SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

On Minkowski's theorem on the finite subgroups of $GL_n(Q)$

av

Albin Andersson

2019 - No K33

On Minkowski's theorem on the finite subgroups of $GL_n(Q)$

Albin Andersson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Wushi Goldring

2019

ON MINKOWSKI'S THEOREM ON THE FINITE SUBGROUPS OF $GL_n\mathbf{Q}$

ALBIN ANDERSSON

ABSTRACT. In his book *"Finite groups: An Introduction"*, Jean-Pierre Serre presents an explanation of Minkowski's theorem regarding the finite subgroups of $GL_n(\mathbf{Q})$. This thesis aims to unpack and explain the steps used in Serre's explanation, and to make explicit many of the tools which Serre uses. The goal of this simplification is to make the theorem understandable to students with only a basic level knowledge of group theory. This is done through a series of steps, starting with explaining how to turn the theorem into a statement about l-groups. The thesis then walks through the steps of linking these l-groups to the order of $GL_n(\mathbf{F}_p)$, followed by constructing the function $M(n,l)$ in a manner such that it can be linked back to this order. Finally, it explains how these steps are connected to prove the first step of Minkowski's theorem for primes $l > 2$.

1. Introduction

This essay aims to introduce the proof of a theorem relating to the group $GL_n(\mathbf{Q})$. For this purpose, we begin by recalling the definition of this group.

Definition 1.0.1. *The group $GL_n(\mathbf{Q})$ is the group of $n \times n$ matrices which have a multiplicative inverse, with entries among the rational numbers.*

Minkowski's theorem is about the finite subgroups of $GL_n(\mathbf{Q})$. It states that finite subgroup G of $GL_n(\mathbf{Q})$, the order of G is bounded by a particular integer $M(n)$, dependent on the factor n. This paper aims to walk through the methods of how the theorem is proven in *Finite Groups: An Introduction* [2], with a focus on deconstructing each proof into separate parts and giving each part a thorough explanation.

For this purpose, the text is primarily focused on articulating the arguments in order to give a coherent surface-level overview of how to approach this theorem with only a basic understanding of group theory.

2. The main theorem

2.1. **Definitions.** To state the main theorem, we first begin by defining $M(n)$ as follows

Definition 2.1.1. *Let $n \in \mathbf{N}$ and let l be a prime number. Set*

$$M(n,l) = \left[\frac{n}{l-1}\right] + \left[\frac{n}{l(l-1)}\right] + \left[\frac{n}{l^2(l-1)}\right] + ...,$$

Date: June 2019.

then

$$M(n) = \prod_l l^{M(n,l)}$$

Here, the brackets indicate that only the integral parts of the results are considered. We can already note that $M(n,l)$ will only give nonzero results for primes $l \leq (n+1)$, meaning that for every n there will be a finite amount of nonzero results given by $M(n,l)$. We can then note that when calculating $M(n)$ there will be a limited amount of primes which do not become one by virtue of their corresponding $M(n,l)$ equaling 0. This ultimately leads to $M(n)$ being a finite integer, despite being defined as an infinite product dependent on an infinite sum.

2.2. **Statement.** The theorem itself consists of two claims, stated as follows:

Theorem 2.2.1. *(1) The order of a finite subgroup of $GL_n(\mathbf{Q})$ divides $M(n)$*
(2) $M(n)$ is the smallest integer having property (1)

We will demonstrate how the theorem is applied by computing $M(10)$, using the definition given above.

Example 2.2.2. *If we wished to compute M(10), it would go as follows:*
We begin by computing all applicable $M(10,l)$ which give nonzero results

$M(10,2) = [10/1] + [10/2] + [10/4] + [10/8] + [10/16] + \ldots = 10 + 5 + 2 + 1 + 0 + \ldots = 18$

$M(10,3) = [10/2] + [10/6] + [10/18] + \ldots = 5 + 1 + 0 + \ldots = 6$

$M(10,5) = [10/4] + [10/20] + \ldots = 2 + 0 + \ldots = 2$

$M(10,7) = [10/6] + [10/42] + \ldots = 1 + 0 + \ldots = 1$

With all applicable $M(10,l)$ calculated, we then know that $M(10)$ is calculated as

$$2^{18} \cdot 3^6 \cdot 5^2 \cdot 7^1 = 262,144 \cdot 729 \cdot 25 \cdot 7 = 33,443,020,800$$

This integer, according to the theorem, will be divided by the order of any finite subgroup of $GL_{10}(\mathbf{Q})$.

