 1, 2, 3, 4, 6, 8. Since \( d \) is the least common multiple of some \( \ell \), with the constraint

\[
\sum S_\ell \phi_K(\ell) \leq n,
\]

the possible values of \( d \) are 1, 2, 3, 4, 6, and 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 \( 2 \times 2 \) matrix of order \( d \) in \( GL_2(\mathbb{Q}[\sqrt{-2}]) \), then

\[
\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}
\]

would be a \( 3 \times 3 \) 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 up to isomorphism, there are only finitely many finite subgroups of \( GL_n(K) \) for a given positive integer \( n \) and an algebraic 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.

Algebraic number fields whose rings of integers are principal ideal domains are important in practical mathematical uses. First of all, it is easier to calculate with elements instead of with ideals. More importantly, the structure of modules over a principal ideal domain is relatively much clearer than that over arbitrary commutative rings, as can be seen from Section 3.1. Therefore, these algebraic number fields are of special interests among all algebraic number fields. Some interesting facts or conjectures about this kind of algebraic number fields are listed below:

1. For an algebraic number field \( K \), \( \mathcal{O}_K \) is a principal ideal domain if and only if it is a unique factorization domain.

2. If \( K \) is an imaginary quadratic number field, i.e., if \( K = \mathbb{Q}[\sqrt{-d}] \) with \( d \) a square-free positive integer, then \( \mathcal{O}_K \) is a principal ideal domain if and only if \( d \) is one of

\[
1, 2, 3, 7, 11, 19, 43, 67, 163
\]

This interesting fact, discovered and conjectured by Carl Friedrich Gauss in 1801, turned out to be very difficult and was finally proven almost 150 years later.
3. Gauss also conjectured that there are infinitely many real quadratic number fields, i.e., number fields of the form \( \mathbb{Q}[\sqrt{d}] \) with \( d \) a positive integer, such that their rings of integers are principal ideal domains. This conjecture remains open nowadays.

We are not using these interesting facts in our article. We list them to show the importance of principal ideal domains in the studying of general algebraic number fields.

### 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 \( n \) are 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 of vector spaces over a field. But the properties of \( A \)-modules are more complicated.

#### 3.1.1. Definition

Let \( A \) be a commutative ring. A module \( M \) over \( A \) is a set endowed with two operations:

\[
\begin{align*}
+: M \times M &\rightarrow M; \\
\cdot: A \times M &\rightarrow M;
\end{align*}
\]

satisfying:

- (+ – axioms) \((M, +)\) is an abelian group;
- (∗ – axioms)
  - \( \forall \lambda, \mu \in A, x \in M, \lambda(\mu x) = (\lambda \mu)x \);
  - \( \forall x \in M, 1 \cdot x = x \);
  - \( \forall \lambda, \mu \in A, x \in M, (\lambda + \mu)x = \lambda x + \mu x \);
  - \( \forall \lambda \in A, x, y \in M, \lambda(x + y) = \lambda x + \lambda y \).

#### 3.1.2. Definition (Basis)

Let \( M \) be an \( A \)-module. \( B \subset M \) is called an \( A \)-basis of \( M \), if the following conditions hold:

- \( \forall x \in M, \exists x_1, \cdots, x_n \in B, \lambda_1, \cdots, \lambda_n \in A \), such that \( x = \sum^n x_i \lambda_i \);
- If \( x_1, \cdots, x_n \in B \) are distinct and for \( \lambda_1, \cdots, \lambda_n \in A \),
  \[
  \sum^n \lambda_i x_i = 0 \Rightarrow \lambda_i = 0, \forall i
  \]

The definition of an A-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:

\[
A^n = \{(x_1, \cdots, x_n) : x_i \in A\}
\]

where \( \forall \lambda \in A, (x_1, \cdots, x_n) \in A^n, \lambda(x_1, \cdots, x_n) := (\lambda x_1, \cdots, \lambda x_n) \). Apparently, \( A^n \) is an \( A \)-module. There exists a basis of \( A^n \), called the canonical basis of \( A^n \), namely, \( B := \{e_1, \cdots, e_n\} \), where \( e_i \) is an element in \( A^n \) which has 1 in its \( i \)-th position and 0 elsewhere. Therefore, we can draw the conclusion that \( A^n \) is a free \( A \)-module.

