Contemporary Mathematics
Volume 420, 2006

Orders of Finite Groups of Matrices

Robert M. Guralnick and Martin Lorenz

To Don Passman, on the occasion of his 65^{th} *birthday*

ABSTRACT. We present a new proof of a theorem of Schur's from 1905 determining the least common multiple of the orders of all finite groups of complex $n \times n$-matrices whose elements have traces in the field $\mathbb{Q}$ of rational numbers. The basic method of proof goes back to Minkowski and proceeds by reduction to the case of finite fields. For the most part, we work over an arbitrary number field rather than $\mathbb{Q}$. The first half of the article is expository and is intended to be accessible to graduate students and advanced undergraduates. It gives a self-contained treatment, following Schur, over the field of rational numbers.

1. Introduction

1.1. How large can a finite group of complex $n \times n$-matrices be if n is fixed? Put differently: if $\mathcal{G}$ is a finite collection of invertible $n \times n$-matrices over $\mathbb{C}$ such that the product of any two matrices in $\mathcal{G}$ again belongs to $\mathcal{G}$, is there a bound on the possible cardinality $|\mathcal{G}|$, usually called the *order* of $\mathcal{G}$? Without further restrictions the answer to this question is of course negative. Indeed, the complex numbers contain all roots of unity; so there are arbitrarily large finite groups inside $\mathbb{C}^*$. Thinking of complex numbers as scalar matrices, we also obtain arbitrarily large finite groups of $n \times n$-matrices over $\mathbb{C}$.

The situation changes when certain arithmetic conditions are imposed on the matrix group $\mathcal{G}$. When all matrices in $\mathcal{G}$ have entries in the field $\mathbb{Q}$ rational numbers, Minkowski **[33]** has shown that the order of $\mathcal{G}$ divides some explicit, and optimal, constant $M(n)$ depending only on the matrix size n. Later, Schur **[39]** improved on this result by showing that Minkowski's bound $M(n)$ still works if only the traces of all matrices in $\mathcal{G}$ are required to belong to $\mathbb{Q}$.

1.2. The first four sections of this article present full proofs of the theorems of Schur and Minkowski that depend on very few prerequisites. These sections follow Schur's approach via character theory and have been written with a readership of beginning graduate

---

2000 *Mathematics Subject Classification.* Primary 20-02, 20C15, 20G40; Secondary 11B99.

Key words and phrases. Finite linear group, group representation, Jordan bound, number field, Minkowski sequence.

RMG was supported in part by NSF Grant DMS 0140578.

Research of ML supported in part by NSA Grant H98230-05-1-0025 and by Leverhulme Research Interchange Grant F/00158/X.

and advanced undergraduate students in mind. Provided the reader is willing to accept one simple fact concerning group representations (Fact 2 in Section 3.2 below), the proofs will be completely understandable with only a rudimentary knowledge of linear algebra, group theory (symmetric groups, Sylow's theorem), and some algebraic number theory (minimal polynomials, Galois groups of cyclotomic fields). The requisite background material will be reviewed in Section 3.

The material in Section 5 is new. We show that Minkowski's original approach used in **[33]** in fact also yields Schur's theorem **[39]**. Minkowski's method is conceptually very simple, and it quickly and elegantly explains why some bound on the order $|\mathcal{G}|$ must exist, even for arbitrary algebraic number fields, that is, finite extensions of $\mathbb{Q}$. The method proceeds by reduction modulo suitably chosen primes and then using information about the orders of certain classical linear groups over finite fields. In fact, the general linear group alone almost suffices; only dealing with the 2-part of $|\mathcal{G}|$ using this strategy requires additional information. Since we work over algebraic number fields, a bit more mathematical background is assumed in this section.

As of this writing, Schur's theorem first appeared in print exactly a century ago and Minkowski's goes even further back. In the final section of this article, we will survey some recent related work of Collins, Feit and Weisfeiler on finite groups of matrices, in particular on the so-called Jordan bound. We will also mention two mysterious coincidences concerning the Minkowski numbers $M(n)$, one proven but unexplained, the other merely based on experimental evidence as of now.

1.3. Minkowski **[33]** proved his remarkable theorem in the course of his investigation of quadratic forms. Stated in group theoretical terms, the theorem reads as follows.

THEOREM 1 (Minkowski 1887). *The least common multiple of the orders of all finite groups of $n \times n$-matrices over $\mathbb{Q}$ is given by*

$$M(n) = \prod_p p^{\left\lfloor \frac{n}{p-1} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots} \tag{1}$$

Here, $\lfloor\,.\,\rfloor$ denotes the greatest integer less than or equal to . and p runs over all primes. Note that if $p > n+1$ then the corresponding factor in the product equals 1 and can be omitted. Therefore, (1) is actually a finite product. The first few values of $M(n)$ are:

$$M(1) = 2^1 = 2 \qquad M(2) = 2^{2+1}\,3^1 = 24$$
$$M(3) = 2^{3+1}\,3^1 = 48 \qquad M(4) = 2^{4+2+1}\,3^2\,5^1 = 5760$$

1.4. For a positive integer m and a prime p, let m_p denote the p-part of m, that is, the largest power of p dividing m. Thus, $M(n)_p = p^{\left\lfloor \frac{n}{p-1} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots}$. This number can be written in a more compact form. Indeed, the p-part of $m! = 1 \cdot 2 \cdot \ldots \cdot m$ is given by

$$(m!)_p = p^{\left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \cdots} . \tag{2}$$

To see this, put $m' = \left\lfloor \frac{m}{p} \right\rfloor$ and note that $m! = p \cdot (2p) \cdot \ldots \cdot (m'p) \cdot (\text{factors not divisible by } p)$. Therefore, $(m!)_p = p^{m'}(m'!)_p$ and (2) follows by induction. Using (2) we can write

$$M(n)_p = p^{\left\lfloor \frac{n}{p-1} \right\rfloor} \left(\left\lfloor \frac{n}{p-1} \right\rfloor ! \right)_p . \tag{3}$$

1.5. The notation $M(n)$, in the variant M_n, was introduced by Schur in [**39**] to honor Minkowski who had originally denoted the same number by $\overline{n|}$. Relaxing the condition in Theorem 1 that all matrix entries be rational and replacing it with the weaker requirement that only the matrix traces belong to $\mathbb{Q}$, Schur was able to prove that Minkowski's bound $M(n)$ still works:

THEOREM 2 (Schur 1905). *If $\mathcal{G}$ is any finite group of $n \times n$-matrices over $\mathbb{C}$ such that* $\operatorname{trace}(g) \in \mathbb{Q}$ *holds for all $g \in \mathcal{G}$ then the order of $\mathcal{G}$ divides $M(n)$.*

Schur's theorem covers a considerably larger class of groups than Theorem 1. In [**39**], the following example of a group covered by Theorem 2 but not Theorem 1 is given.

EXAMPLE 3. Consider the matrices $g = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $h = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, where $i = \sqrt{-1} \in \mathbb{C}$. Then $g^2 = h^2 = -1_{2\times 2}$ and $gh = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right) = -hg$. Thus $\mathcal{G} = \{\pm 1_{2\times 2}, \pm g, \pm h, \pm gh\}$ is a group of complex 2×2-matrices of order 8; it is isomorphic to the so-called quaternion group $\mathcal{Q}_8$. Note that the traces of all elements of $\mathcal{G}$ are rational – they are either 0 or ± 2 – but $\mathcal{G}$ certainly does not consist of matrices over $\mathbb{Q}$. In fact, there does not even exist an invertible complex 2×2-matrix a such that the matrices $x = aga^{-1}$ and $y = aha^{-1}$ both have entries in the field $\mathbb{R}$ of real numbers. To see this, note that x and y both would have determinant 1 and trace 0, as g and h do. A direct calculation shows that the product matrix $z = xy$ then satisfies ${z_{12}}^2 + {x_{12}}^2 + {y_{12}}^2 = -x_{12}y_{12}\operatorname{trace}(z)$, where $._{12}$ indicates the $(1,2)$-entry of the matrix in question. However, $\operatorname{trace}(z) = \operatorname{trace}(gh) = 0$. Hence, if x and y are matrices over $\mathbb{R}$ then all terms on the left will be zero. But then $1 = \det(x) = x_{11}x_{22} = -{x_{11}}^2$ which is impossible.