2.3. **Strategy for the proof.** The proof that these functions have the properties described in (1) was presented by Minkowski in three parts:

(i) He showed that if G is a finite subgroup of $GL_n(\mathbf{Q})$, then the order of G will divide the order of $GL_n(\mathbf{F}_p)$ for every prime greater than 2. This will be shown in Section 3.
(ii) He showed that if p is greater than 2, then any l-factor which is part of the prime factorisation of the order of $GL_n(\mathbf{F}_p)$ is $l^{M(n,l)}$. This is shown in Section 5 using the propositions established in section 4.
(iii) The second step is then shown to apply for $p = 2$ as well, by replacing GL_n with the orthogonal group O_n.

While working with these steps, part of the proof of (ii) will include the use of

the cyclic nature of $(\mathbf{Z}/l^2\mathbf{Z})^\times$, specifically in Section 4, Proposition 4.0.13. These groups are only cyclic for $l > 2$, and proving the case $l = 2$ requires moving beyond the propositions established in this thesis, hence this thesis only covers the case $l > 2$.
This paper only aims to explain the methods used to show (i) and (ii) as described in *Finite Groups: An introduction* [2] pp. 143-146.

3. First reductions from $GL_n(\mathbf{Q})$ to $GL_n(\mathbf{F}_p)$

This section will explain how the order of a finite subgroup G of $GL_n(\mathbf{Q})$ is related to the order of the group $GL_n(\mathbf{F}_p)$ through proving three separate propositions. The key purpose of this is to transform statement (1) of the theorem into a statement about l-subgroups.

Definition 3.0.1. *Let l be a prime. A finite l-subgroup of a group G is then a finite subgroup of G whose order is a power of l.*

Proposition 3.0.2. *We can replace replace statement (1) of Theorem 2.2.1 with a modified but equivalent version (1'), which goes as follows:*
(1') If l is a prime number, and A is a finite l-subgroup of $GL_n(\mathbf{Q})$, then $|A| \leq l^{M(n,l)}$

First we recall the definition of l-sylow subgroups, as well as Sylow's theorem as presented by Serre [2] p. 16.

Definition 3.0.3. *For any given group G, an l-sylow subgroup is a subgroup whose order is the greatest power of l which divides $|G|$*

Theorem 3.0.4. *For any given group G, there exists an l-sylow subgroup.*

Proof. (1) $\Rightarrow$ (1′)
To begin, we look at statement (1), which posits that the order of G divides $M(n)$. This would mean that the prime-factorisations of $|G|$ and $M(n)$ would have to consist of the same primes in order for divisibility to be maintained. We also know that no power of any one prime in $|G|$ can be greater than the power of the same prime in $M(n)$, or divisibility would fail. Therefore, it is clear that if $|G|$ divides $M(n)$, then the order of any given l-subgroup would be less than or equal to the l-factor of $M(n)$ which is $l^{M(n,l)}$ by definition. Therefore, (1) implies (1').
(1′) $\Rightarrow$ (1) Theorem 3.0.4 tells us that any given group G will have a subgroup A, whose order is the greatest power of l which divides the order of G. If we assume the validity of (1'), then any l-subgroup must have an order less than or equal to its corresponding $l^{M(n,l)}$. By theorem 3.0.4, there will be one such l-group A whose order is the greatest power of l which divides G. Since the order of A, according to (1'), is less than or equal to $l^{M(n,l)}$, any given l-factor of G will be less than the corresponding l-factor of $M(n)$. This means that as in (1), every l-component of G is shared with $M(n)$, and the powers in G are less than or equal to the powers in $M(n)$, ensuring that divisibility is always maintained, and subsequently showing that (1′) $\Rightarrow$ (1). As each statement implies the other, they are therefore equivalent. □

Proposition 3.0.2 allows us to focus our efforts on establishing propositions related to l groups, as opposed to all finite subgroups of $GL_n(\mathbf{Q})$. From here on, l is fixed, as is the l-group $A \subset GL_n(\mathbf{Q})$.