#### 3.1.3. Definition

Let \( M, N \) be \( A \)-modules. \( \phi: M \rightarrow N \) is called a homomorphism of \( A \)-modules (or \( A \)-linear map), if the following conditions hold:

\[
\begin{align*}
\forall x \in M, \lambda \in A, \phi(\lambda x) &= \lambda \phi(x); \\
\forall x, y \in M, \phi(x + y) &= \phi(x) + \phi(y).
\end{align*}
\]

Furthermore, \( \phi: M \rightarrow N \) is an A- isomorphism, denoted as \( M \cong N \), if it is a bijective homomorphism.

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.
Assume that \( M \) is not a submodule of \( N \). We can construct a map \( \phi : V \rightarrow N \). If \( V \) is a free \( N \)-module with rank \( r \), then \( \phi \) is surjective.

We define a module \( \mathbb{A} \) for \( N \) as follows: The follows directly from the above lemma. Since \( V \) is a submodule of \( N \) and \( \phi \) is surjective, then \( \phi \) is an \( N \)-module.

\[ \phi(x) \phi(y) = \phi(x+y) \]

mean that \( \phi \) is a homomorphism of \( N \)-modules.

Since \( A \) is a commutative ring, \( \mathbb{A} \) is a maximal ideal of \( A \). Then \( A' \) is the quotient ring of \( A \) by the ideal \( \mathbb{A} \). This follows directly from the above lemma.
\[ \text{Im} \psi \subset A^{n-1} \]. By induction assumption, \( M/M \cap N \) is free of rank \( \leq n - 1 \). Then, we need to prove that \( M \) is a free module. Let \( \{ \tilde{e}_1, \ldots, \tilde{e}_k \} \) be a basis of \( M/M \cap N \) and \( \{ f_1, \ldots, f_p \} \) be a basis of \( M \cap N \). May take \( e_1 \in \tilde{e}_1, \ldots, e_k \in \tilde{e}_k \). We would like to show that \( \{ e_1, \ldots, e_k, f_1, \ldots, f_p \} \) forms a basis of \( M \).

\[
\forall x \in M, x \in \tilde{x} \in M/M \cap N, x = n_1 \tilde{e}_1 + \cdots + n_k \tilde{e}_k \in M/M \cap N. \ \text{Therefore, } x - (n_1 e_1 + \cdots + n_k e_k) = 0, \ \text{i.e., } x - (n_1 e_1 + \cdots + n_k e_k) \in M \cap N. \ \text{Since } \{ f_1, \ldots, f_p \} \text{ is a basis of } M \cap N, \text{there exists } m_1, \ldots, m_p \text{ such that } x - (n_1 e_1 + \cdots + n_k e_k) = (m_1 f_1 + \cdots + m_p f_p). \ \text{Hence, } \{ e_1, \ldots, e_k, f_1, \ldots, f_p \} \text{ spans } M \text{ for } x = n_1 e_1 + \cdots + n_k e_k + m_1 f_1 + \cdots + m_p f_p. \]

While \( n_1 e_1 + \cdots + n_k e_k + m_1 f_1 + \cdots + m_p f_p = 0 \), i.e., in \( M/M \cap N, n_1 e_1 + \cdots + n_k e_k + m_1 f_1 + \cdots + m_p f_p = 0 \) if \( n_1 = \cdots = n_k = 0 \) since \( \{ e_1, \ldots, e_k \} \) is a basis of \( M \cap N \). Then, because \( m_1 f_1 + \cdots + m_p f_p = 0 \) in \( M \cap N \), we can know that \( m_1 = \cdots = m_p = 0 \).

Therefore, \( M \) is a free module of rank less than or equal to \( n \).

**From \( GL_n(\mathbb{Z}) \) to \( GL_n(\mathbb{O}_K) \)**

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

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

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

We make the convention of the sum \( \sum_{i=1}^{0} = 0 \).

Apparently, we can know that \( \Gamma \) is an \( \mathbb{O}_K \)-module. Then, we are going to show that there exists \( d \in \mathbb{O}_K \) such that \( \mathbb{O}_K^n \subset \Gamma \subset \mathbb{O}_K^n \). Furthermore, we can deduce that \( \Gamma \) is a free \( \mathbb{O}_K \)-module of rank \( n \). In fact, \( \forall x \in \mathbb{O}_K^n \), let \( g_1 = 1, x_i = x \) for any positive integer \( i \), then \( x = g_1 x_i \in \Gamma \), which means \( \mathbb{O}_K^n \subset \Gamma \).

