FINITE GROUPS OCCURRING AS GROUPS OF INTEGER MATRICES

- Papia Bera

IISER Pune

In this project, we study groups of matrices. In particular, we try and determine the possible orders of matrices of finite order in the group $GL(n,\mathbb{Z})$, the group of $n \times n$ matrices with determinant ± 1. We prove certain results due to Minkowski regarding the torsion of the groups $GL(n,\mathbb{Z})$ and $GL(n,\mathbb{Q})$. We then proceed to determine the possible order of elements in these groups.

I would like to express my gratitude to my project guide Prof. B. Sury, for giving me this opportunity to work with him under the IAS Summer Research fellowship. His patience and help was greatly appreciated and added to my experience.

I recognize that this project would not have been possible without the Indian Academy of Sciences and thank them for granting me this fellowship.

Lastly, this project would not have even begun without the motivation provided by my college, the Indian Institute of Science Education and Research, Pune and its faculty, especially Prof. A. Raghuram who wholeheartedly supports any such research endeavors taken by his students.

INTRODUCTION –

The role of group theory is immensely central not only to mathematics but also in other sciences viz. physics, chemistry etc. Whenever there is symmetry, often there is a group in the background. Historically, study of groups started as permutations of finitely many objects, however at a later stage this contributed to the development of an abstract theory beyond the groups of finite numbers. As such, analyzing an abstract group in diverse ways as a group of matrices (representation theory) threw light in various fields of science – the representation theory plays crucial role in quantum mechanics, number theory etc., even Langland's conjecture is stated in the language of representation theory.

In our present report we have dealt with finite groups represented as matrices whose entries are integers. Under this project titled ``Finite groups occurring as groups of integer matrices", we study finite subgroups of $GL(n, Z)$, the group of all invertible matrices which have integer entries and whose inverses also have integer entries.

One of the famous classical theorems due to Minkowski tells us that, infinite groups like the group $GL(n, Z)$ admits only finitely many possibilities of finite order for elements or subgroups of the group. This leads us to investigate the nature of these possible orders and how they might vary with n. Due to the fact that there exists a finite number of them, therefore there must exist some maximal possible finite order of subgroups.

We start by recollecting the basics of group theory.

Lagrange's theorem **[4]**:

If a finite group G has a subgroup H, then the order of the subgroup H is a divisor of the order of G.

A map $\phi : G \to H$ is said to be a homomorphism from the group $(G,*)$ to the group $(H,\oplus)$, if and only if, $\phi(x * y) = \phi(x) \oplus \phi(y)$. If a homomorphism ϕ is a bijection (one-one and onto), it is said to be an isomorphism. The image of a homomorphism to H is a subgroup of Hand the kernel of a homomorphism (the elements mapping to the identity element) from a group G is a normal subgroup of G.

Under group isomorphisms, group-theoretic properties are preserved.

A group homomorphism from a group G to a group H which is one-one makes it possible to identify G isomorphically with a subgroup of H. In particular, the following result shows that every finite group can be regarded as a group of permutations.

Cayley's Theorem [4]:

Every group of order n is isomorphic to a subgroup of the group of permutations or the group S_n.

Let us now look at groups of matrices under matrix multiplication.

The group $GL(n,\mathbb{R})$ is the set of all matrices with real number entries and non-zero determinant, considered under the operation of matrix multiplication. All elements of the group have inverses under multiplication since they are all invertible and the identity under multiplication is the identity matrix I_n. Similarly, the group $GL(n,\mathbb{Q})$ is the group of all matrices with rational entries and non-zero determinant.

One defines the group $GL(n,\mathbb{Z})$ to be the group of all matrices with integer entries and determinant 1 or -1. Note that each matrix in this set has an inverse which is also an integer matrix. In fact, an integral matrix has an inverse matrix which also has integer entries if and only if, the determinant of the matrix is ±1. If an integer matrix A has an inverse matrix B, then the determinants of A and of B are integers whose product is 1; this implies that the determinant must be 1 or -1. Conversely, if the determinant of an integer matrix is 1 or -1, the inverse of a matrix A is given by dividing all the entries of its adjoint matrix by the determinant of A.

$$A^{-1} = \frac{1}{|A|} adj(A)$$

Note that the adjoint matrix of A, if A has integer entries, will also have integer entries.

Now we can prove that any finite group can be regarded as a subgroup of $GL(n,\mathbb{Z})$ for some n.

Theorem:

Any group of order n is isomorphic to a subgroup of $GL(n,\mathbb{Z})$*, for the same n.*

PROOF :

Cayley's Theorem states that any finite group G of order n can be embedded in the group S_n. Thus, to show that the group G embeds in the group $GL(n,\mathbb{Z})$, it is sufficient to show that S_n embeds in the group $GL(n,\mathbb{Z})$.

Consider any permutation $\sigma \in S_n$. Let $T_\sigma : \mathbb{Q}^n \to \mathbb{Q}^n$ be the linear transformation defined by $T_\sigma(e_i) = e_{\sigma(i)}$ where $\mathrm{B} = \{e_1, e_2, \cdots, e_n\}$ is the canonical basis for $\mathbb{Q}^n$.

We define a map, $\Phi : S_n \to GL(n,\mathbb{Z})$ by sending $\sigma \in S_n$ to the matrix corresponding to the transformation T_σ with respect to the basis set B.