Definition 3.0.5. *The group $GL_n(\mathbf{Z}[1/q])$ is the group of invertible $n \times n$ matrices consisting of the rational numbers whose denominator divide q.*

Lemma 3.0.6. *There exists positive integer q such that $GL_n(\mathbf{Z}[1/q])$ contains $A \subset GL_n(\mathbf{Q})$.*

Proof. It is possible to construct the group $GL_n(\mathbf{Z}[1/q])$ by using a specific q for every A such that A is contained in $GL_n(\mathbf{Z}[1/q])$. We do this by taking as q, the product of all denominators of all coefficients of every matrix belonging to A. □

Remark 3.0.7. *This is not the most efficient method of constructing this group, but it is sufficient for the purpose of this theorem.*

We then recall the definition of the finite field $\mathbf{F}_p$.

Definition 3.0.8. *The finite field $\mathbf{F}_p$ is the set of integers* **mod** *p. It can also be denoted as $\mathbf{Z}/p\mathbf{Z}$*

Lemma 3.0.9. *If p is a prime number which does not divide q, then q is invertible in $\mathbf{F}_p$.*

This gives us a ring homomorphism $\mathbf{Z}[1/q] \to \mathbf{F}_p$, as every element of $\mathbf{Z}[1/q]$ can be taken to the integers $\mathbf{Z}$ by applying the multiplicative inverse of q. The result can then be reduced to $\mathbf{F}_p$, creating a ring. This then also gives us a homomorphism between the invertible matrices using the elements of $\mathbf{Z}[1/q]$ and $\mathbf{F}_p$:

$$GL_n(\mathbf{Z}[1/q]) \to GL_n(\mathbf{F}_p).$$

Proposition 3.0.10. *The homomorphism*

$$A \to GL_n(\mathbf{Z}[1/q]) \to GL_n(\mathbf{F}_p)$$

is injective.

In order to prove this proposition, we are going to show that no matrix $a \in A$, outside of the identity, reduces to the identity in $GL_n(\mathbf{F}_p)$. This will be done by examining all non-identity matrices $a \in A$ and for each of them, identifying a nonzero entry x_a which is not placed along the diagonal of the matrix. We will then use the product of all these entries to identify a p for which the proposition holds true.

Notation 3.0.11. *For every matrix $a \in A$, except the identity, create the associated matrix $q(a - I)$. In this matrix, some non-diagonal entry will be a nonzero integer. We denote this entry x_a.*

We know that x_a will be an integer. By lemma 3.0.6 all entries in a have denominators which divide q. This means that the entries in qa has purely integer coefficients, as does $q(a-I)$. As we have excluded the identity from the examination, we also know that for every a, at least one non-diagonal entry of $q(a - I)$ will be nonzero. This is the entry where we find the value for x_a.

Remark 3.0.12. *While we know that this nonzero entry of the matrix $q(a - I)$ must exist, it will not necessarily be the same entry for every matrix a.*

Lemma 3.0.13. *No matrix in A except for the unit matrix reduces to the identity in $Gl_n(\mathbf{F}_p)$.*

First we establish a lemma.

Lemma 3.0.14. *Reduction from $M_n(\mathbf{Z}[1/q])$ to $M_n(\mathbf{F}_p)$ is a ring homomorphism.*

After which we recall the definition of a ring homomorphism

Definition 3.0.15. *A ring homomorphism from a ring R to a ring S is a function $f : R \to S$ such that $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ i.e. f takes sums to sums and products to products.*

Proof of Lemma 3.0.13. We will now make use of the fact that $GL_n(\mathbf{Z}[1/q])$ is a subset of $M_n(\mathbf{Z}[1/q])$, and that $GL_n(\mathbf{F}_p)$ is a subset of $M_n(\mathbf{F}_p)$. This allows us to make a broader observation within $M_n(\mathbf{Z}[1/q])$ and $M_n(\mathbf{F}_p)$, which we can then apply back to $GL_n(\mathbf{Z}[1/q])$ and $GL_n(\mathbf{F}_p)$ respectively. The primary reason for this is to make use of lemma 3.0.14 and Definition 3.0.15.