Since \( G \) is a finite subgroup of \( GL_n(\mathbb{Z}) \), there are finite elements in \( G \). For \( \mathbb{O}_K \) is the ring of integers in \( K \), \( K \) is the fraction field of \( \mathbb{O}_K \). Let \( d \) be the least common multiple of the denominators of entries in \( G \) whose existence is guaranteed by the fact that \( \mathbb{O}_K \) is a principal ideal domain and thus a unique factorization domain. \( \forall x \in \Gamma, x = \sum_{i=1}^{m} g_i x_i \) where \( g_i \in G, x_i \in \mathbb{O}_K^n \) and \( m \in \mathbb{N} \). Since the entries of \( g_i \) are in \( \mathbb{Z} \mathbb{O}_K^n \), we conclude that \( x \in \mathbb{Z} \mathbb{O}_K^n \). That is to say, \( \Gamma \subset \mathbb{Z} \mathbb{O}_K^n \).

Since \( \Gamma \) is a submodule of \( \mathbb{Z} \mathbb{O}_K^n \), \( \Gamma \) is a free \( \mathbb{O}_K \)-module of rank less than or equal to \( n \). Since \( \mathbb{O}_K^n \) is a submodule of \( \Gamma \), \( \mathbb{O}_K^n \) is of rank \( n \) less than or equal to the rank of \( \Gamma \). Then, \( \Gamma \) is a free \( \mathbb{O}_K \)-module of rank \( n \).

Therefore, there exists an \( \mathbb{O}_K \)-basis of \( \Gamma \), namely, \( \{ e_1, \ldots, e_n \} \). Write every \( e_i \) in the coordinate form:

\[
e_1 = [a_{11} a_{21} \cdots a_{n1}]
\]

\[
e_k = [a_{1k} a_{2k} \cdots a_{nk}]
\]

\[
e_n = [a_{1n} a_{2n} \cdots a_{nn}]
\]

where each entry is an element in \( K \). Then, we can define a matrix \( Q \):
Then, \( g \in G \) is invertible if and only if \( g \) is a bijection. If \( g \) is injective, then \( g \) is termed an injective homomorphism. Conversely, for any \( x, y \in \mathbb{Z} \), there exists a unique \( g \in G \) such that \( g(x) = y \), which is to say, \( G \) is bijective since \( \ker g = \{1\} \).

\[ Q = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \]

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 \( Q^{-1} g Q \in GL_n(O_K) \) so that we can deduce that \( G \) is isomorphic to a subgroup of \( GL_n(O_K) \).

**3.1.8. Lemma.** For any \( g \in G \), \( Q^{-1} g Q \) is an invertible map from \( O_K^n \) to \( O_K^n \).

**Proof:** Let \( \{v_1, \ldots, v_n\} \) be the canonical basis of \( O_K^n \) and \( \{e_1, \ldots, e_n\} \) be a basis of \( \mathbb{Z} \). We can understand \( Q \) as a map from \( O_K^n \) to \( : \{v_1, \ldots, v_n\} \mapsto \{e_1, \ldots, e_n\} \).

**Surjectivity:** \( \forall x \in \mathbb{Z} \), \( \exists s_1, \ldots, s_n \in \mathbb{Z} \) such that \( x = s_1 e_1 + \cdots + s_n e_n = s_1 v_1 + \cdots + s_n v_n = Q(s_1 v_1 + \cdots + s_n v_n) \). Therefore, \( Q \) is bijective. Similarly, we can consider the matrix \( g \in G \) as a map from \( \Gamma \) to \( : \{e_1, \ldots, e_n\} \mapsto \{ge_1, \ldots, ge_n\} \). Obviously, \( g \) is bijective since \( g \) is an invertible matrix whose inverse is also a map from \( \Gamma \) to \( \Gamma \). Then, for any \( x \in O_K^n, Q^{-1} g Q x \) is in \( O_K^n \), which means that \( Q^{-1} g Q \) is a map from \( O_K^n \) to \( O_K^n \). Therefore, \( Q^{-1} g Q \) is invertible since it is bijective. Then, \( Q^{-1} g Q \) is in \( GL_n(O_K) \).

We are ready to prove that \( G \) is isomorphic to a subgroup of \( GL_n(O_K) \). Define a map \( \varphi \) from \( G \) to \( GL_n(O_K) \): \( g \mapsto Q^{-1} g Q \). We will prove that \( \varphi \) gives an isomorphism of \( G \) to a subgroup of \( GL_n(O_K) \): \( \phi \).