We observe that the transformation matrix of each of these T_σ is a matrix where each entry is either 0 or 1 and with exactly one non-zero entry in each row and column. Such matrices are called permutation matrices and the set of all such matrices is denoted by P_n . We also observe that, $P_n = \Phi(S_n)$.

The matrix T_σ has determinant equal to the signature of the corresponding permutation.

We see that Φ is a homomorphism as it respects the corresponding operations – the composition of permutations and the multiplication of matrices.

We observe now that this is one-one.
Consider for a given $\sigma_1 , \sigma_2 \in S_n$, $T_{\sigma_1}(e_i) = T_{\sigma_2}(e_i) \; \forall \; i = 1,2,\ldots,n$,
$\Rightarrow e_{(\sigma_1(i))} = e_{(\sigma_2(i))} \; \forall \; i = 1,2,\ldots,n$, $\because e_i = e_j$ iff $i = j \Rightarrow \sigma_1(i) = \sigma_2(i) \; \forall \; i = 1,2,\ldots,n$
Thus, $\sigma_1 = \sigma_2$ and, $\Phi : S_n \to GL(n,\mathbb{Z})$ is a **one-one homomorphism**.

Therefore, S_n is embedded in the group $GL(n,\mathbb{Z})$. By Cayley's theorem, we know that the group G is embedded in S_n .

Thus, the group G of order n is embedded in the group $GL(n,\mathbb{Z})$ or in other words, G is isomorphic to a subgroup of $GL(n,\mathbb{Z})$.

This completes the proof.

Orders of finite subgroups of $GL(n,\mathbb{Z})$:

We now observe that, in the group $GL(n,\mathbb{Z})$, for any given n , there will always exist a subgroup of order n and also a subgroup of order $n!$ such as S_n . In fact, we will observe the surprising fact that there may also exist subgroups of order greater than n! (!)

For example –

Let C_n be a subgroup of $GL(n,\mathbb{Z})$ consisting of all diagonal matrices with ± 1 diagonal entries.

Then, $C_n \cong \underbrace{Z_2 \times Z_2 \times \cdots \times Z_2}_{n}$. Let $B_n = C_n P_n$.

Here, and elsewhere,
Let $A_1, A_2 \in B_n \Rightarrow A_i = X_i Y_i$ where $X_i \in C_n$ and $Y_i \in P_n$ and $i = 1,2$.

$A_1 \oplus A_2 = A_1 A_2 = X_1 Y_1 X_2 Y_2 = X_1 X_2 Y_1 Y_2$. $[\because Y_1 \in P_n \Rightarrow Y_1 A = A Y_1 \; \forall \; A \in GL(n,\mathbb{Z})]$

$X_1 X_2 \in C_n$ and $Y_1 Y_2 \in P_n \Rightarrow X_1 X_2 Y_1 Y_2 \in B_n$, $A_1 \oplus A_2 \in B_n$

Let $A_1 \in B_n, \exists\, A_1^{-1} \in GL(n,\mathbb{Z})$ s.t. $A_1 A_1^{-1} = I$.
$\because A_1 \in B_n \Rightarrow A_1 = X_1 Y_1$ s.t. $X_1 \in C_n$ and $Y_1 \in P_n$
$\Rightarrow A_1^{-1} = Y_1^{-1} X_1^{-1} = X_1^{-1} Y_1^{-1} \left[\because Y_1^{-1} \in P_n \Rightarrow Y_1^{-1} A = A Y_1^{-1}\ \forall\, A \in GL(n,\mathbb{Z})\right]$
where $X_1^{-1} \in C_n$ and $Y_1^{-1} \in P_n$, $\therefore\ A_1^{-1} \in B_n$

$I \in C_n$ and $I \in P_n \Rightarrow I.I = I \in B_n$

Thus, B_n is closed over addition, contains the inverse of each of its elements and also contains the identity element. Therefore B_n is a subgroup of $GL(n,\mathbb{Z})$.

From the previous proof, we can see that, $P_n \cong S_n$. $\therefore |P_n| = |S_n| = n!$. Also,

$\because C_n \cong \underbrace{Z_2 \times Z_2 \times \cdots \times Z_2}_{n} \Rightarrow |C_n| = 2^n$. Thus, the cardinality of B_n is determined by the product of $|P_n|$ and $|C_n|$. $\Rightarrow |B_n| = |C_n||P_n| = 2^n n!$.

Thus, there exists a subgroup B_n of $GL(n,\mathbb{Z})$ with order $2^n n!$.

Structure of finitely generated abelian groups

A group G is said to be abelian if the group operation is also commutative on all elements of the group.

An abelian group G is said to be a finitely generated abelian group if there exists a finite subset A of G such that the smallest subgroup of G containing A is the whole of G; we write $G = \langle A \rangle$. This means that every element of G is a finite, integer linear combinarion of elements of A (here, we write the operation on G additively).

Fundamental Theorem of finitely generated Abelian groups **[2]*:***

Let G be a finitely generated Abelian group. Then,

1. $G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$, for some integers $r, n_1, n_2, \ldots, n_s$ satisfying the following conditions –
   a. $r \geq 0$ and $n_j \geq 2$ for all j
   b. n_{i+1} divides n_i , $1 \leq i \leq s-1$
2. The expression in (1) is unique given the conditions (a) and (b).