We remark in passing that, for any "irreducible" finite group $\mathcal{G}$ of complex $n \times n$-matrices, a necessary and sufficient condition for the existence of an invertible complex $n \times n$-matrix a such that aga^{-1} is real for all $g \in \mathcal{G}$ is that

$$\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} \operatorname{trace}(g^2) = 1 .$$

The sum on the left is called the *Frobenius-Schur indicator* of $\mathcal{G}$; see, e.g., Isaacs [**20**, Chapter 4]. The group $\mathcal{G} = \mathcal{Q}_8$ in the example above has Frobenius-Schur indicator -1.

1.6. The proof of Theorems 1 and 2 to be given in Section 4 below proceeds by first exhibiting sufficiently large groups of rational (in fact, integer) matrices showing that the least common multiple of the orders of all finite groups of $n \times n$-matrices over $\mathbb{Q}$ must be at least equal to $M(n)$. Thereafter, we may concentrate on Theorem 2 which in particular implies that the least common multiple in Theorem 1 does not exceed $M(n)$. Apart from updating terminology and notation to current usage and adding more generous details to the exposition, we have followed Schur's original approach in [**39**] quite closely. For a proof of Schur's theorem using slightly more sophisticated tools from representation theory, see Isaacs [**20**, Theorem 14.19]. A proof of Minkowski's Theorem 1 is also presented in Burnside [**6**, pp. 479–484] and in Bourbaki [**4**, chap. III §7, Exerc. 5–8]. Stronger results can be found in Feit [**17**] and in Serre [**41**, pp. 518–519].

1.7. This article is dedicated to our friend and colleague Don Passman. Don's contributions to group theory and ring theory in general and his expository masterpieces [**35**], [**36**] in particular have profoundly influenced our own work. In the course of various collaborations with Don, we have both benefitted from his deep insights and his generosity in sharing ideas.

NOTATIONS. Throughout, $\mathrm{GL}_n(R)$ will denote the group of all invertible $n \times n$-matrices over the commutative ring R. Recall that a matrix over R is invertible if and only if its determinant is an invertible element of R.

2. Large groups of integer matrices

The principal goal of this section is to construct certain groups of $n \times n$-matrices over $\mathbb{Z}$ such that the least common multiple of their orders equals the Minkowski bound $M(n)$ in (1). This will then allow us to give a reformulation of the core of Theorem 2.

2.1. Construction of groups. The main building blocks of the construction will be the symmetric groups $\mathcal{S}_r$ for various r. Recall that $\mathcal{S}_r$ consists of all permutations of $\{1, \dots, r\}$ and has order $r!$.

PROPOSITION 4. *Let a, m and n be positive integers with $am \leq n$. Then $\mathrm{GL}_n(\mathbb{Z})$ has a subgroup $\mathcal{G}$ of order $|\mathcal{G}| = (m+1)!^a\, a!$.*

PROOF. If we can realize $\mathcal{G}$ inside $\mathrm{GL}_{am}(\mathbb{Z})$ then we can view $\mathcal{G}$ as a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ via

$$\mathcal{G} \subseteq \mathrm{GL}_{am}(\mathbb{Z}) \cong \begin{pmatrix} \boxed{\mathrm{GL}_{am}(\mathbb{Z})} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \subseteq \mathrm{GL}_n(\mathbb{Z}) .$$

Therefore, we may assume that $n = am$. Think of the rows of any $n \times n$-matrix as partitioned into a blocks of m adjacent rows, and similarly for the columns. Now consider all matrices in $\mathrm{GL}_n(\mathbb{Z})$ that have exactly one $m \times m$-identity matrix $1_{m\times m}$ in each block of rows and each block of columns and 0s elsewhere; these are special permutation matrices. In fact, the collection of all these matrices forms a subgroup $\Pi \subseteq \mathrm{GL}_n(\mathbb{Z})$ that is isomorphic to the symmetric group $\mathcal{S}_a$:

$$\mathcal{S}_a \cong \Pi = \left\{ \left(\begin{array}{c|c|c|c|c} 1_{m\times m} & \cdots & & & \\ \hline & \cdots & & 1_{m\times m} & \\ \hline & \ddots & & & \\ \hline & \cdots & 1_{m\times m} & & \end{array} \right) \right\} \subseteq \mathrm{GL}_n(\mathbb{Z}) .$$

Next, we turn to the symmetric group $\mathcal{S}_{m+1}$. This group acts on the lattice $\mathbb{Z}^{m+1}$ by permuting its canonical basis $e_1 = (1, 0, \dots, 0), \dots, e_{m+1} = (0, \dots, 0, 1)$ via $\sigma(e_i) = e_{\sigma(i)}$. Note that this action maps the following sublattice to itself:

$$A_m = \{(z_1, \dots, z_{m+1}) \in \mathbb{Z}^{m+1} \mid \sum_i z_i = 0\} \cong \mathbb{Z}^m$$

(The notation A_m comes from the theory of root systems; cf. [3].) Thus, fixing some $\mathbb{Z}$-basis of A_m, each permutation $\sigma \in \mathcal{S}_{m+1}$ yields a matrix $\widetilde{\sigma} \in \mathrm{GL}_m(\mathbb{Z})$. It is easy to see that the map $\sigma \mapsto \widetilde{\sigma}$ is an injective group homomorphism $\mathcal{S}_{m+1} \to \mathrm{GL}_m(\mathbb{Z})$. Stringing each a-tuple $(\widetilde{\sigma_1}, \dots, \widetilde{\sigma_a})$ along the diagonal in $\mathrm{GL}_n(\mathbb{Z})$ we obtain a subgroup

$\Delta \subseteq \mathrm{GL}_n(\mathbb{Z})$ that is isomorphic to $\mathcal{S}_{m+1}^a$:

$$\mathcal{S}_{m+1}^a = \underbrace{\mathcal{S}_{m+1} \times \cdots \times \mathcal{S}_{m+1}}_{a \text{ factors}} \cong \Delta = \left\{ \begin{pmatrix} \boxed{\widetilde{\sigma_1}} & & & \\ & \boxed{\widetilde{\sigma_2}} & & \\ & & \ddots & \\ & & & \boxed{\widetilde{\sigma_a}} \end{pmatrix} \right\} \subseteq \mathrm{GL}_n(\mathbb{Z}) \, .$$

The subgroup Π of $\mathrm{GL}_n(\mathbb{Z})$ constructed earlier has only the identity matrix in common with Δ. Moreover, conjugating a matrix in Δ with a matrix from Π simply permutes the $\widetilde{\sigma_i}$-blocks along the diagonal. Therefore, defining $\mathcal{G}$ to be the subgroup of $\mathrm{GL}_n(\mathbb{Z})$ that is generated by Π and Δ, we obtain

$$|\mathcal{G}| = |\Delta|\,|\Pi| = (m+1)!^{\,a}\, a! \, ,$$

as desired. □

Now fix a prime $p \leq n+1$. Taking $m = p-1$ and $a = \left\lfloor \frac{n}{p-1} \right\rfloor$ in Proposition 4 we obtain a subgroup $\mathcal{G}$ of $\mathrm{GL}_n(\mathbb{Z})$ of order $p!^{\,a}\, a!$; so $|\mathcal{G}|_p = p^a (a!)_p$. In view of (3), this says that $|\mathcal{G}|_p = M(n)_p$. Letting p range over all primes $\leq n+1$, we have exhibited a collection of subgroups of $\mathrm{GL}_n(\mathbb{Z})$ such that the least common multiple of their orders is $M(n)$.