**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 \( \ker \phi \). Since \( \phi(x) = Q^{-1} x Q = 1 \), we can know that \( I = QIQ^{-1} = QQ^{-1} x QQ^{-1} = x \), which is to say, \( \ker \phi = \{1\} \), i.e., \( \phi \) is injective.

Hence, \( G \) is isomorphic to the image of \( \varphi \) as groups. Therefore, in this subsection, we have proven the following theorem:

**3.1.9. Theorem.** Let \( n \) be a positive integer and \( K \) be an algebraic number field whose ring of integers \( O_K \) is a principal ideal domain. Then, any finite subgroup of \( GL_n(K) \) is isomorphic to a finite subgroup of \( GL_n(O_K) \).

**Finite Subgroups of \( GL_n(O_K) \)**

In this subsection, we are going to prove that, up to isomorphism, there are only finitely many finite subgroups in \( GL_n(O_K) \).

First of all, we define a set of prime numbers:

\[ E = \{ p : p \text{ is a prime number and is the order of an element in } GL_n(O_K) \} \cup \{2\} \]

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 2.2.3 Corollary, we can see that \( E \) is a finite set. This is an important fact that we will use continuously in what follows.

Now let \( p \notin E \) be a non-exceptional prime number and \( x \) be a prime factor of \( p \) in \( O_K \). Let us recall the general definition of prime elements: Let \( A \) be a commutative ring. \( x \in A \) is called a prime element in \( A \), if for any \( y_1, y_2 \in A \), \( y_1 \sim 1 \) or \( y_2 \sim x \). Here \( \sim \) means \( a \) is equal to \( b \) up to an invertible element. The definition of prime elements is a generalization of prime numbers in integers.
3.1.10. Lemma. \( O_K/(x) \) is a finite field.

Proof: \( O_K/(x) \) is a field since \( x \) is a prime element in \( O_K \). We can define a map:\
\[
\phi: \mathbb{Z} \hookrightarrow O_K \twoheadrightarrow O_K/(x).
\]
Clearly, since \( \ker \phi = p\mathbb{Z} \), \( \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker \phi \cong O_K/(x) \). Therefore, \( O_K/(x) \) is an extension of \( F_p \). As a well-known fact, \( O_K \) is a free \( \mathbb{Z} \) - module of finite rank \( [K: \mathbb{Q}] \) (c.f. [4, p.45]). Then, let \( \{e_1, \cdots, e_n\} \) be a \( \mathbb{Z} \) basis of \( O_K \). For any \( x \in O_K \), we can write \( x = \sum \lambda_i e_i \) where \( \lambda_i \in \mathbb{Z} \). Hence, \( x = \sum \lambda_i e_i \in O_K/(x) \) where \( \lambda_i \in \mathbb{Z}/\mathbb{Z} \cap (x) = \mathbb{Z}/p\mathbb{Z} \). So, \( O_K/(x) \) can be spanned by \( \{\bar{e}_1, \cdots, \bar{e}_n\} \) as the vector space of \( \mathbb{Z}/p\mathbb{Z} \). The dimension of \( O_K/(x) \) is no bigger than \( n \) over \( F_p \), which implies that \( O_K/(x) \) is a finite field.

Now, we can define a group homomorphism:\
\[
\tau_x: GL_n(O_K) \rightarrow GL_n(O_K/(x))
\]
by modulo \( x \) for each entry. This homomorphism has the following interesting property:

3.1.11. Proposition. For \( g \in \ker \tau_x \) and a positive integer \( l \) 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 \( x \) divides all entries of \( h \). It suffices to prove the proposition for \( l \) a prime number. In fact, for \( l \geq 2 \), \( l = p_1 \cdots p_r \), and \( g' \) is defined to be \( g^{p_1 \cdots p_{r-1}} \). Then, \( g' \equiv 1^{p_1 \cdots p_{r-1}} = 1 \mod x \). Since \( g^{p_r} \equiv g^l \equiv 1 \mod x \), we can know that \( g^l = 1 \) 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 \( x dh' \) where \( d \in O_K \) and \( h' \in M_n(O_K) \) such that the greatest common divisor of entries of \( h' \) is 1.

\[
g^l = (1 + h)^l = (1 + xdh')^l = (xdh')^l + \binom{l}{1}(xdh')^{l-1} + \cdots + lxdh' + 1.
\]