What these lemmas tell us is, that any given $a \in A$ might reduce to I in $M_n(\mathbf{F}_p)$, through use of the morphism between $M_n(\mathbf{Z}[1/q])$ and $M_n(\mathbf{F}_p)$, which I will label f. If this were to happen then $f(a) - f(I) = I - I = 0$, and according to lemma 3.0.15, this also means that $f(a - I) = 0$, and vice versa. Since this morphism includes a reduction **mod** p, such a result would imply that any potential non-diagonal, nonzero entries in a were divisible by p and thus reduced to 0 **mod** p. Such an element has already been identified earlier, in the form of x_a.
This tells us that for any given p we might want to reduce to, if $q(a - I)$ has an x_a which is divisible by said p, then x_a would reduce to 0 in $\mathbf{F}_p$. If this is the case, then it becomes possible, though not guaranteed, that a could reduce to the identity in $M_n(\mathbf{F}_p)$. If, on the other hand, p does not divide the product of all identified x_a, thus not dividing any of them individually, this means that every matrix $a \in A$ has some nonzero element not placed on the diagonal after reduction to $\mathbf{F}_p$. By definition, the identity matrix only has nonzero integers along the diagonal, therefore this result contradicts the possibility of any a reducing to the identity. Thus, as long as we choose a p which divides no x_a we can conclude that no element in A apart from the identity reduces to the identity in $\mathbf{F}_p$, proving that the homomorphism is injective. □

Proposition 3.0.16. *If p is large enough, then the order of the l-subgroup A divides $r_n(p) = \prod_{i=1}^{n}(p^i - 1)$.*

We have already proven that every element of A reduces to an equivalent element in $GL_n(\mathbf{F}_p)$. As such, A is isomorphic to a subgroup B within $GL_n(\mathbf{F}_p)$. This tells us that the orders of these subgroups are the same, which subsequently tells us that the order of A also divides the order of $GL_n(\mathbf{F}_p)$. This leaves for us to prove that the order of $GL_n(\mathbf{F}_p)$ does indeed contain the mentioned $r_n(p)$.

Lemma 3.0.17. *The order of $GL_n(\mathbf{F}_p)$ contains the part $\prod_{i=1}^{n}(p^i - 1)$.*

Proof of lemma 3.0.17. $GL_n(\mathbf{F}_p)$ stands in bijection to the bases of $\mathbf{F}_p^n$, as every base for such a space can be represented by the columns of any given element of $GL_n(\mathbf{F}_p)$. This means that the order of $GL_n(\mathbf{F}_p)$ can be discerned by looking at all the possible ways in which we can construct the bases of $(\mathbf{F}_p)^n$.
For the first element of the base, we can choose any combination of n elements between 0 and p, save for making a base entirely out of zeroes, giving us $(p^n - 1)$ choices. Next, we can choose any base, except the p multiples of the first base,

giving us $(p^n - p)$ choices, and so on. Eventually this process will give us the product of all these binomials from $(p^n - 1)$ to $(p^n - p^{(n-1)})$.
From each of these separate binomials, we then factor out different power of p. For instance, from the first one we do not factor out anything, as there are no common factors in $(p^n - 1)$, then from the second we factor p from $(p^n - p)$, followed by factoring p^2 from $(p^n - p^2)$, and so on.
At the end of this process, we will be left with the product of a rather large power of p, as well as the remaining binomials, which, after rearranging them, are in the form of $r_n(p)$. Expressed as such:

$$|GL_n(\mathbf{F}_p)| = p^{n(n-1)/2} r_n(p)$$

At this point, we know that the order of an l-subgroup, A, divides a power of p times $r_n(p)$. As l is a prime, and we can choose p to be a prime greater than l so that we know that l can not divide p or its powers. Thus l must divide the other part of the order, proving that l divides $r_n(p)$. □

Why we are interested in $r_n(p)$ in particular will be explained in Section 5.