2.2. Reformulation of Theorem 2. Let $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{C})$ be as in Theorem 2. Our goal is to show that, for all primes p, the p-part $|\mathcal{G}|_p$ divides $M(n)_p = p^a\,(a!)_p$ with $a = \left\lfloor \frac{n}{p-1} \right\rfloor$ as in (3). Now Sylow's Theorem tells us that $\mathcal{G}$ has subgroups of order $|\mathcal{G}|_p$, the so-called Sylow p-subgroups of $\mathcal{G}$. Replacing $\mathcal{G}$ by one of its Sylow p-subgroups, the issue becomes to show that $|\mathcal{G}|$ divides $p^a a!$. Therefore, in order to prove Theorem 2, and thereby complete the proof of Theorem 1, it suffices to establish the following proposition.

PROPOSITION 5. *Let $\mathcal{G}$ be finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ whose order is a p-power for some prime p and such that* $\mathrm{trace}(g) \in \mathbb{Q}$ *holds for all $g \in \mathcal{G}$. Then $|\mathcal{G}|$ divides $p^a a!$ with $a = \left\lfloor \frac{n}{p-1} \right\rfloor$.*

3. Tools for the proof

The proof of Proposition 5 will depend on three ingredients: a lemma to narrow down the possible trace values, some basic facts on characters of group representations, and an observation concerning the familiar Vandermonde matrix. We will discuss each of these topics in turn.

3.1. Traces. This section uses a small amount of algebraic number theory. The book [23] by Janusz is a good background reference.

Besides the usual matrix traces, we will use a notion of trace that is associated with field extensions. Specifically, let K/F be a finite Galois extension with Galois group $\Gamma = \mathrm{Gal}(K/F)$. Then the trace $\mathrm{Tr}_{K/F}\colon K \to F$ is defined by $\mathrm{Tr}_{K/F}(\alpha) = \sum_{\gamma \in \Gamma} \gamma(\alpha)$ for $\alpha \in K$. If $x^m + cx^{m-1} + \ldots$ is the minimal polynomial of α over F then

$$\mathrm{Tr}_{K/F}(\alpha) = -\frac{|\Gamma|}{m} \cdot c \, . \tag{4}$$

This follows from the fact that the minimal polynomial of α is equal to $\prod_{i=1}^{m}(x-\alpha_i)$, where $\{\alpha_i\}_1^m$ are the distinct Galois conjugates $\gamma(\alpha)$ with $\gamma \in \Gamma$. We will only be concerned with the special case where $F = \mathbb{Q}$ and $K = \mathbb{Q}(e^{2\pi i/p^r})$ with p prime. The Galois group of $\mathbb{Q}(e^{2\pi i/p^r})/\mathbb{Q}$ is isomorphic to the group of units $(\mathbb{Z}/p^r\mathbb{Z})^*$ of the ring $\mathbb{Z}/p^r\mathbb{Z}$; its order is $\varphi(p^r) = p^{r-1}(p-1)$.

LEMMA 6. *Let $g \in \mathrm{GL}_n(\mathbb{C})$ be a matrix of finite order. Then* $|\operatorname{trace}(g)| \leq n$ *and* $\operatorname{trace}(g) = n$ *holds only for $g = 1_{n\times n}$. If the order of g is a power of p and* $\operatorname{trace}(g) \in \mathbb{Q}$ *then* $\operatorname{trace}(g)$ *must be one of the integers $\{n, n-p, n-2p, \ldots, n-ap\}$, where $a = \left\lfloor \frac{n}{p-1} \right\rfloor$.*

PROOF. By hypothesis, $g^q = 1_{n\times n}$ for some positive integer q. Let $\varepsilon_1, \ldots, \varepsilon_n$ denote the eigenvalues of g; they are all powers of $\zeta = e^{2\pi i/q}$. Hence, $\operatorname{trace}(g) = \sum_i \varepsilon_i$ belongs to the subring $\mathbb{Z}[\zeta] \subseteq \mathbb{C}$. By the triangle inequality, $|\operatorname{trace}(g)| \leq \sum_i |\varepsilon_i| = n$ and $\leq$ is equality if and only if all ε_i are the same, that is, g is a scalar matrix. In particular, $\operatorname{trace}(g) = n$ holds only for $g = 1_{n\times n}$.

Now assume that $q = p^r$ and $\operatorname{trace}(g) \in \mathbb{Q}$. Then $\operatorname{trace}(g)$ is actually an integer; see [**23**, Section I.2]. Let $\mathfrak{p} = (\zeta - 1)$ denote the ideal of $\mathbb{Z}[\zeta]$ that is generated by the element $\zeta - 1$. So $\zeta \equiv 1 \mod \mathfrak{p}$, and hence all $\varepsilon_i \equiv 1 \mod \mathfrak{p}$ and $\operatorname{trace}(g) \equiv n \mod \mathfrak{p}$. Therefore, $\operatorname{trace}(g) - n \in \mathfrak{p} \cap \mathbb{Z} = (p)$; see [**23**, Theorem I.10.1] for the last equality. Since we have already shown that $\operatorname{trace}(g) \leq n$, we conclude that $\operatorname{trace}(g) = n - pt$ for some non-negative integer t. It remains to show that $t \leq \frac{n}{p-1}$ or, equivalently,

$$\operatorname{trace}(g) \geq -\frac{n}{p-1}\,.$$

To this end, consider the Galois extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ and its trace $\operatorname{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$. The minimal polynomial over $\mathbb{Q}$ of a root of unity of order $p^s > 1$ is given by $x^{p^{s-1}(p-1)} + x^{p^{s-1}(p-2)} + \ldots + 1$ ([**23**, Theorem I.10.1] again). Therefore, equation (4) yields

$$\operatorname{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\varepsilon_i) = \begin{cases} \varphi(p^r) & \text{if } \varepsilon_i = 1\,, \\ -p^{r-1} & \text{if } \varepsilon_i \text{ has order } p\,, \\ 0 & \text{otherwise.} \end{cases}$$

Put $n_0 = \#\{i \mid \varepsilon_i = 1\}$ and $n_1 = \#\{i \mid \varepsilon_i \text{ has order } p\}$; so $0 \leq n_i \leq n$. Using the fact that $\operatorname{trace}(g) \in \mathbb{Q}$ we obtain

$$\varphi(p^r)\operatorname{trace}(g) = \operatorname{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\operatorname{trace}(g)) = \sum_i \operatorname{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\varepsilon_i) = \varphi(p^r)n_0 - p^{r-1}n_1\,.$$

Hence, $\operatorname{trace}(g) = n_0 - \frac{n_1}{p-1} \geq -\frac{n}{p-1}$, as desired. □

3.2. Characters. A *complex representation* of a group $\mathcal{G}$ is a homomorphism $\rho\colon \mathcal{G} \to \mathrm{GL}(V)$ for some $\mathbb{C}$-vector space V. If $n = \dim_{\mathbb{C}} V$ then we may identify $\mathrm{GL}(V)$ with $\mathrm{GL}_n(\mathbb{C})$; the integer n is called the *degree* of the representation ρ. The *character* $\chi = \chi_\rho$ of ρ is the complex-valued function on $\mathcal{G}$ that is given by $\chi(g) = \operatorname{trace}(\rho(g))$ for $g \in \mathcal{G}$.

Fact 1 *The sum $\sum_{g\in\mathcal{G}} \chi(g)$ is always an integer that is divisible by $|\mathcal{G}|$.*

To see this, consider the linear operator $e_\rho \in \operatorname{End}_{\mathbb{C}}(V) \cong \mathrm{M}_n(\mathbb{C})$ that is defined by $e_\rho = \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} \rho(g)$. Note that $\rho(g)e_\rho = e_\rho$ holds for all $g \in \mathcal{G}$, because multiplication with $\rho(g)$ simply permutes the summands of e_ρ. Hence, e_ρ is an idempotent operator: $e_\rho^2 = e_\rho$. Therefore, the trace of e_ρ is equal to the rank of e_ρ: $\operatorname{trace}(e_\rho) = \dim_{\mathbb{C}} e_\rho(V)$. On the other hand, $\operatorname{trace}(e_\rho) = \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} \operatorname{trace}(\rho(g)) = \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} \chi(g)$. This proves

Fact 1. We remark that Fact 1 is a special case of the so-called *orthogonality relations* of characters.