An abelian group G is said to be free abelian of rank n if $G \cong Z^n$, the group of all n-tuples of integers under the operation of adding entry-wise. For convenience in working with matrices, we will regard Z^n as column vectors with integer entries. The Fundamental Theorem of Finitely generated Abelian Groups implies that an abelian group is free abelian if it is a finitely generated abelian group with no nontrivial elements of finite order. It also implies that any subgroup of a free abelian group is free with rank less than or equal to n.

The next theorem proves the surprising fact that finite subgroups of $GL(n,Q)$ are essentially already subgroups of $GL(n,Z)$. More precisely, we prove:

Theorem* [1] *:

If G is a finite subgroup of $GL(n,Q)$, then G is conjugate to a subgroup of $GL(n,Z)$.

PROOF :

G is a finite subgroup of $GL(n,Q)$ and $|G| = k$

Let $F = \sum_{g \in G} g(Z^n) = \left\{ \sum_{i=1}^{k} g_i v_i \mid g_r \neq g_s \forall r \neq s, g_i \in G, v_i \in Z^n \right\}$

$$g(F) = \left\{ g \sum_{i=1}^{k} g_i v_i \mid g_r \neq g_s \forall r \neq s, g, g_i \in G, v_i \in Z^n \right\}$$

$$g(F) = \left\{ \sum_{i=1}^{k} g g_i v_i \mid g_r \neq g_s \forall r \neq s, g, g_i \in G, v_i \in Z^n \right\}$$

$$\because g, g_i \in G \Rightarrow g g_i \in G \ \forall \ i = 1,2,\cdots,k \Rightarrow \sum_{i=1}^{k} g g_i v_i \in F$$

$$\Rightarrow g(F) \subseteq F \quad \forall \ g \in G \qquad \cdots\cdots(1)$$

We observe that $I \in G \because G$ is a subgroup of $GL(n,Q)$.

Then, $\exists \ H \subseteq F$ s.t. $H = \left\{ I v_k + \sum_{i=1}^{k-1} g_i v_j \mid g_i \neq I \ \forall \ i, v_j = 0, v_k \in Z^n \right\}$. Also, we find that,

$$H = \{ v_k \mid v_k \in Z^n \} = Z^n .$$

$$\Rightarrow Z^n \subseteq F \qquad \cdots\cdots(2)$$

$F = \sum_{g \in G} g(Z^n)$, Thus, the set of generators for F is found to be –

$f = \{g(e_i) \mid e_i \in \text{standard basis for } \mathbb{Z}^n, \forall\, g \in G\}$

Which is a finite set as G is of finite order. Thus, the Fundamental Theorem of Abelian groups ensures that F is free.

Let d be a common denominator for all the generators of F (LCM of all denominators).

$\Rightarrow df \subseteq \mathbb{Z}^n \Rightarrow dF \subseteq \mathbb{Z}^n$ i.e., there exists a one-one mapping between f and $\mathbb{Z}^n$, thus, there exists a homomorphism between F and $\mathbb{Z}^n$ (property of a free group). We also observe that this homomorphism must be one-one. Therefore, F is isomorphic to a subgroup of $\mathbb{Z}^n$.

From (2), $\because \mathbb{Z}^n \subseteq F$ we can conclude that, $\mathbb{Z}^n \cong F$.

Let $\gamma : \mathbb{Z}^n \to F$ be such an isomorphism. Now, we define a linear transformation, $\Gamma : \mathbb{Q}^n \to \mathbb{Q}^n$ by $\Gamma(e_i) = \gamma(e_i)$ for $i = 1, 2, \ldots, n$ with a transformation matrix C with respect to the standard basis s.t. $\Gamma(v) = Cv \;\forall\, v \in \mathbb{Q}^n$. When restricted to $\mathbb{Z}^n$, $\Gamma = \gamma$. C^{-1} gives the transformation matrix for Γ^{-1} or when restricted to F, it gives $\gamma^{-1} : F \to \mathbb{Z}^n$.

For some $g \in G$,

$\Rightarrow C^{-1} g C(\mathbb{Z}^n) = C^{-1}(g(C(\mathbb{Z}^n)))$

$C(\mathbb{Z}^n) = F$

$\Rightarrow C^{-1} g C(\mathbb{Z}^n) = C^{-1}(g(F))$

From (1), $\because g(F) \subseteq F$

$\Rightarrow C^{-1}(g(F)) \subseteq \mathbb{Z}^n$

$\Rightarrow C^{-1} g C(\mathbb{Z}^n) \subseteq \mathbb{Z}^n \;\; \forall\, g \in G$

If $A \in \mathrm{M}_n(\mathbb{Q})$, then $A \in \mathrm{M}_n(\mathbb{Z})$ iff $A\vec{b} \in \mathbb{Z}^n \;\forall\, \vec{b} \in \mathbb{Z}^n$.

$C^{-1} g C \in \mathbb{Q}^n$, from the above we can say, $\Rightarrow C^{-1} g C \in \mathbb{Z}^n \;\forall\, g \in G$

$\Rightarrow C^{-1} G C \subseteq \mathrm{M}_n(\mathbb{Z})$ Also, $C^{-1} G C$ is a subgroup of $GL(n, \mathbb{Q})$

$\Rightarrow C^{-1} G C$ is a subgroup of $GL(n, \mathbb{Z})$

Any finite subgroup of $GL(n, \mathbb{Q})$ is conjugate to a subgroup of $GL(n, \mathbb{Z})$.