By \( g^l = 1 \), we can know that
\[
(xdh')^l + \binom{l}{1}(xdh')^{l-1} + \cdots + lxdh' = 0.
\]

Since \( O_K \) is a domain,
\[
(xd)^{-1}h^l + \binom{l}{1}(xd)^{-2}h'^{-1} + \cdots + lh' = 0.
\]

Then, from the fact that \( x \) divides \( (xd)^{l-1}h^l + \binom{l}{1}(xd)^{l-2}h'^{-1} + \cdots + \binom{l}{2}xh'^2 \) we conclude that \( x|lh' \). Therefore, \( x|l \) in \( O_K \), since the greatest common divisor of entries of \( h \) is 1. Because \( x \) divides \( p, l \) are not coprime in \( O_K \), which implies 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, \( h = 0 \), which is to say, \( g = 1 \).

3.1.12. Theorem. Let \( x \) be a prime factor of non-exceptional prime number \( p \) in \( O_K \). For any finite subgroup \( G \subset GL_n(O_K) \),
\[
\tau_x: GL_n(O_K) \rightarrow GL_n(O_K/(x))
\]
gives an isomorphism of \( G \) to a subgroup of \( GL_n(O_K/(x)) \).

Proof: We define a map \( \phi: G \rightarrow GL_n(O_K/(x)) \) by modulo \( x \) for each entry. We are going to show that \( \phi \) gives an isomorphism of \( G \) to the image of \( \phi \). Apparently, \( \phi \) is a group homomorphism. It suffices to show \( \phi \) is injective. For any \( g \in \ker \phi \), there exists a positive integer \( m \) such that \( g^m = 1 \). From our choice of \( p \), \( p \) does not divide \( m \). Since \( \ker \phi = \ker \tau_x \cap G \), by the preceding
proposition, \( g = 1 \). This proves the injectivity of \( \phi \). Hence, \( \phi \) gives an isomorphism of \( G \) to the image of \( \phi \).

From this theorem, we conclude that any finite subgroup of \( GL_n(O_K) \) is isomorphic to a subgroup of \( GL_n(O_K/(x)) \), whereas the latter, being a finite group since \( O_K/(x) \) 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:

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

4. **A Multiplicative Bound for the Orders 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 a multiplicative bound for the orders of finite 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 a multiplicative bound and apply it to special cases.

4.1. **Preliminaries**

In this subsection, we will present some tools and theorems that will be used in calculating the multiplicative bound.

**Definition 4.1.1.** Let \( A \) be a finite set of positive integers. A multiplicative bound of \( A \) is a positive integer \( M \) such that each element of \( A \) divides \( M \). In this case, \( A \) is the set of orders of finite subgroups of \( GL_n(O_K) \).

4.1.1. **Lemma.** Let \( \mathbb{F}_q \) be a finite field with \( q \) elements and \( n \) be a positive integer. Then there are \( \frac{q^n(q^n-1)}{2} \cdots (q-1) \) 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 \((0, \cdots, 0)\), 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 \( (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\cdots(q-1) \) choices of invertible matrices.

4.1.2. **Lemma.** Let \( \ell \) 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, we notice that \( \mathbb{Z}/\ell^2\mathbb{Z}^\times \) is cyclic since \( \mathbb{Z}/\ell\mathbb{Z} \) is a finite field. We can find an integer \( x' \) such that the order of \( x' \) modulo \( \ell \) is \( \ell - 1 \). The order of \( x' \) modulo \( \ell^2 \) 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 \( \ell^2 \). Then, we find that \( y = 1 + \ell \) is of order \( \ell \) modulo \( \ell^2 \) by noticing the following congruence equation:

\[
(1 + \ell)^x \equiv 1 + k\ell \pmod{\ell^2}.
\]

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

4.1.3. **Theorem** (Dirichlet’s arithmetic progression) Let \( m, n \) be two coprime integers and \( m > 0 \). Then there are infinitely 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].

4.1.4. **Theorem** (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
\[ x \equiv a \mod m, x \equiv b \mod n \]

Such \( x \) is unique modulo \( mn \).