4. l-adic valuations as they are used in the construction of $M(n, l)$

This section aims to use what are called l-adic valuations in order to construct the form of $M(n, l)$ as it was described in the statement of the theorem. This section will also serve as the basis for linking $M(n, l)$ to the order of $GL_n(\mathbf{F}_p)$

Definition 4.0.1. *The l-adic valuation of a number x, denoted by $v_l(x)$, is the largest integer m such that l^m divides x.*

In essence, l-adic valuations are statements about the maximum powers of primes which are contained within an integer's prime factorization. As the previous section makes several statements regarding prime factorizations and divisibility, these estimations will be valuable tools, as will be established in the following propositions.

Proposition 4.0.2. *If m is a non-zero integer, then the l-adic valuation of $m!$ will be*

$$v_l(m!) = [\frac{m}{l}] + [\frac{m}{l^2}] + [\frac{m}{l^3}] + ...$$

The proof for the proposition will come after we have established several lemmas, beginning with a basic rule.

Lemma 4.0.3. *The valuation of a product, is equal to the sum of the individual valuations of the factors:*

$$v_l(xy) = v_l(x) + v_l(y)$$

Proof. We rewrite the factors x and y as compound integers of the forms $x = l^m \cdot a$ and $y = l^n \cdot b$. Here, $m = v_l(x)$ and $n = v_l(y)$. This implies that $xy = l^m \cdot a \cdot l^n \cdot b = l^{m+n} \cdot ab$. It then becomes clear that the greatest power of l which divides xy can be found by adding up their individual valuations □

Corollary 4.0.4. *If we label each factor of $m!$ as z, then $v_l(m!) = \sum_{z=1}^{m} v_l(z)$.*

We then define the term a_j so we can construct a more compact form of the sum in Corollary 4.0.4

Definition 4.0.5. *For every possible integer j, we let a_j be the value of z for which $v_l(z) = j$.*

Example 4.0.6. *To illustrate, if we were to look at $v_2(3!)$, then we can establish that the valuations of $3!$'s individual factors are:*
$v_2(1) = 0$, $v_2(2) = 1$, and $v_2(3) = 0$.
Looking at this, we see that there are two factors, 1 and 3, which have as their valuation, 0. This gives us two z between 1 and 3, for which $v_2(z) = 0$, meaning that $a_0 = 2$. The same method is applied to the only remaining integer, 2, whose valuation is 1. This tells us that there is one integer z between 1 and 3, whose $v_2(z) = 1$, and therefore $a_1 = 1$. Finally, any other indexes of a_j become 0, as any other power of 2 would be too large to divide any factor of $3!$.

If we use this definition of a_j in conjunction with lemma 4.0.3 , we get the equality

$$v_l(m!) = \sum_{z=1}^{m} v_l(z) = \sum_j j a_j.$$

Notation 4.0.7. *Let b_j denote $[\frac{m}{l^j}]$*

We know this is a valid division, as every j is a possible valuation for some component z of $m!$, and as such it will then also be less than m, giving us a nonzero result. The number b_j shows how many integer multiples of l^j are present in m, stated as the following lemma.

Lemma 4.0.8. *Let m, k, and q be positive integers. Then $[m/k]$ is the quotient q left when dividing m by k with remainder.*

Proof.

$$m = k \cdot q + r,\ 0 \leq r < k$$
$$\frac{m}{k} = q + \frac{r}{k},\ 0 \leq \frac{r}{k} < 1$$

hence, by definition of the integer part

$$q = [\frac{m}{k}]$$

□

Corollary 4.0.9. *Using lemma 4.0.8, $[\frac{m}{l^j}]$ is the number of integral multiples $q \cdot l^j$, $q > 0$ between 0 and m.*

Proof. Take $k = l^j$

□

Example 4.0.10. *Going back to $v_2(3!)$, we examine its different b_j:*

$$b_0 = [\frac{3}{2^0}] = 3$$
$$b_1 = [\frac{3}{2^1}] = 1$$
$$b_2 = [\frac{3}{2^2}] = 0$$

.