Fact 2 *The product of any two characters of $\mathcal{G}$ is again a character of $\mathcal{G}$. In particular, all powers χ^s $(s \geq 0)$ of a character χ are also characters of $\mathcal{G}$.*

Here, the 0^{th} power χ^0 is the constant function with value 1; it is the character of the so-called trivial representation $\mathcal{G} \to \mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$ sending every $g \in \mathcal{G}$ to 1. In order to show that the product of two characters, χ_ρ and $\chi_{\rho'}$, is itself a character, one needs to construct a complex representation of $\mathcal{G}$ whose character is $\chi_\rho \cdot \chi_{\rho'}$. This is achieved by the so-called tensor product $\rho \otimes \rho'$ of the representations ρ and ρ', a complex representation of degree equal to $\deg \rho \cdot \deg \rho'$ for whose detailed construction the reader is referred to Isaacs [**20**, Chapter 4] or any other text on group representation theory. More generally, tensor products of representations can be defined for *Hopf algebras*; they form an important aspect of the current investigation of *quantum groups*.

3.3. Vandermonde matrix. Given a collection $z_0, \ldots, z_a$ of elements in some commutative ring R (later we will take $R = \mathbb{Z}$), form the familiar Vandermonde matrix

$$V = \begin{pmatrix} 1 & z_0 & z_0^2 & \cdots & z_0^a \\ 1 & z_1 & z_1^2 & \cdots & z_1^a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & z_a & z_a^2 & \cdots & z_a^a \end{pmatrix}.$$

We will exhibit a matrix E over R so that the matrix product $V \cdot E$ is diagonal:

$$V \cdot E = \operatorname{diag}\left(\prod_{\substack{0 \leq s \leq a \\ s \neq 0}} z_0 - z_s, \prod_{\substack{0 \leq s \leq a \\ s \neq 1}} z_1 - z_s, \ldots, \prod_{\substack{0 \leq s \leq a \\ s \neq a}} z_a - z_s \right). \tag{5}$$

To this end, let $e_s = e_s(x_1, \ldots, x_a)$ denote the s^{th} elementary symmetric function in the commuting variables $x_1, \ldots, x_a$. These functions can be defined by

$$\prod_{i=1}^{a}(x - x_i) = \sum_{s=0}^{a} x^s (-1)^{a-s} e_{a-s}, \tag{6}$$

where x is an additional commuting variable. Explicitly, $e_s = \sum_I \prod_{i \in I} x_i$, where I runs over all subsets $I \subseteq \{1, \ldots, a\}$ with $|I| = s$. Specializing x to $z_{t'}$ and $(x_1, \ldots, x_a)$ to $(z_0, \ldots, \widehat{z_t}, \ldots, z_a)$, where $\widehat{z_t}$ signals that z_t has been deleted from the list, and defining

$$E = \left((-1)^{a-s} e_{a-s}(z_0, \ldots, \widehat{z_t}, \ldots, z_a)\right)_{s,t=0,\ldots,a}$$

equation (6) becomes the desired equation (5).

4. Schur's proof of Theorems 1 and 2

It remains to prove Proposition 5. So fix a prime p and let $\mathcal{G}$ be finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ whose order $|\mathcal{G}|$ is a power of p. We assume that $\operatorname{trace}(g) \in \mathbb{Q}$ holds for all $g \in \mathcal{G}$. Since the order of each g divides $|\mathcal{G}|$, Lemma 6 implies that the traces $\operatorname{trace}(g)$ can only take the values

$$z_t = n - pt \quad \text{with } 0 \leq t \leq a = \left\lfloor \tfrac{n}{p-1} \right\rfloor.$$

Put $m_t = \#\{g \in \mathcal{G} \mid \operatorname{trace}(g) = z_t\}$; so $m_0 = 1$ by Lemma 6. Proposition 5 is the case $t = 0$ of the following

CLAIM. For all $0 \le t \le a$, the order $|\mathcal{G}|$ divides the product $m_t p^a \prod_{\substack{0 \le s \le a \\ s \ne t}} s - t$.

To prove this, note that the inclusion $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{C})$ is a complex representation of $\mathcal{G}$ with character $\chi(g) = \operatorname{trace}(g)$. Therefore, it follows from Facts 1 and 2 above that, for each non-negative integer s, the sum $\sum_{g \in \mathcal{G}} \operatorname{trace}(g)^s$ is an integer that is divisible by $|\mathcal{G}|$. In other words, $\sum_{t=0}^{a} m_t z_t^s \equiv 0 \mod |\mathcal{G}|$ or, in matrix form,

$$(m_0, \ldots, m_a) \cdot V \equiv (0, \ldots, 0) \mod |\mathcal{G}|\,, \tag{7}$$

where $V = (z_t^s)_{t,s=0,\ldots,a}$ is the Vandermonde matrix, as in §3.3. Multiplying both sides of equation (7) with the matrix E constructed in §3.3, we deduce from equation (5) that

$$m_t \prod_{\substack{0 \le s \le a \\ s \ne t}} z_t - z_s \equiv 0 \mod |\mathcal{G}|$$

holds for all $0 \le t \le a$. Since $z_t - z_s = p(s-t)$, this is exactly what the claim states. This completes the proof of Proposition 5, and hence Theorems 1 and 2 are proved as well.

REMARK. It has been pointed out to us by Serre that the Claim above can be stated more generally as follows. Let $\mathcal{G}$ be a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$. Put $X = \{\operatorname{trace}(g) \mid g \in \mathcal{G}\}$ and, for each $\xi \in X$, let $m_\xi = \#\{g \in \mathcal{G} \mid \operatorname{trace}(g) = \xi\}$. Note that $X \subseteq \mathbb{Z}[\zeta]$ for some root of unity $\zeta \in \mathbb{C}$ so that the eigenvalues of each $g \in \mathcal{G}$ are powers of ζ; no a priori hypothesis on trace values is necessary. The above argument, with the obvious notational changes, proves the following:

For each $\xi \in X$, the product $m_\xi \prod_{\eta \in X \setminus \{\xi\}} (\xi - \eta)$ is divisible by $|\mathcal{G}|$.

The matrices V and E will now be matrices over $\mathbb{Z}[\zeta]$ and divisibility is to be understood in $\mathbb{Z}[\zeta]$. However, X is stable under the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, because each Galois automorphism sends ζ to some power ζ^s, and hence $\operatorname{trace}(g)$ is sent to $\operatorname{trace}(g^s) \in X$. Thus, if ξ is rational then so is the product $\prod_{\eta \in X \setminus \{\xi\}} (\xi - \eta)$, and hence this product is actually an integer and $|\mathcal{G}|$ divides $m_\xi \prod_{\eta \in X \setminus \{\xi\}} (\xi - \eta)$ in $\mathbb{Z}$. This applies in particular to $\xi = n \in X$, with $m_\xi = 1$. Therefore, $|\mathcal{G}|$ always divides $\prod_{\eta \in X \setminus \{n\}} (n - \eta)$ in $\mathbb{Z}$. Now, if $|\mathcal{G}|$ is a power of p and $\operatorname{trace}(g) \in \mathbb{Q}$ holds for all $g \in \mathcal{G}$ then Lemma 6 implies that $\prod_{\eta \in X \setminus \{n\}} (n - \eta)$ is a divisor of $\pm p^a a!$; so $|\mathcal{G}|$ divides $p^a a!$, as desired.