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

\[ \Phi: \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \]

\[ x \mapsto (x \mod m, x \mod n) \]

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

### 4.2. General Method to Calculate the Multiplicative Bound

Let \( G \subseteq GL_n(K) \) be a finite group. Let \( p > 2 \) be a prime number and \( x \in O_K \) be a prime factor of \( p \) in \( O_K \). Since the characteristic of \( O_K/(x) \) is \( p \), \( O_K/(x) \) is isomorphic to \( \mathbb{F}_{p^r} \) for some \( r \geq 1 \). To make the notation pithy, we write \( \mathbb{F}_{p^r} \) as \( \mathbb{F}_p \). Aside from finitely many exceptional prime numbers \( p, G \) can be viewed as a subgroup of \( GL_n(O_K/(x)) \), i.e., \( GL_n(\mathbb{F}_p) \). (2.2.2 Corollary and 3.3.3 Theorem)

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

\[ |GL_n(\mathbb{F}_p)| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1), \]

By Fermat’s little theorem, \( p^{\ell^2 - 1} - 1 \equiv 0 \mod \ell \), so \( \ell \) is certainly a factor of \( |GL_n(\mathbb{F}_p)| \) as \( n \) becomes large. However, we do not know clearly the power of \( \ell \) and we want it to be as small as possible. Then we consider what the power of \( \ell^2 \) is in \( |GL_n(\mathbb{F}_p)| \). As we know from 4.1.2. Lemma above, \( (\mathbb{Z}/\ell^2\mathbb{Z})^n \) is a cyclic group, which is to say, there exists an \( x \in \mathbb{Z} \) such that \( \text{Ord}_{\ell^2}(p) = \ell(\ell - 1) \). Then, we define \( x \) in this way and as long as \( p \equiv x \mod \ell^2 \), \( p \) satisfies \( \text{Ord}_{\ell^2}(p) = \ell(\ell - 1) \). According to Dirichlet’s arithmetic progression [6], there are infinitely many prime numbers in \( \{k\ell^2 + x\} \), while there are only finitely many exceptions which \( p \) cannot be chosen from, then we can find a prime number \( p = k\ell^2 + x \) such that \( \text{Ord}_{\ell^2}(p) = \ell(\ell - 1) \).

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

\[ v_\ell(p^k - 1) = \begin{cases} 1 + v_\ell(k) & \text{if } \ell - 1 \mid k \\ 0 & \text{if } \ell - 1 \nmid k \end{cases} \]

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

\[ v_\ell([GL_n(\mathbb{F}_p)]) = \sum_{k=1}^{n} v_\ell(p^{rk} - 1) \]

\[ = \sum_{d=1}^{\left\lfloor \frac{m}{\ell - 1} \right\rfloor} v_\ell(p^{r \left\lfloor \frac{\ell - 1}{m} \right\rfloor} - 1) \]

\[ = \left\lfloor \frac{mn}{\ell - 1} \right\rfloor + \sum_{d=1}^{\left\lfloor \frac{m}{\ell - 1} \right\rfloor} v_\ell(rd \left\lfloor \frac{\ell - 1}{m} \right\rfloor) \]

\[ = \left\lfloor \frac{mn}{\ell - 1} \right\rfloor (1 + v_\ell(r)) + \sum_{d=1}^{\left\lfloor \frac{m}{\ell - 1} \right\rfloor} v_\ell(d) \]
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 \( p^k = (2^e x + 1)^k = 1 + k 2^e x + \binom{k}{2}(2^e x)^2 + \cdots + (2^e x)^k \).

We classify the possible values of \( e \) into two parts:

- When \( e > 1 \), \( v_\ell(p^k - 1) = v_\ell(k) + e \). To make \( e \) as small as possible, we consider \( e = 2 \), which means \( p \equiv 5 \) by modulo 8. Therefore, \( \sum_{k=1}^{n} v_\ell(p^k - 1) = \sum_{k=1}^{n} (2 + v_\ell(rk)) = n(2 + v_\ell(r)) + v_\ell(n!) \).

- When \( e = 1 \), i.e., \( p \equiv 3 \) by modulo 4, we can know that \( v_\ell(p^k - 1) = v_\ell(2kx + 2(k - 1)x^2) = v_\ell(2kx(1 + (k - 1)x)) = v_\ell(k) + v_\ell(1 + (k - 1)x) \). To avoid possible explosion of \( v_\ell(1 + (k - 1)x) \) as \( k \) varies, we can take \( p \) as small as we can. Take \( p = 3 \) when \( 3 \) is not in the exceptions, then \( v_\ell(3^k - 1) = 1 + 2v_\ell(3) \).