Hence, the theorem is proved.

Reduction mod p homomorphisms

Let p be a prime number.

Consider the set Z_p consisting of the non-negative integers not exceeding p. It is not only a group with addition modulo p as the group operation, but it also has another operation which is multiplication modulo p. All the non-zero elements have multiplicative inverses. If $\mathrm{M}_n(Z_p)$ denotes the set of all matrices of size n and entries from Z_p, the matrix multiplication operation involves both the addition and multiplication operations of Z_p. We consider the group $GL(n, Z_p)$ is the group of all invertible matrices from $\mathrm{M}_n(Z_p)$; the matrices in it have determinant which is not zero in Z_p.

Each entry of a matrix with integer entries can be reduced moulo p. With this operation, one may define a map $\nu_p : \mathrm{M}_n(Z) \to \mathrm{M}_n(Z_p)$ which will be called the reduction mod p for a prime p.

For example, if p=3,

$$\nu\left(\begin{bmatrix} 5 & 8 \\ 3 & 5 \end{bmatrix}\right) = \begin{bmatrix} \bar{2} & \bar{2} \\ \bar{0} & \bar{2} \end{bmatrix}$$

When restricted to $GL(n, Z)$, $\nu_p : GL(n, Z) \to GL(n, Z_p)$ is a group homomorphism.

The following result goes towards determining a subgroup of finite index in $GL(n, Z)$ with no nontrivial matrices of finite order.

Proposition **[1]** ***:*** Let q be a prime and suppose that $g^q = I$ for some $g \in GL(n, Z)$. If $p \neq 2$ is a prime, and if $\nu_p(g) = I$, then $g = I$.

PROOF :

Suppose, $g \neq I$ with $\nu_p(g) = I$. Then we can write $g = I + pH_1$ for some non-zero matrix H_1.

$\Rightarrow g = I + pdH$ where, d is the gcd of the entries of H_1 and the gcd of all the entries of H is 1.

$g^q = (I + pdH)^q$. Applying Binomial theorem,

$$g^q = I^q + qpdH + \frac{q(q-1)}{2} p^2 d^2 H^2 + \cdots + (pdH)^q$$

$$I = I + qpdH + \frac{q(q-1)}{2} p^2 d^2 H^2 + \cdots + (pdH)^q$$

$$qH + \frac{q(q-1)}{2} pdH^2 + \cdots + (pdH)^{q-1} H = 0 \quad \begin{bmatrix} \text{After cancelling common terms} \\ \text{and dividing by } pd \end{bmatrix}$$

In the above equation, we find that p divides each term, therefore p must divide qH.

$\Rightarrow p$ divides q OR p divides H

$\because$ All entries of H have no common factor. $\Rightarrow$ p divides q

$\because$ Both are primes $\Rightarrow$ $p = q$

Now, dividing each term by either p or q we get,

$$H + \frac{p(p-1)}{2} dH^2 + \cdots + p^{q-2} d^{q-1} H^q = 0$$

Similarly as above, we can say that p must divide H. This is a contradiction $\because$ gcd of H is 1 $\Rightarrow$ H is the zero matrix.

$\Rightarrow g = I$

Hence, proved.

Now, we can prove a beautiful, classical result due to Hermann Minkowski.

Minkowski's Theorem [1]:

If G is a finite subgroup of $GL(n, \mathbb{Z})$, then G is isomorphic to a subgroup of $GL(n, \mathbb{Z}_p)$ for all primes $p \neq 2$. In particular, the group $GL(n, \mathbb{Z})$ contains, upto isomorphism, finitely many finite subgroups.

PROOF :

Let $G \neq \{I\}$ be a finite subgroup of $GL(n, \mathbb{Z})$. For some prime $p \neq 2$, let ν_p be a map defined as above. Suppose that $G \cap Ker(\nu_p) \neq \{I\}$.

$\Rightarrow \exists\, x \in G$ s.t. $\nu_p(x) = I$ and $x^y = I$ where $y \in \mathbb{N}$ is the order of x and $x \neq I$

y may either be composite or prime. If it is composite, then there must exist some prime q s.t. q divides y.

$\because x \in G \Rightarrow x^{y/q} = g \in G$ as all powers of x must belong to G, G being a subgroup.

$\Rightarrow g^q = I$

$\nu_p(x) = I \Rightarrow \nu_p(x^{y/q}) = \nu_p(x)^{y/q} = I^{y/q} = I$

$\Rightarrow \exists\, g \in G$ s.t. $g^q = I$ where q is prime and $\nu_p(g) = I \Rightarrow g = I$ from the propositio n

$\therefore \;\; x^{y/q} = I$ and y is not the order of x. This is a contradiction.

If y was prime, then from the proposition we conclude that $x = I$, again a contradiction.

Therefore, $G \cap Ker(\nu_p) = \{I\}$. Thus, the map ν_p is injective when restricted to the subgroup G.

In other words, G is isomorphic to a subgroup of $GL(n, \mathbb{Z}_p)$.

Being a finite group, $GL(n, \mathbb{Z}_p)$ has only a finite number of subgroups.
Therefore, the group $GL(n, \mathbb{Z})$ contains, upto isomorphism, finitely many finite subgroups.