5. Minkowski's reduction method

Minkowski's original proof of Theorem 1 is quite different from Schur's. The essential tool are reduction homomorphisms to the general linear group over certain finite fields. The reduction method applies to algebraic number fields K, that is, finite extensions of $\mathbb{Q}$, and very quickly yields rough bounds for the orders of all finite subgroups $\mathcal{G} \subseteq \mathrm{GL}_n(K)$; see Proposition 11 below. In fact, subgroups $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{C})$ satisfying only $\operatorname{trace}(g) \in K$ for all $g \in \mathcal{G}$ can also be treated by this strategy due to the fact that linear groups over finite fields can be realized over the subfield generated by the traces; see Lemma 8. A sharp bound for the $2'$-part of $|\mathcal{G}|$ can be easily deduced in this way from the well-known order of the general linear group over a finite field together with some elementary number theoretic observations; see Proposition 15. The 2-part of $|\mathcal{G}|$ requires additional information concerning certain classical groups associated to hermitian or skew-hermitian forms. This will be explained in §§ 5.5 and 5.6 below.

As usual, the field with q elements will be denoted by $\mathbb{F}_q$. We will also occasionally write the p-part of an integer m as $m_p = p^{v_p(m)}$, and $m_{p'}$ will denote the p'-part of m; so $m_{p'} = m/m_p$.

5.1. The general linear group over finite fields. It is well-known and easy to see that $\mathrm{GL}_n(\mathbb{F}_q)$ has order $\prod_{i=0}^{n-1}(q^n - q^i)$; cf., e.g., Rotman [**38**, Theorem 8.5]. Thus, if $q = p^f$ then

$$(8) \qquad |\,\mathrm{GL}_n(\mathbb{F}_q)|_{p'} = \prod_{i=1}^{n}(q^i - 1)\,.$$

LEMMA 7. *Let ℓ be an odd prime. There are infinitely many primes p such that*

$$|\,\mathrm{GL}_n(\mathbb{F}_{p^f})|_\ell = \ell^{(1+v_\ell(f))\lfloor n/\tau\rfloor}\,(\lfloor n/\tau\rfloor!)_\ell$$

holds for all positive integers n and f, where $\tau = \frac{\ell-1}{(\ell-1,f)}$.

PROOF. We use the fact that, for odd primes ℓ, the group of units $(\mathbb{Z}/\ell^s\mathbb{Z})^*$ of the ring $\mathbb{Z}/\ell^s\mathbb{Z}$ is cyclic of order $\varphi(\ell^s) = \ell^{s-1}(\ell-1)$. Any integer whose residue class modulo ℓ^2 generates $(\mathbb{Z}/\ell^2\mathbb{Z})^*$ will also generate the units modulo all powers ℓ^s; see [**19**, proof of Theorem 2 on p. 43]. Moreover, by Dirichlet's theorem on primes in arithmetic progression (e.g., [**40**, p. 61]), the residue class modulo ℓ^2 of any generator of $(\mathbb{Z}/\ell^2\mathbb{Z})^*$ contains infinitely many primes p. Let p be one of these primes. Then p has order $\varphi(\ell^s)$ in $(\mathbb{Z}/\ell^s\mathbb{Z})^*$; so $p^i \equiv 1 \mod \ell^s$ if and only if i is divisible by $\varphi(\ell^s)$. In other words, ℓ divides $p^i - 1$ if and only if $\ell - 1$ divides i and, in this case,

$$(p^i - 1)_\ell = \ell\left(\tfrac{i}{\ell-1}\right)_\ell\,.$$

Now put $q = p^f$. Then ℓ divides $q^i - 1$ if and only if τ divides i and, in this case, $(q^i-1)_\ell = \ell\, f_\ell\,(i/\tau)_\ell$. For $1 \le i \le n$, this applies to $i = \tau, 2\tau, \ldots, \alpha\tau$, where $\alpha = \lfloor n/\tau\rfloor$. Thus, $|\,\mathrm{GL}_n(\mathbb{F}_{p^f})|_\ell = \prod_{i=1}^{n}(q^i-1)_\ell = (\ell\, f_\ell)^\alpha\,(\alpha!)_\ell$, which proves the lemma. □

We remark that, for $f = 1$, the expression $\ell^{(1+v_p(f))\lfloor n/\tau\rfloor}\,(\lfloor n/\tau\rfloor!)_\ell$ in Lemma 7 is identical with the ℓ-part of the Minkowski bound $M(n)$; see equation (3). Thus, for an odd prime ℓ,

$$(9) \qquad |\,\mathrm{GL}_n(\mathbb{F}_p)|_\ell = M(n)_\ell$$

holds for infinitely many primes p. Lemma 7 fails for the prime $\ell = 2$, because the linear group is too big. For example, for all odd primes p, $|\,\mathrm{GL}_2(\mathbb{F}_p)|_2 = (p-1)_2(p^2-1)_2$ is divisible by 16 while $M(2)_2 = 8$.

LEMMA 8. *Let $\mathcal{G}$ be a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$, where $q = p^f$. Assume that p does not divide $|\mathcal{G}|$ and that $p > n$. If all $g \in \mathcal{G}$ satisfy $\mathrm{trace}(g) \in F$ for some subfield $F \subseteq \mathbb{F}_q$ then $\mathcal{G}$ is conjugate to a subgroup of $\mathrm{GL}_n(F)$.*

PROOF. Let $\Bbbk = F^{\mathrm{alg}}$ denote an algebraic closure of F with $\mathbb{F}_q \subseteq \Bbbk$, and let σ denote the canonical topological generator of $\mathrm{Gal}(\Bbbk/F) \cong \widehat{\mathbb{Z}}$. Then σ acts on $\mathrm{GL}_n(\Bbbk)$ by $(g_{i,j})^\sigma_{n\times n} = \left(g^\sigma_{i,j}\right)_{n\times n}$. By our hypothesis on traces, the map $\mathcal{G} \to \mathrm{GL}_n(\Bbbk)$, $g \mapsto g^\sigma$, is a $\Bbbk$-representations of $\mathcal{G}$ having the same character as the inclusion $\mathcal{G} \hookrightarrow \mathrm{GL}_n(\Bbbk)$. Since both representations are semisimple, by Maschke's theorem, they are isomorphic. (The proof of [**5**, § 12, Proposition 3] works in characteristic $p > n$.) Thus, there exists a matrix

$u \in \mathrm{GL}_n(\Bbbk)$ such that $ugu^{-1} = g^\sigma$ holds for all $g \in \mathcal{G}$. By Lang's theorem [**28**], we can write $u = v^\sigma v^{-1}$ for some $v \in \mathrm{GL}_n(\Bbbk)$. Thus, each $v^{-1}gv$ is fixed by σ, and hence it belongs to $\mathrm{GL}_n(F)$. By the Noether-Deuring Theorem (e.g., Curtis-Reiner [**12**, p. 139]), we may replace v by a matrix in $\mathrm{GL}_n(\mathbb{F}_q)$, proving the lemma. □

REMARKS. (a) Lang's theorem is a much more general result than what is actually needed for the proof of Lemma 8; see, e.g., Borel [**2**, Corollary 16.4]. Indeed, we only invoke the theorem for the algebraic group GL_n and, in this case, it is a special case of Speiser's version of Hilbert's Theorem 90: the Galois cohomology set $H^1(F, \mathrm{GL}_n)$ is trivial for every field F; cf. Serre [**42**, Proposition X.3] or Knus et. al. [**26**, Remark 29.3]. For a finite field F, triviality of $H^1(F, \mathrm{GL}_n)$ amounts to the desired fact that every $u \in \mathrm{GL}_n(F^{\mathrm{alg}})$ can be written as $u = v^\sigma v^{-1}$, where σ is the Frobenius generator of $\mathrm{Gal}(F^{\mathrm{alg}}/F)$; see [**26**, Exercise 2 on p. 442].

(b) It follows from (a) that $H^1(\mathbb{F}_q, \mathrm{PGL}_n)$ is trivial as well: every $U \in \mathrm{PGL}_n(\mathbb{F}_q^{\mathrm{alg}}) = \mathrm{GL}_n(\mathbb{F}_q^{\mathrm{alg}})/(\mathbb{F}_q^{\mathrm{alg}})^*$ can be written as $U = V^\sigma V^{-1}$ for some $V \in \mathrm{PGL}_n(\mathbb{F}_q^{\mathrm{alg}})$. Moreover, triviality of $H^1(\mathbb{F}_q, \mathrm{PGL}_n)$ is equivalent to Wedderburn's commutativity theorem for finite division rings; see [**42**, Proposition X.8] or [**26**, p. 396]. For an alternative proof of a version of Lemma 8 based on Wedderburn's commutativity theorem, see Isaacs [**20**, Theorem 9.14]. Incidentally, Wedderburn's article [**45**] appeared in 1905, as did Schur's, and Speiser's generalization of Hilbert's Theorem 90 appeared in 1919 [**44**, Satz 1]. None of this was available to Minkowski when [**33**] was written.