Therefore, we can get the minimum possible value of \( GL_n(\mathbb{F}_p^r) \):

\[
\sum_{k=1}^{n} v_\ell(3^r - 1) = \sum_{k=1}^{n}(1 + 2v_\ell(r)) = n(1 + 2v_\ell(r)) + 2v_\ell(n!)
\]

4.3. Some Examples

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

4.3.1. 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 \( v_\ell(r) \) in the calculation of \( |GL_n(\mathbb{F}_p)| \), we want the value of \( r \) as small as possible. We hope that \( r = 1 \), i.e., \( \mathbb{Z}[\sqrt{-1}]/(x) \equiv \mathbb{F}_p \) where \( x \) is a prime element in \( \mathbb{Z}[\sqrt{-1}] \) that divides \( p \). When can this happen?

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

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 \( a = 0, \cdots, p - 1 \). Let \( e = g + hi = a + di \) 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 \( s = 0, \cdots, p - 1 \). Then, we make \( s \) equal to \( a + mp \) where \( m \in \mathbb{Z} \) and \( a = 0, \cdots, p - 1 \). Since \( x = x \), we know that \( M + Ni = (g + hi)(c + di) + a + mxh = x(g + hi + mx) + a \). Thus, we represent \( M + Ni \) as \( kx + a \) for some \( k \in \mathbb{Z}[\sqrt{-1}] \) and \( a \in \{0, \cdots, p - 1\} \). 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 multiplicative 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 \( p \equiv 1 \mod 4 \) which is not an exception. In this case, \( r = m = 1 \) in the formula of \( v_\ell(|GL_n(\mathbb{F}_p^r)|) \). For \( r > 3 \), we find that \( \frac{mn}{\ell - 1} = 0 \), and thus

\[
|GL_n(\mathbb{F}_p)| \leq v_\ell(|GL_n(\mathbb{F}_p^r)|) = \frac{mn}{\ell - 1} (1 + v_\ell(r)) + v_\ell\left(\frac{mn}{\ell - 1}!\right) = 0
\]

For \( r = 3, 4 \), we find

\[
|GL_n(\mathbb{F}_p)| \leq v_\ell(|GL_n(\mathbb{F}_p^r)|) = \frac{mn}{\ell - 1} (1 + v_\ell(r)) + v_\ell\left(\frac{mn}{\ell - 1}!\right) = 1 \times (1 + 0) + 0 = 1.
\]

For \( r = 2 \), by taking a prime number \( p \equiv 5 \mod 8 \) which is not an exception and by utilizing the formula of the preceding part, we find

\[
v_\ell(|GL_n(\mathbb{F}_p^r)|) = \frac{mn}{\ell - 1} (1 + v_\ell(r)) + v_\ell\left(\frac{mn}{\ell - 1}!\right) = 1 	imes (1 + 0) + 0 = 1.
\]
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 $p \equiv 1 \mod 4$ which is not an exception. In this case, $r = m = 1$ in the formula of $v_\ell(\left|GL_n(F_{p^r})\right|)$. For $\ell > 3$, we find that $\frac{mn}{\ell-1} = 0$, and thus

$$v_\ell(\left|G\right|) \leq v_\ell(\left|GL_n(F_{p^r})\right|) = \left\lfloor \frac{mn}{\ell-1} \right\rfloor (1 + v_\ell(r)) + v_\ell(\left\lfloor \frac{mn}{\ell-1} \right\rfloor!) = 0$$

For $\ell = 3$, we find that

$$v_3(\left|G\right|) \leq v_3(\left|GL_n(F_{p^r})\right|) = \left\lfloor \frac{mn}{3-1} \right\rfloor (1 + v_3(r)) + v_3(\left\lfloor \frac{mn}{3-1} \right\rfloor!) = 1 \times (1 + 0) + 0 = 1.$$  

For $\ell = 2$, if $y$ taking a prime number $p \equiv 5 \mod 8$ which is not an exception and by utilizing the formula of the preceding part, we find

$$v_2(\left|G\right|) \leq n(2 + v_2(r)) + v_2(n!) = 3 \times 2 + 1 = 7.$$  

Taking account of all the calculations above, we conclude that $|G|$ divides $2^7 \times 3^1 = 384$.

4.3.3. Example. $K = \mathbb{Q}[\sqrt{-2}]$, then $O_K = \mathbb{Z}[\sqrt{-2}]$. 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 $p \equiv 1, 3 \mod 8$.