We immediately deduce:

Corollary :

Upto isomorphism, $GL(n, \mathbb{Q})$ contains only finitely many finite subgroups.

POSSIBLE ORDERS OF ELEMENTS OF $GL(n, \mathbb{Z})$:

The above proofs show us that there are only finitely many possibilities for orders of elements or subgroups of $GL(n, \mathbb{Z})$ and $GL(n, \mathbb{Q})$. Then, we try to find what these possible orders are and how they vary with n. Due to the finiteness of these possibilities we can also say that there must exist a maximal possible order for subgroups of $GL(n, \mathbb{Z})$.

For example :

Consider the matrix $A = \begin{bmatrix} 2 & -16 & 3 & -1 \\ 1 & -2 & 0 & 0 \\ 4 & 5 & -3 & 1 \\ 0 & 35 & -8 & 3 \end{bmatrix}$

The matrix A is a 4×4 matrix with order 12. Thus, we can say that $GL(4, \mathbb{Z})$ has an element and a subgroup of order 12. We will later verify that 12 is the maximal order of subgroups in $GL(4, \mathbb{Z})$.

Cyclotomic Polynomials

Consider a matrix A of order k; this implies that A satisfies the equation $x^k - 1 = 0$.

The roots of this polynomial are the kth roots of unity. Since A satisfies the given polynomial, the eigenvalues of A must also satisfy the given polynomial. Thus, the eigenvalues of k are kth roots of unity.

Minimal polynomial of an element is the monic polynomial of the smallest degree which when evaluated at the given element gives zero. The minimal polynomials of the roots of unity are called the cyclotomic polynomials.

The roots of the equation $x^m - 1 = 0$, the mth roots of unity, are given by-

$$\mu_m = \left\{ e^{2k\pi i/m} = \cos\left(2k\pi/m\right) + i\sin\left(2k\pi/m\right) : k = 1,2,\ldots,m \right\}$$

The above set of roots forms a cyclic group under multiplication of complex numbers. The generators of this group are called the primitive mth roots of unity. The primitive mth roots of unity are given by reducing the set of roots of unity by allowing only those values of k which are co-prime to m –

$$\mu_m = \langle \mu_d \rangle$$
$$\mu_d = \left\{ e^{2k\pi i/m} = \cos\left(2k\pi/m\right) + i\sin\left(2k\pi/m\right) : (k,m) = 1, 1 \le k \le m, k \in Z \right\}$$

The number of primitive mth roots of unity is given by $\phi(m)$, where $\phi(m)$ is the Euler's ϕ-function; $\phi(m)$ gives the number of positive integers lesser than or equal to m which are relatively prime to m.

For integers $n \ge 1$, $x^n - 1 = \prod_{m=0}^{n-1} \left(x - e^{2\pi i m/n} \right)$, over $\mathbb{C}$.

The mth cyclotomic polynomial is defined by $\Phi_{\mathrm{m}}(x) = \prod_{\gamma} (x - \gamma)$, where γ ranges over μ_d the set of all primitive mth roots of unity. Some properties of cyclotomic polynomials are as follows :

1. From the definition above, we can see that the degree of $\Phi_m(x)$ is given by $\phi(m)$ where ϕ is defined as above.

2. From the factorization of $x^n - 1 = \prod_{\gamma \in \mu_n} (x - \gamma)$, we group the factors together such that all γ s of order d are grouped together. By Lagrange's Theorem, d must always divide n. Since, γ has order d , therefore γ is a primitive d th root of unity.

   $\Rightarrow x^n - 1 = \prod_{d|n} \prod_{\gamma \in \mu_d} (x - \gamma)$

   Thus, we can also write

   $x^n - 1 = \prod_{d|n} \Phi_d(x)$

3. The cyclotomic polynomial, $\Phi_{\mathrm{m}}(x)$ is a monic polynomial over integers **[3]**.

   Proof :

   We fix a value for n

   $\Phi_1(x) = x - 1$, from the definition of cyclotomic polynomials.

We assume that $\Phi_d(x)$ is a monic polynomial over integers for all $d < n$.

Consider the polynomial, $F(x) = \prod_{d|n, d<n} \Phi_d(x)$.

$F(x) \in \mathbb{Z}[x]$ and its leading term has co-efficient 1, since $\forall d < n, \Phi_d(x)$ are monic polynomials over integers.

By division algorithm, $\exists\ h(x), r(x) \in \mathbb{Z}[x]$ such that $h(x)$ is monic and,

$x^n - 1 = F(x)h(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(F(x))$

By previous theorem we have $x^n - 1 = F(x)\Phi_n(x)$. Therefore, by uniqueness of quotient and remainder over $\mathbb{C}$, $h(x) = \Phi_n(x)$

Thus, $\Phi_n(x) \in \mathbb{Z}[x]$ and is a monic polynomial.

By principle induction, we can say that any cyclotomic polynomial is a monic polynomial over integers.

4. Cyclotomic polynomials are irreducible over $\mathbb{Q}$ **[3]**. Therefore, $x^n - 1 = \prod_{d|n} \Phi_d(x)$ is the irreducible factorization of $x^n - 1$.

Companion matrices of cyclotomic polynomials

With the help of cyclotomic polynomials we can create matrices of specified orders in $GL(n, \mathbb{Z})$.