And any greater j will once again continue to return the value 0. As we can see, the results tell us that there are 3 multiples of 2^0, and 1 multiple of 2^1 between 0 and 3, as we would expect.

Lemma 4.0.11. *Let a_j be as defined as in Definition 4.0.5, and let b_j denote the same as in Notation 4.0.7. Then $a_j = b_j - b_{j+1}$.*

Proof. To start, we recall that the statement that some integer k has the valuation j can be broken down into two statements. First: it means that l^j divides k. Second: it means that l^{j+1} does not divide k.
Therefore, when evaluating how many integers up to m have valuation j, we first examine how many multiples of l^j there are up to m, as this is equivalent to examining how many integers up to m have the valuation of at least j. Next, we count how many integers have the valuation of at least $j+1$ and subtract these, to ensure that we only keep the integers which have a valuation strictly smaller than $j+1$, fulfiling both parts of the statement. Thus, $a_j = b_j - b_{j+1}$ □

Proof of proposition 4.0.2. Substitution of the terms from lemma 4.0.11 into the sum from lemma 4.0.3 then gives us the following equality

$$\begin{aligned} v_l(m!) &= a_1 + 2a_2 + 3a_3 + ... \\ &= (b_1 - b_2) + 2(b_2 - b_3) + 3(b_3 - b_4) + ... \\ &= b_1 + b_2 + b_3 + ... \\ &= [\frac{m}{l}] + [\frac{m}{l^2}] + [\frac{m}{l^3}] + ... \end{aligned}$$

which is the form proposed by Proposition 4.0.2. □

Proposition 4.0.12. *Let x, a, and b be integers such that $a, b \geq 1$. Then $[[x/a]/b] = [x/ab]$*

We omit the proof of this and refer to Serre [2] p. 145.

The following propositions will make use of the group $(\mathbf{Z}/l^2\mathbf{Z})^\times$, which is the group of integers **mod** l^2 that have a multiplicative inverse.

Proposition 4.0.13. *Let $x \in \mathbf{Z}$ be such that its class mod l^2 generates $(\mathbf{Z}/l^2\mathbf{Z})^\times$. Let k be an integer such that $k \geq 1$. Then:*

$$v_l(x^k - 1) = \begin{cases} 0, & \text{if } k \text{ is not divisible by } l-1 \\ v_l(k) + 1, & \text{if } k \text{ is divisible by } l-1 \end{cases}$$

First, we recall what it means for x to be a generator of $(\mathbf{Z}/l^2\mathbf{Z})^\times$. The group in question is cyclic for all primes $l > 2$, meaning that every element of the group can be expressed as a power of a single element when using multiplicative notation as we will be doing here. This single element is what we use for our x in the following lemmas. We will also be making use of the fact that if an element is a generator for $(\mathbf{Z}/l^2\mathbf{Z})^\times$, then it also follows that it generates $(\mathbf{Z}/l\mathbf{Z})^\times$ [2].
An important consequence of this is that that $x^y \equiv 1$ (**mod** l^2) if and only if $y = mn$ where $m \geq 1$ and n is the order of the group which x generates. The order of $(\mathbf{Z}/l^2\mathbf{Z})^\times$ is $l(l-1)$ and the order of $(\mathbf{Z}/l\mathbf{Z})^\times$ is $(l-1)$ [2].

We can now prove this proposition case by case.