5.2. The reduction map. Throughout this section, K will denote an algebraic number field and $\mathcal{G}$ will be a finite subgroup of $\mathrm{GL}_n(K)$. Furthermore, $\mathcal{O} = \mathcal{O}_K$ will denote the ring of algebraic integers in K.

Put $L = \sum_{g \in \mathcal{G}} g \cdot \mathcal{O}^n \subset K^n$; this is a $\mathcal{G}$-stable finitely generated $\mathcal{O}$-submodule of K^n. If $\mathcal{O}$ is a principal ideal domain (or, put differently, K has class number 1) then the theory of modules over PIDs tells us that L is isomorphic to $\mathcal{O}^n$; see, e.g., Jacobson [**21**, Section 3.8]. Therefore:

If $\mathcal{O} = \mathcal{O}_K$ is a PID then $\mathcal{G}$ is conjugate in $\mathrm{GL}_n(K)$ to a subgroup of $\mathrm{GL}_n(\mathcal{O})$.

For $K = \mathbb{Q}$, for example, this says that every finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ can be conjugated into $\mathrm{GL}_n(\mathbb{Z})$. This explains why it was enough to look at integer matrices rather than matrices over $\mathbb{Q}$ in Section 2.

In general, $\mathcal{O}$ is a Dedekind domain and the foregoing applies "locally": for every prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the localization $\mathcal{O}_\mathfrak{p}$ is a PID; see Jacobson [**22**, Section 10.2]. Consequently, as above, we may conclude that $\mathcal{G}$ is conjugate in $\mathrm{GL}_n(K)$ to a subgroup of $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$, and hence we may assume that $\mathcal{G} \subseteq \mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ after replacing $\mathcal{G}$ by a conjugate. In fact, except for finitely many primes of $\mathcal{O}$, the group $\mathcal{G}$ is actually contained in $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ at the outset: if $a \in \mathcal{O}$ is a common denominator for all matrix entries of all elements of the original $\mathcal{G}$ then $\mathcal{G} \subseteq \mathrm{GL}_n(\mathcal{O}[1/a])$; so any prime $\mathfrak{p}$ not containing a will do. Now let $\mathfrak{p} \neq 0$ and put $(p) = \mathfrak{p} \cap \mathbb{Z}$. Then $\mathcal{O}/\mathfrak{p}$ is a finite field of characteristic p. The number of elements of $\mathcal{O}/\mathfrak{p}$ is often called the *absolute* or *counting norm* of $\mathfrak{p}$; it will be denoted by $\mathcal{N}(\mathfrak{p})$. Thus,

$$\mathcal{O}/\mathfrak{p} \cong \mathbb{F}_{\mathcal{N}(\mathfrak{p})} \quad \text{and} \quad \mathcal{N}(\mathfrak{p}) = p^f ,$$

where $f = f(\mathfrak{p}/\mathbb{Q})$ is the relative degree of $\mathfrak{p}$ over $\mathbb{Q}$. Reduction of all matrix entries modulo the maximal ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ gives a homomorphism

$$\mathrm{GL}_n(\mathcal{O}_\mathfrak{p}) \to \mathrm{GL}_n(\mathbb{F}_{\mathcal{N}(\mathfrak{p})}) , \tag{10}$$

because $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \cong \mathcal{O}/\mathfrak{p}$. The following lemma is well-known. Only the first assertion will be needed later; the second is included for its own sake. Recall that, since $\mathcal{O}_\mathfrak{p}$ is a local PID, its non-zero ideals are exactly the powers of the maximal ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$. The *ramification index* of $\mathfrak{p}$ over $\mathbb{Q}$ is the power e such that $p\mathcal{O}_\mathfrak{p} = \mathfrak{p}^e\mathcal{O}_\mathfrak{p}$.

LEMMA 9. *The kernel of the reduction homomorphism* (10) *has at most p-torsion. In fact, any torsion element g in the kernel satisfies* $g^{p^i} = 1_{n\times n}$ *for some* $p^i \le ep/(p-1)$.

PROOF. For each $g \in \mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$, define $d(g) = \sup\{m \mid g - 1_{n\times n} \in \mathrm{M}_n(\mathfrak{p}^m\mathcal{O}_\mathfrak{p})\}$; so $d(g) = \infty$ if and only if $g = 1_{n\times n}$ and $d(g) > 0$ if and only if g belongs to the kernel of (10). Now assume that $0 < d = d(g) < \infty$ and write $g = 1_{n\times n} + \pi^d h$, where π is a generator of the ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ and $h \in \mathrm{M}_n(\mathcal{O}_\mathfrak{p}) \setminus \mathrm{M}_n(\mathfrak{p}\mathcal{O}_\mathfrak{p})$. Then $g^r = 1_{n\times n} + \pi^d(rh+s)$ with $s = \sum_{i=2}^{\ell}\binom{r}{i}\pi^{d(i-1)}h^i \in \mathrm{M}_n(\mathfrak{p}\mathcal{O}_\mathfrak{p})$. If $(r,p) = 1$ then $rh + s \notin \mathrm{M}_n(\mathfrak{p}\mathcal{O}_\mathfrak{p})$ and so $g^r \ne 1_{n\times n}$. This shows that the kernel of (10) has at most p-torsion.

We claim that any $g \in \mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ with $d = d(g) > 0$ satisfies $d(g^p) \ge \min\{e+d, pd\}$, and $d(g^p) = e + d$ if $pd > e + d$. Indeed, we may assume that $d < \infty$. Writing $g = 1_{n\times n} + \pi^d h$ be as above, we obtain $g^p = 1_{n\times n} + \pi^{dp}h^p + t$ with $t = \sum_{i=1}^{p-1}\binom{p}{i}\pi^{di}h^i$. Since p divides all binomial coefficients $\binom{p}{i}$ occurring in t, we have $t \in \mathrm{M}_n(\mathfrak{p}^{e+d}\mathcal{O}_\mathfrak{p}) \setminus \mathrm{M}_n(\mathfrak{p}^{e+d+1}\mathcal{O}_\mathfrak{p})$. The claim follows from this. We conclude in particular that $g^p \ne 1_{n\times n}$ if $\infty > (p-1)d > e$.

Now assume that $g \in \mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ is a torsion-element with $0 < d(g) < \infty$. Then $g^{p^i} = 1_{n\times n}$ for some positive integer i. If i is chosen minimal then our observations in the previous paragraph imply that $e \ge (p-1)d(g^{p^{i-1}}) \ge (p-1)p^{i-1}d(g)$. Hence, $p^i \le ep/(p-1)$ which proves our second assertion. □

The above proof also shows that if $m(p-1) > e$ then there is no non-trivial torsion in the kernel of the homomorphism $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p}) \to \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^m)$ that is defined by reduction of all matrix entries modulo $\mathfrak{p}^m\mathcal{O}_\mathfrak{p}$.

EXAMPLE 10. Let $K = \mathbb{Q}$. Then $\mathfrak{p} = (p)$ and $e = 1$. Thus, in Lemma 9, we must have $i = 0$ when p is an odd prime, and $i \le 1$ when $p = 2$. In other words, the kernel of the reduction map $\mathrm{GL}_n(\mathbb{Z}_{(p)}) \to \mathrm{GL}_n(\mathbb{F}_p)$ is torsion-free for odd p. For $p = 2$, the only non-trivial torsion possible is order 2. The kernel of $\mathrm{GL}_n(\mathbb{Z}_{(2)}) \to \mathrm{GL}_n(\mathbb{Z}/4\mathbb{Z})$ is torsion-free.