Consider a positive integer m and the cyclotomic polynomial $\Phi_m(x)$.

We can construct a matrix of order m in the group of $\phi(m) \times \phi(m)$ matrices.

Let A be the companion matrix for the cyclotomic polynomial, $\Phi_m(x)$.

Recall that if $p(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ is a polynomial, then its companion matrix is given by

$$C = \begin{bmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{k-1} \end{bmatrix}$$

It can be checked that, $p(x)$ is the characteristic polynomial of its companion matrix C; so p(C) = 0.

From the properties of cyclotomic polynomials we can say that the coefficients of $\Phi_m(x)$ are integers. Thus, A is an integer matrix as A is of the form above. Also, since $\Phi_m(x)$ is an irreducible factor of $x^m - 1$, and $\Phi_m(A) = 0 \Rightarrow A^m = I$.

Let us assume that A has a minimal polynomial, $m_A(x) \in \mathbb{Z}[x]$. By the definition of minimal polynomials, $m_A(x)$ is a monic polynomial of the smallest degree for which, $m_A(A) = 0$. Consider, some polynomial $p(x) \in \mathbb{Z}[x]$ such that, $p(A) = 0$. By division algorithm of polynomials, $p(x) = m_A(x)h(x) + r(x)$ such that, $h(x), r(x) \in \mathbb{Z}[x]$ and $r(x) = 0$ or $\deg(r(x)) < \deg(m_A(x))$. Evaluating at A we get, $r(A) = 0$. If $r(x) \neq 0$, it will contradict the fact that $m_A(x)$ is the minimal polynomial of A. Therefore, $r(x) = 0$, $m_A(x)$ is a factor of any such polynomial $p(x)$ which when evaluate at A gives the zero matrix.

Thus, $m_A(x)$ is a factor of $\Phi_m(x)$. Since, $\Phi_m(x)$ is an irreducible polynomial, $\Rightarrow \Phi_m(x) = m_A(x)$. Therefore, m is the least degree for which A satisfies the polynomial, $x^m - 1$.

$\Rightarrow m$ is the order of A.

Now, we have a $\phi(m) \times \phi(m)$ matrix, A of order m with integer entries.

Now, consider the matrix in the previous example. We try and construct that matrix by using a cyclotomic polynomial.

Example :

$\phi(12) = 4$

If we factor $x^{12} - 1$, we find that $\Phi_{12}(x) = x^4 - x^2 + 1$. The companion matrix of $\Phi_{12}(x)$ is as follows-

$$C = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

By performing a few row operations on the 4×4 identity matrix, we obtain the following matrix –

$$B = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix} \text{ and with inverse } B^{-1} = \begin{bmatrix} 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -4 & 1 & 0 \\ 0 & 12 & -3 & 1 \end{bmatrix}$$

B and B^{-1} are elements of $GL(n, \mathbb{Z})$. Consider the matrix, $A = BCB^{-1}$, Conjugate of C in the group $GL(n, \mathbb{Z})$. Given that, $C^{12} = I$

$$\Rightarrow A^n = \left(BCB^{-1}\right)^n = \underbrace{BC\left(B^{-1}B\right)C\left(B^{-1}B\right)CB^{-1} \cdots BCB^{-1}}_{n} = BC^n B^{-1}$$

$$\Rightarrow A^{12} = BC^{12}B^{-1} = BIB^{-1} = I$$

Thus, the order of A is the same as C, 12.

On evaluating $A = BCB^{-1}$,

$$\begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -4 & 1 & 0 \\ 0 & 12 & -3 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 4 & 1 & 0 & 1 \\ 0 & 3 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -4 & 1 & 0 \\ 0 & 12 & -3 & 1 \end{bmatrix} = \begin{bmatrix} 2 & -16 & 3 & -1 \\ 1 & -2 & 0 & 0 \\ 4 & 5 & -3 & 1 \\ 0 & 35 & -8 & 3 \end{bmatrix}$$

We find that A is the same matrix as given in the previous example.

Remark on coefficients of cyclotomic polynomials:

Though, for the first 104 integers for n, the coefficients of $\Phi_n(x)$ belong only to $\{\pm 1, 0\}$, for $n = 105$, $\Phi_{105}(x)$ has two coefficients as -2. In fact, J.Suzuki proved the amazing fact that every integer occurs as a coefficient in some cyclotomic polynomial.

Finally, we find a way to determine if for a given integer m there exists a matrix of order m and size $n \times n$ for a fixed n and thus calculate the maximum possible order of a matrix in $GL(n, \mathbb{Z})$ for a fixed n.

The following theorem is the final result in this direction.

[1] MAIN THEOREM :

Let $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ with $p_1 < p_2 < \cdots < p_t$ distinct primes. Then $GL(n, \mathbb{Q})$ - and hence $GL(n, \mathbb{Z})$ - has an element of order m if, and only if,

1. $\sum_{i=1}^{t}(p_i - 1)p_i^{e_i - 1} - 1 \le n$ for $p_1^{e_1} = 2$
2. $\sum_{i=1}^{t}(p_i - 1)p_i^{e_i - 1} \le n$ otherwis***e***

For the proof of the above theorem, we need the following lemma.