Proof of case 1. Under these conditions, k is not a multiple of the order of $(\mathbf{Z}/l\mathbf{Z})^\times$. Therefore, x^k is not equivalent to 1 (**mod** l). Since the l-adic valuation of an integer is a statement about whether some powers of l divide that integer, the statement that $v_l(x^k-1)=0$ is equivalent to stating that l does not divide (x^k-1).
As x is a generator of $(\mathbf{Z}/l\mathbf{Z})^\times$ this means that any power of it will be part of $(\mathbf{Z}/l\mathbf{Z})^\times$. If a power is not divisible by $l-1$ then it will be any other element than 1 of the group, i.e. $x^k = ql + r$, $1 < r < l^2$. As r is strictly greater than 1, it follows that $x^k - 1$ will always have a remainder when divided by l, and thus is not divisible by l.
Since not being divisible by l is equivalent to having an l-adic valuation of 0, this tells us that $v_l(x^k-1)=0$ in this case. □

Proof of case 2. In this case k is a multiple of $l-1$, i.e. $k=(l-1)m$, for $m \geq 1$, then we are going to prove that $v_l(x^k-1) = v_l(k)+1$
Since k is now a multiple of the order of $(\mathbf{Z}/l\mathbf{Z})^\times$, and x is a generator of $(\mathbf{Z}/l\mathbf{Z})^\times$ we know that x^k is equivalent to 1 (mod l). In other words: $x^k = lq+1$. It then follows that x^k-1 when divided by l would leave the remainder 0, telling us that x^k-1 is a multiple of l. As such, it will have a nonzero l-adic valuation.

Notation 4.0.14. *Let, x remain as the generator of $(\mathbf{Z}/l\mathbf{Z})^\times$, and let y denote x^{l-1}*

This notation implies that if $k=(l-1)m$, then $x^k = y^m$. Because x is a generator (mod l), the definition also implies that $y = lq+1$, or in other words, it is congruent to 1 mod l. We also know that l does not divide z. This is because x, as a generator by definition is only equivalent to 1 when raised to the order of the group it generates. Since it also generates the group $(\mathbf{Z}/l^2\mathbf{Z})^\times$, this means that it is equivalent to 1 mod l^2 if and only if it is raised to the power of $l(l-1)$: $x^{l(l-1)} = zl^2+1$. If z divides l, this result would look different, which it by definition can not. We also know that z is not a multiple of l, as that would make it equivalent to 0 (mod l).
We then note that $m = r\cdot l^a$ if $a = v_l(m)$. The equivalence is clear as m by definition will consist of some product of primes, as well as the a-th power of l thanks to the definition of the l-adic valuation.
With these terms defined, we can set up the following equality, which will bring us to the proof of case 2:

$$x^k = y^m = (y^{l^a})^r = ((1+lz)^{l^a})^r = (1+l^{a+1}z+...)^r = 1+l^{a+1}zr+...$$

The first three steps are substitutions, and the latter two are the expansions of the binomials. Serre tells us that the unwritten terms are all divisible by l^{a+2} [2]. As we already know that z and r are not divisible by any powers of l, we then know that the l-adic valuation of the second term is equal to $a+1$, as it is the greatest power of l contained therein. As all other terms, except for the initial 1, are divisible by at least l^{a+2}, we then know that l^{a+1} is the greatest power of l which divides all terms in the equality, discounting the 1.
If we then subtract 1 from y^m, this leaves us with only the parts divisible by l left in the binomial, and thus the greatest power of l which divides all of them would be the

answer to $v_l(y^m - 1)$. As we know that l^{a+1} divides all terms in the expansion, and that l^{a+2} divides all terms except for one of them, this brings us to the conclusion that the greatest power of l dividing all terms in the expansion is $a + 1$, and thus $v_l(y^m - 1) = a + 1$. Substituting our terms back, gives us $v_l(x^k - 1) = v_l(k) + 1$, proving case 2. □

Proposition 4.0.15. *If we allow x to be as previously defined, then*

$$v_l(\prod_{i=1}^{n}(x^i - 1)) = M(n, l).$$

Proof. We begin by denoting

Notation 4.0.16. *Let N denote $\prod_{i=1}^{n}(x^i - 1)$.*

This notation implies that $v_l(N)$ will be equal to the sum of the valuation of each factor of N according to lemma 4.0.3: $v_l(N) = \sum_{i=1}^{n} v_l(x^i - 1)$. By proposition 4.0.13 we already know that the valuation of $(x^i - 1) = 0$ for every i which is not divisible by $l - 1$. Therefore, for any index for which the valuation is not 0, we can state that $i = y(l - 1)$, $1 < y \leq m = [\frac{n}{l-1}]$. The form of m reflects how the upper limit of the sum changes once we substitute i with y. We also know by the same proposition that when i is divisible by $l - 1$ the valuation is $v_l(i) + 1$. Finally, writing these substitutions down gives us:

$$v_l(N) = \sum_{i=1}^{n} v_l(x^i - 1) = \sum_{y=1}^{m} v_l(x^{(l-1)y} - 1) = \sum_{y=1}^{m} v_l((l - 1)y) + 1 = \sum_{y=1}^{m} 1 + v_l(y).$$

Now, a sum of valuations from 1 to m is equal to $v_l(m!)$, therefore

$$\sum_{y=1}^{m} 1 + v_l(y) = m + v_l(m!)$$

and by proposition 4.0.2 $v_l(m!)$ is equal to $[\frac{m}{l}] + [\frac{m}{l^2}] + [\frac{m}{l^3}] + ...$ Substituting back $m = [\frac{n}{l-1}]$ then gives us

$$[\frac{m}{l^\alpha}] = [\frac{\frac{n}{l-1}}{l^\alpha}] = [\frac{n}{(l - 1)l^\alpha}]$$

which tells us that

$$v_l(N) = \sum_{\alpha \geq 0} [\frac{n}{(l - 1)l^\alpha}] = M(n, l)$$

proving the lemma. □

5. Proof of statement (1) for primes $l > 2$

We have now established all the propositions needed in order to prove statement (1) of Theorem 2.2.1, which we recall as follows:

(1) The order of a finite subgroup of $GL_n(\mathbf{Q})$ divides $M(n)$.

5.1. **Proof of (1).** As previously stated, we will only present the proof of (1) for all primes $l > 2$ as follows.

Proof. Beginning with recalling Dirichlet's theorem on arithmetic progressions as presented in *A Course in Arithmetic* [1]:

Theorem 5.1.1. *If a and b are relatively prime integers, then there are infinitely many primes of the form $ax + b$, as x ranges over the integers.*

Therefore, we can find an arbitrarily large prime p whose equivalence class mod l^2 generates $(\mathbf{Z}/l^2\mathbf{Z})^\times$. This makes the p which we have chosen equivalent to the x used as a generator in Propositions 4.0.13 and 4.0.15. As it is a large enough prime, it also has the characteristics of the p chosen in Proposition 3.0.16. With these requirements met, proposition 4.0.15 tells us that $v_l(r_n(p)) = v_l(\prod_{i=1}^{n}(p^i - 1)) = M(n, l)$.
With this equality established, we go back to proposition 3.0.16 which established that the order of A will divide $r_n(p)$. As $|A|$ divides $r_n(p)$ the l-adic valuation of $|A|$ must be either less than or equal to the valuation of $r_n(p)$. That is to say, for $|A|$ to divide $r_n(p)$, they must share the prime l as part of their factorisations, and the greatest power of that prime present in the factorisation of $|A|$ must be less than or equal to the power of the same prime in $r_n(p)$: $v_l(|A|) \leq v_l(r_n(p))$.
Therefore, as A is a finite l-subgroup, meaning its order is a power of l, stating that the l-adic valuation of A is lesser than the l-adic valuation of $r_n(p)$ is equivalent to stating that the entire order of A is less than l raised to the valuation of $r_n(p)$. As Proposition 4.0.15 tells us that $v_l(r_n(p)) = M(n, l)$, this tells us that $|A| \leq l^{M(n,l)}$. This proves statement (1'), which by Proposition 3.0.2 is equivalent to statement (1), therefore proving statement (1) for primes $l > 2$. □

References

[1] J.-P. Serre. *A course in arithmetic*, volume 7 of *Graduate Texts in Math.* Springer-Verlag, 1973.
[2] J.-P. Serre. *Finite groups: an introduction*, volume 10 of *Surveys of Modern Mathematics.* International Press, Somerville, MA; Higher Education Press, Beijing, 2016. With assistance in translation provided by Garving K. Luli and Pin Yu.