The first assertion of Lemma 9 implies that the p'-part $|\mathcal{G}|_{p'}$ of the order of $\mathcal{G}$ divides $|\mathrm{GL}_n(\mathbb{F}_{\mathcal{N}(\mathfrak{p})})|_{p'}$. In view of equation (8), this yields the following proposition.

PROPOSITION 11. *Let $\mathcal{G}$ be a finite subgroup of* $\mathrm{GL}_n(K)$, *where K is an algebraic number field. Then, for each non-zero prime $\mathfrak{p}$ of $\mathcal{O}_K$ lying over $p \in \mathbb{Z}$, $|\mathcal{G}|_{p'}$ divides* $\prod_{i=1}^{n}(\mathcal{N}(\mathfrak{p})^i - 1)$.

Applying Proposition 11 with any two choices of $\mathfrak{p}$ lying over different rational primes yields a bound for the order of $\mathcal{G}$. Moreover, Proposition 11 comes close to establishing the Minkowski bound $M(n)$ for the field of rational numbers:

EXAMPLE 12. For a finite subgroup $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Q})$ and a given prime ℓ, Proposition 11 implies that the ℓ-part $|\mathcal{G}|_\ell$ of the order of $\mathcal{G}$ divides $|\mathrm{GL}_n(\mathbb{F}_p)|_\ell$, where p is any prime other than ℓ. Furthermore, if $\ell \ne 2$ then $|\mathrm{GL}_n(\mathbb{F}_p)|_\ell = M(n)_\ell$ for infinitely many primes p, by (9). Thus, we have shown (again) that if $\mathcal{G}$ is a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ then $|\mathcal{G}|_\ell$ divides $M(n)_\ell$ for all primes $\ell \ne 2$. In order to extend this to the prime $\ell = 2$, Minkowski uses additional facts about quadratic forms. This will be explained below.

5.3. The Schur bound. Fix an algebraic number field K. We will describe certain constants $S(n,K)$, introduced by Schur in [**39**], for the purpose of extending Theorem 2 to general algebraic number fields. Thus, $S(n,\mathbb{Q})$ will be identical to $M(n)$. Like $M(n)$, the constant $S(n,K)$ will be defined as a product of ℓ-factors for all prime numbers ℓ, and almost all ℓ-factors will be 1. Throughout, we put

$$\zeta_m = e^{2\pi i/m} \in \mathbb{C}\,.$$

For a given prime ℓ, the chain $K\cap\mathbb{Q}(\zeta_\ell)\subseteq\cdots\subseteq K\cap\mathbb{Q}(\zeta_{\ell^m})\subseteq K\cap\mathbb{Q}(\zeta_{\ell^{m+1}})\subseteq\dots$ of subfields of K must stabilize, since K is finite over $\mathbb{Q}$. Thus we may define

$$m(K,\ell)=\min\{m\geq 1 \mid K\cap\mathbb{Q}(\zeta_{\ell^m})=K\cap\mathbb{Q}(\zeta_{\ell^{m+1}})=\dots\}\,. \tag{11}$$

Now put

$$t(K,\ell)=[\mathbb{Q}(\zeta_{\ell^{m(K,\ell)}}):K\cap\mathbb{Q}(\zeta_{\ell^{m(K,\ell)}})]\,. \tag{12}$$

and define

$$\begin{aligned} S(n,K) &= 2^{n-\lfloor\frac{n}{t(K,2)}\rfloor}\prod_\ell \ell^{m(K,\ell)\lfloor\frac{n}{t(K,\ell)}\rfloor+\lfloor\frac{n}{\ell t(K,\ell)}\rfloor+\lfloor\frac{n}{\ell^2 t(K,\ell)}\rfloor+\dots} \\ &= 2^{n-\lfloor\frac{n}{t(K,2)}\rfloor}\prod_\ell \ell^{m(K,\ell)\lfloor\frac{n}{t(K,\ell)}\rfloor}\left(\left\lfloor\frac{n}{t(K,\ell)}\right\rfloor!\right)_\ell\,. \end{aligned} \tag{13}$$

Here, ℓ runs over all rational primes, including 2, and the second equality follows from equation (2). Since $t(K,\ell)[K:\mathbb{Q}]\geq\ell-1$, only finitely many ℓ will satisfy $t(K,\ell)\leq n$ and so almost all ℓ-factors are trivial.

EXAMPLE 13. Let $K=\mathbb{Q}(\zeta_k)$ for some positive integer k. Since $\mathbb{Q}(\zeta_k)\cap\mathbb{Q}(\zeta_t)=\mathbb{Q}(\zeta_{(k,t)})$, we have $m(K,\ell)=\max\{1,v_\ell(k)\}$. If ℓ does not divide k then $t(K,\ell)=\ell-1$; otherwise $t(K,\ell)=1$. For $K=\mathbb{Q}$ in particular, we obtain $m(\mathbb{Q},\ell)=1$ and $t(\mathbb{Q},\ell)=\ell-1$ for all ℓ. Thus, equation (13) reduces to (1) and so $S(n,\mathbb{Q})=M(n)$.

In [**39**], Schur proved the following generalization of Theorem 2 using a larger dose of character theory than what was needed in Section 4.

THEOREM 14 (Schur 1905). *Let $\mathcal{G}$ be a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ such that the traces of all elements of $\mathcal{G}$ belong to some fixed algebraic number field K. Then $|\mathcal{G}|$ divides $S(n,K)$.*

An alternative description of the constants $S(n,K)$ is as follows. Let μ_{ℓ^∞} denote the group of all ℓ-power complex roots of unity. Then $K\cap\mathbb{Q}(\mu_{\ell^\infty})=K\cap\mathbb{Q}(\zeta_{\ell^{m(K,\ell)}})$.

- If ℓ is odd then each $K\cap\mathbb{Q}(\zeta_{\ell^m})/\mathbb{Q}$ is a subextension of $\mathbb{Q}(\zeta_{\ell^m})/\mathbb{Q}$ which is cyclic with Galois group isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^*\cong\mathbb{Z}/\ell^{m-1}\mathbb{Z}\times\mathbb{Z}/(\ell-1)\mathbb{Z}$. Also, $K\cap\mathbb{Q}(\zeta_\ell)$ is the fixed subfield of $K\cap\mathbb{Q}(\zeta_{\ell^m})$ under the group $\mathbb{Z}/\ell^{m-1}\mathbb{Z}$. Thus, $[K\cap\mathbb{Q}(\zeta_{\ell^m}):\mathbb{Q}]=[K\cap\mathbb{Q}(\zeta_\ell):\mathbb{Q}][K\cap\mathbb{Q}(\zeta_{\ell^m}):\mathbb{Q}]_\ell$ and $[K\cap\mathbb{Q}(\zeta_\ell):\mathbb{Q}]$ is a divisor of $\ell-1$. Hence, for odd primes ℓ,

$$\begin{aligned} m(K,\ell) &= 1+v_\ell([K\cap\mathbb{Q}(\mu_{\ell^\infty}):\mathbb{Q}]) \\ t(K,\ell) &= [\mathbb{Q}(\zeta_\ell):K\cap\mathbb{Q}(\zeta_\ell)]=\frac{\ell-1}{(\ell-1,[K\cap\mathbb{Q}(\mu_{\ell^\infty}):\mathbb{Q}])}\,. \end{aligned} \tag{14}$$