We now use the result of the preceding section to give multiplicative bounds of finite subgroups of $GL_n(O_K)$ for $n = 2$. Let $G$ be a finite subgroup of $GL_n(K)$. Let $x \in O_K$ such that $O_{rd_{G}x} = \ell (\ell - 1)$. We take a prime number $p \equiv 1, 3 \mod 8$ by modulo 8 and $p \equiv x \mod \ell^2$ which is not an exception. In this case, $r = m = 1$ in the formula of $v_\ell(\left|GL_n(F_{p^r})\right|)$. For $\ell > 3$, we find that $\frac{mn}{\ell-1} = 0$, and thus

$$v_\ell(\left|G\right|) \leq v_\ell(\left|GL_n(F_{p^r})\right|) = \left\lfloor \frac{mn}{\ell-1} \right\rfloor (1 + v_\ell(r)) + v_\ell(\left\lfloor \frac{mn}{\ell-1} \right\rfloor!) = 0$$

For $\ell = 3$, we find

$$v_3(\left|G\right|) \leq v_3(\left|GL_n(F_{p^r})\right|) = \left\lfloor \frac{mn}{3-1} \right\rfloor (1 + v_3(r)) + v_3(\left\lfloor \frac{mn}{3-1} \right\rfloor!) = 1 \times (1 + 0) + 0 = 1.$$  

For $\ell = 2$, since $p \equiv 1, 3 \mod 8$, we take $p \equiv 3 \mod 4$ in this case. To avoid possible explosion of $v_2(1 + (k - 1)x)$ 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 $GL_2(K)$, while the elements in $GL_2(K)$ have 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 $v_2(11^k - 1) = v_2(k) + 1 + v_2(5k - 4)$. Hence,

$$v_2(\left|G\right|) \leq v_2(\left|GL_n(F_{11})\right|) = \sum_{k=1}^{n} (1 + v_2(k) + v_2(5k - 4)) = n + v_2(n!) + \sum_{k=1}^{n} v_2(5k - 4) = 4.$$  

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

5. Conclusion

For a given positive integer $n$, it is well-known that, up to isomorphism, there are finitely many finite subgroups of $GL_n(\mathbb{Q})$. This result is generalized to any algebraic number filed by Schur. In this article, by a series of isomorphisms, we propose another proof of Schur’s result when the ring of integers in $K$ is a principal ideal domain, without using the character theory of finite groups. Then, we give a general method to calculate an upper bound for the order of finite subgroups of $GL_n(K)$, for a given $n$ and a given algebraic number field $K$. We also give examples of $GL_2(\mathbb{Q}[\sqrt{-1}])$, $GL_3(\mathbb{Q}[\sqrt{-1}])$ and $GL_2(\mathbb{Q}[\sqrt{-2}])$ to show how sharp the upper bound is.
Moreover, we give a general method to classify finite cyclic subgroups of $\text{GL}_n(K)$, where $K$ is an algebraic number field, by considering the irreducible decomposition of $n$-th cyclotomic polynomial $\Phi_n(X)$ in $K[X]$ where $K$ is an algebraic number field. To specify, we classify finite cyclic subgroups for $\text{GL}_2(\mathbb{Q}[\sqrt{-1}])$, $\text{GL}_3(\mathbb{Q}[\sqrt{-1}])$, $\text{GL}_2(\mathbb{Q}[\sqrt{-2}])$ and $\text{GL}_3(\mathbb{Q}[\sqrt{-2}])$ as examples.

6. References

[1] P. M. Gudivok, A. A. Kiriyuk, V. P. Rudko, and A. I. Tsitkin, Finite Subgroups of the Group $\text{GL}(n, \mathbb{Z})$, Translated from Kibernetika, No. 6, pp. 71-82, November-December, 1982. Original article submitted June 30, 1982.

[2] G. Mackiw, Finite Groups of $2 \times 2$ Integers Matrices, Mathematics Magazine, Vol. 69, No. 05, Dec. 1996.

[3] H. Minkowski, Zur Theorie der positiven quadratischen Formen, J. Crelle 101 (1887), 196–202.

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

[5] I. Schur, Über eine Klasse von endlichen Gruppen linearer Substitutionen, Sitz. Preuss. Akad. Wiss. Berlin (1905), 77–91.

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

[7] S. H. Weintraub, Galois Theory, 2009, Springer-Verlag New York.