We define a map, $W : \mathbb{Z} \to \mathbb{Z}$, such that, for

$m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ with $p_1 < p_2 < \cdots < p_t$

$$W(m) = \begin{cases} \sum_{i=1}^{t}(p_i - 1)p_i^{e_i - 1} - 1 \cdots \text{for } p_1^{e_1} = 2 \\ \sum_{i=1}^{t}(p_i - 1)p_i^{e_i - 1} \qquad \cdots \text{otherwise} \end{cases}$$

[1] ***Lemma:***

If $m \in \mathbb{N}$ and if $\{d_1, d_2, \cdots, d_s\}$ is a set of distinct divisors of m such that $lcm(d_1, d_2, \cdots, d_s) = m$, then $W(m) \le \sum_{i=1}^{s} \phi(d_i)$.

Proof :

Write $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$.

Since, $lcm(d_1, d_2, \cdots, d_s) = m$, upon separating out the common terms, we can obtain a set of integers, $\{c_1, c_2, \cdots, c_s\}$ such that for each i, c_i is a divisor of d_i, $c_1 c_2 \cdots c_s = m$, and gcd$(c_i, c_j) = 1$ $\forall\, i \ne j$.

Since, c_i divides d_i, then $\phi(c_i) \le \phi(d_i) \Rightarrow \sum_{i=1}^{s} \phi(c_i) \le \sum_{i=1}^{s} \phi(d_i) \qquad \cdots\cdots(1)$

Consider the sets S_i, for each $i = 1, 2, \cdots .s$, defined as $S_i = \left\{p_j^{e_j} : p_j^{e_j} \mid c_i\right\}$. Since all the c_i's are pairwise relatively prime to each other, therefore, $S_i \cap S_j$ gives the empty set $\forall\, i \ne j$. Since, $c_1 c_2 \cdots c_s = m$, therefore, $\bigcup_{i=1}^{s} S_i = \left\{p_1^{e_1}, p_2^{e_2}, \cdots, p_t^{e_t}\right\}$. Thus, $S_1, \cdots, S_s$ forms a partition on the set of maximal prime power factors of m. By partitioning this set we ensure that, given any $p_j^{e_j}$ we can always find an unique $i(j)$ such that, $p_j^{e_j}$ divides $c_{i(j)}$.

Without, loss of generality we can assume that $p_1^{e_1}$ divides c_1, as we can always rearrange the terms to make it so. Since, $\phi(ab) \geq \phi(a)+\phi(b)$ for all $a,b>2$, $\phi(c_i) \geq \sum_{p_j^{e_j} \in S_i} \phi\left(p_j^{e_j} \right)$ for all $i>1$.

Suppose $p_1^{e_1} \neq 2$, then similar to above, $\phi(c_1) \geq \sum_{p_j^{e_j} \in S_1} \phi(p_j^{e_j})$. Thus, $\sum_{i=1}^{s} \phi(c_i) \geq \sum_{i=1}^{t} \phi\left(p_j^{e_j} \right) = W(m)$.

Suppose $p_1^{e_1} = 2$, then we can say $\phi(c_1) \geq \phi\left({}^{c_1}\!/_{2} \right) \geq \sum_{p_j^{e_j} \in S_1, j\neq 1} \phi\left(p_j^{e_j} \right) = \sum_{p_j^{e_j} \in S_1} \phi\left(p_j^{e_j} \right) - 1$. Thus,

$\sum_{i=1}^{s} \phi(c_i) \geq \sum_{i=1}^{t} \phi\left(p_j^{e_j} \right) - 1 = W(m)$

From the above results and (1), we get, $\sum_{i=1}^{s} \phi(d_i) \geq W(m)$

Hence, the lemma is proved.

Now, using the above lemma we can prove the main theorem -

PROOF OF THEOREM:

Recall that

$$W(m) = \begin{cases} \sum_{i=1}^{t} (p_i - 1) p_i^{e_i - 1} - 1 \cdots \text{for } p_1^{e_1} = 2 \\ \sum_{i=1}^{t} (p_i - 1) p_i^{e_i - 1} \quad \cdots \text{otherwise} \end{cases}$$

To prove the above statement we must show that, $GL(n, Q)$ has an element of order m if and only if $W(m) \leq n$.

Case –I:

Suppose that, m is a positive integer such that $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ and $p_1^{e_1} \neq 2$ and $W(m) \leq n$. For each $p_i^{e_i}$ we can construct a matrix A_i of order $p_i^{e_i}$ and size $p_i^{e_i-1}(p_i - 1) \times p_i^{e_i-1}(p_i - 1)$ $\left[\because \Phi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)\right]$. We do this in the same manner as done in the example above. Then, we define a matrix B such that,

$$B = A_1 \oplus A_2 \oplus \cdots \oplus A_t = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & A_t \end{bmatrix}$$

The size of B is $\sum_{i=1}^{t} \phi\left(p_i^{e_i}\right) = \sum_{i=1}^{t} (p_i - 1) p_i^{e_i-1} = W(m)$, $\because \phi\left(p_i^{e_i}\right) = p_i^{e_i-1}\left(p_i - 1\right)$ and the order of B is $lcm(p_1^{e_1}, p_2^{e_2}, \ldots, p_t^{e_t}) = m$. Suppose $W(m) = n$, then, $A = B$ is the desired matrix. If, $W(m) < n$, then, $A = B \oplus I_s$,is the desired matrix where, $s = n - W(m)$.

Case-II:

Suppose that, $p_1^{e_1} = 2$ and $W(m) \leq n$.

$W(m) = \sum_{i=1}^{t} (p_i - 1) p_i^{e_i-1} - 1$, Substitute $p_1^{e_1} = 2$

$$\Rightarrow W(m) = p_1^{e_1-1}(p_1 - 1) + \sum_{i=2}^{t} p_i^{e_i-1}(p_i - 1) - 1 = 2^{1-1}(2-1) - 1 + \sum_{i=2}^{t} p_i^{e_i-1}(p_i - 1)$$
$$\Rightarrow W(m) = \sum_{i=2}^{t} p_i^{e_i-1}(p_i - 1) = W(m/2)$$
$$\Rightarrow W(m/2) \leq n$$

Thus, from the previous case we can see that, given $W(m/2) \leq n$, there must exist some matrix A of order $m/2$ belonging to $GL(n, Q)$. Since, $m/2$ is odd, then, $-A$ has order m.

Therefore, for any positive integer $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, When $W(m) \leq n$, then there must exist a matrix of order m in the group $GL(n, Q)$, and hence in $GL(n, Z)$.

Conversely suppose that, $A \in GL(n, Q)$ has order m for some $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$. Let, $m_A(x)$ be the minimal polynomial of the matrix A. Let the irreducible factorization of $m_A(x)$ be $m_A(x) = m_1(x)^{f_1} m_2(x)^{f_2} \cdots m_s(x)^{f_s}$. From the previous results we know that, $m_A(x)$ is the factor of any polynomial that when evaluated at A gives the zero matrix. Since, order of A is m, then $A^m = I$ and A satisfies the polynomial, $x^m - 1$. Thus, $m_A(x)$ is a factor of $x^m - 1$. Since the irreducible factorization of $x^m - 1 = \prod_{d|m} \Phi_d(x)$ gives distinct factors, thus $f_1 = f_2 = \cdots = f_s = 1$. By comparing these two factorizations, for each $i = 1,2,\cdots,s$ we get, $m_i(x) = \Phi_{d_i}(x)$, for some d_i which must be a divisor of m. Since, A has order m, $lcm(d_1, d_2, \cdots, d_s) = m$. By primary decomposition, A is similar over Q to a matrix of the form –

$$\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & - \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_s \end{bmatrix}$$

Where, the minimal polynomial of each A_i is $\Phi_{d_i}(x)$ for each $i = 1,2,\cdots,s$. For each i let l_i be the size of each A_i. Then, $l_i \geq \deg(m_i(x)) = \phi(d_i)$ for each i. Therefore, $\sum_{i=1}^{s} \phi(d_i) \leq \sum_{i=1}^{s} l_i = n$

From the above lemma, $W(m) \leq \sum_{i=1}^{s} \phi(d_i) \Rightarrow W(m) \leq n$.

Hence, we have proved the main theorem.

Here is an amusing corollary.

Corollary :

$GL(2k, Q)$ has an element of order m, if and only if, $GL(2k+1, Q)$ does.

PROOF:

Consider some positive integer m such that, $GL(2k, Q)$ has an element of order m.

$\Rightarrow W(m) \leq 2k$. But, this also gives the result that $W(m) \leq 2k+1$

Therefore, given, $GL(2k, Q)$ has an element of order m, then $GL(2k+1, Q)$ also has an element of order m.

Conversely, suppose $GL(2k+1, Q)$ has an element of order m. $\Rightarrow W(m) \leq 2k+1$. $W(m) = \sum_{i=1}^{t} p_i^{e_i - 1}(p_i - 1)$, where $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ and $p_1^{e_1} \neq 2$ as $2k+1$ is odd. Since each p_i is odd, then $p_i - 1$ is even for each i. Thus, each term is even, hence $W(m)$ is even. $W(m)$ will never be equal to $2k+1$.

Therefore, $W(m) \le 2k$, and $GL(2k, \mathbb{Q})$ has an element of order m , if and only if $GL(2k+1, \mathbb{Q})$ does.

Hence, the corollary is proved.

Table with orders of elements

Using the theorem described above and its following corollaries we can now find the possible orders of subgroups for a given n in $GL(n, \mathbb{Q})$ or $GL(n, \mathbb{Z})$ and thus, we can also find the maximal possible order of subgroups in these groups. In a similar manner we can also try and look at finite subgroups of the group $GL(n, \mathbb{R})$. But in such a case, the possibilities for a finite order need not be finite.

We conclude this report by observing the maximal finite order of elements in $GL(n, \mathbb{Z})$ for the first few terms of n **[1]**.

n	maximal order	n	maximal order
2	6	4	12
6	30	8	60
10	120	12	210
14	420	16	840
18	1260	20	2520
22	2520	24	5040

BIBLIOGRAPHY:

1. James Kuzmanovich and Andrey Pavlichenkov, Finite Groups of Matrices Whose Entries are Integers, The American Mathematical Monthly -109 –(2002)
2. D.S. Dummit & R.M. Foote, Abstract Algebra, 3rd ed., John Wiley and sons (2004)
3. R. Thangadurai, On coefficients of cyclotomic polynomials, in: Cyclotomic fields and related topics, Pune 1999, Bhaskaracharya, Pune, 2000, 311.
4. M. Artin, Algebra, Prentice Hall, 1991.