- For the prime $\ell=2$, the extension $\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}$ has Galois group $(\mathbb{Z}/2^m\mathbb{Z})^*\cong\mathbb{Z}/2^{m-2}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ $(m\geq 2)$. The factor $\mathbb{Z}/2\mathbb{Z}$ is generated by complex conjugation. When $m>2$, the field $\mathbb{Q}(\zeta_{2^m})$ has exactly three subfields that are not contained in $\mathbb{Q}(\zeta_{2^{m-1}})$: besides $\mathbb{Q}(\zeta_{2^m})$, there are $\mathbb{Q}(\zeta_{2^m}+\zeta_{2^m}^{-1})$ and $\mathbb{Q}(\zeta_{2^m}-\zeta_{2^m}^{-1})$. If $t(K,2)=1$, which certainly holds when $m(K,2)=1$ or $m(K,2)=2$, then $K\cap\mathbb{Q}(\mu_{2^\infty})=\mathbb{Q}(\zeta_{2^{m(K,2)}})$, and so $[K \cap \mathbb{Q}(\mu_{2^\infty}) : \mathbb{Q}] = 2^{m(K,2)-1}$. If $t(K,2) \neq 1$ then $K \cap \mathbb{Q}(\mu_{2^\infty})$ must be equal to either $\mathbb{Q}(\zeta_{2^{m(K,2)}} + \zeta_{2^{m(K,2)}}^{-1})$ or $\mathbb{Q}(\zeta_{2^{m(K,2)}} - \zeta_{2^{m(K,2)}}^{-1})$. Thus, $t(K,2) = 2$ and $[K \cap \mathbb{Q}(\mu_{2^\infty}) : \mathbb{Q}] = 2^{m(K,2)-2}$. In either case, the 2-factor of $S(n,K)$ in (13) simplifies to

$$S(n,K)_2 = [K \cap \mathbb{Q}(\mu_{2^\infty}) : \mathbb{Q}]^{\lfloor \frac{n}{t(K,2)} \rfloor} 2^n (n!)_2 \tag{15}$$

The following properties of $S(n,K)$ are easy to verify:

$$S(m,K)S(n,K) \text{ divides } S(m+n,K) \tag{16}$$

and

$$S(n,K) \text{ divides } S(n,F) \text{ if } K \subseteq F. \tag{17}$$

5.4. Odd primes. The following proposition establishes Theorem 14 for the $2'$-part of $|\mathcal{G}|$. The special case where $K = \mathbb{Q}$ was done earlier in Example 12.

PROPOSITION 15. *Let $\mathcal{G}$ be a finite subgroup of* $\mathrm{GL}_n(\mathbb{C})$. *Assume that the traces of all elements of $\mathcal{G}$ belong to some algebraic number field K. Then $|\mathcal{G}|_\ell$ divides $S(n,K)$ for all odd primes ℓ.*

PROOF. Replacing $\mathcal{G}$ by a conjugate in $\mathrm{GL}_n(\mathbb{C})$ if necessary, we can make sure that $\mathcal{G} \subseteq \mathrm{GL}_n(F)$ for some algebraic number field $F \supseteq K$. Indeed, any splitting field for $\mathcal{G}$ that is finite over K will serve this purpose; see [**20**, Theorem 9.9]. Let $\mathcal{O} = \mathcal{O}_F$ denote the ring of algebraic integers of F and consider any non-zero prime $\mathfrak{p}$ of $\mathcal{O}$ such that $\mathcal{G} \subseteq \mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ and $\ell \notin \mathfrak{p}$. Put $(p) = \mathfrak{p} \cap \mathbb{Z}$ and assume that p is chosen as in Lemma 7 and also satisfies $p > n$. Let $\rho\colon \mathcal{G} \to \mathrm{GL}_n(\mathbb{F}_{\mathcal{N}(\mathfrak{p})})$ denote the reduction homomorphism (10) restricted to $\mathcal{G}$. Upon replacing $\mathcal{G}$ by a Sylow ℓ-subgroup, the map ρ becomes injective, by Lemma 9, and our goal now is to show that $|\mathcal{G}|$ divides $S(n,K)_\ell$.

As in the first paragraph of the proof of Lemma 6, one sees that the traces of all elements of $\mathcal{G}$ actually belong to the ring of algebraic integers $\mathcal{O}_{K'}$ of the field $K' = K \cap \mathbb{Q}(\mu_{\ell^\infty})$. Therefore, $\mathrm{trace}(\rho(g)) \in \mathbb{F}_q$ holds for all $g \in \mathcal{G}$, where $q = \mathcal{N}(\mathfrak{p} \cap \mathcal{O}_{K'}) = p^f$. Lemma 8 now implies that $\rho(\mathcal{G})$ is conjugate to a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ and Lemma 7 further gives that

$$|\mathcal{G}| \quad \text{divides} \quad |\,\mathrm{GL}_n(\mathbb{F}_q)|_\ell = \ell^{(1+v_\ell(f))\lfloor \frac{n}{\tau} \rfloor} \left(\lfloor \tfrac{n}{\tau} \rfloor !\right)_\ell ,$$

where $\tau = \frac{\ell-1}{(\ell-1,f)}$. Now, for odd ℓ,

$$S(n,K)_\ell = \ell^{m(K,\ell)\lfloor \frac{n}{t(K,\ell)} \rfloor} \left(\left\lfloor \frac{n}{t(K,\ell)} \right\rfloor ! \right)_\ell$$

with $m(K,\ell) = 1 + v_\ell([K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}])$ and $t(K,\ell) = \frac{\ell-1}{(\ell-1,[K\cap\mathbb{Q}(\mu_{\ell^\infty}):\mathbb{Q}])}$ by (14). Since the residue class of p generates $(\mathbb{Z}/\ell^s\mathbb{Z})^*$ for all s, p remains prime in $\mathbb{Z}[\zeta_{\ell^s}]$; see the proof of Lemma 7 and [**19**, Theorem 2 on p. 196]. In particular, p remains prime in $\mathcal{O}_{K'}$, and so $f = f(\mathfrak{p} \cap \mathcal{O}_{K'}/\mathbb{Q}) = [K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}]$. Therefore, $|\,\mathrm{GL}_n(\mathbb{F}_q)|_\ell = S(n,K)_\ell$ and the proposition is proved. □

5.5. Unitary, orthogonal and symplectic groups. In this section, we review some standard facts about hermitian and skew-hermitian forms and certain classical groups that are associated with them. Throughout, $\Bbbk$ will denote a field and $a \mapsto a^\theta$ will be an automorphism of $\Bbbk$ satisfying $\theta^2 = \mathrm{Id}$. We assume for simplicity that $\mathrm{char}\,\Bbbk \neq 2$.

5.5.1. *Sesquilinear forms.* Let V denote an n-dimensional vector space over $\Bbbk$. A bi-additive map $\beta\colon V \times V \longrightarrow \Bbbk$ is called *sesquilinear* (with respect to θ) if

$$\beta(av, bw) = ab^{\theta}\beta(v, w)$$

holds for all $v, w \in V$ and $a, b \in \Bbbk$. When θ is the identity, sesquilinear forms are ordinary bilinear forms. A sesquilinear form β is called *non-singular* if β satisfies the following equivalent conditions: (i) $\beta(v, V) = \{0\}$ for $v \in V$ implies $v = 0$; (ii) $\beta(V, v) = \{0\}$ for $v \in V$ implies $v = 0$; (iii) for any basis $\{v_1, \ldots, v_n\}$ of V, the matrix $(\beta(v_i, v_j))_{n\times n}$ has non-zero determinant; see [**29**, Proposition XIII.7.2]. If β is any sesquilinear form on V and $g \in \mathrm{GL}(V)$ then, defining $\beta^g(v, v') := \beta(g(v), g(v'))$ for $v, v' \in V$, one again obtains a sesquilinear form β^g on V with respect to θ; it is called *equivalent* to β.

Sesquilinear forms β satisfying $\beta(w, v) = \beta(v, w)^{\theta}$ (resp. $\beta(w, v) = -\beta(v, w)^{\theta}$) for all $v, w \in V$ are called *hermitian* (resp. *skew-hermitian*). The stabilizer in $\mathrm{GL}(V)$ of a non-singular hermitian or skew-hermitian form β is called the group of *isometries* of (V, β) and is denoted by $\mathrm{Iso}(V, \beta)$; so

$$\mathrm{Iso}(V, \beta) = \{g \in \mathrm{GL}(V) \mid \beta(g(v), g(v')) = \beta(v, v') \text{ for all } v, v' \in V\}\,.$$

Let β be non-singular skew-hermitian. If $\beta(v, v) \neq 0$ for some $v \in V$ then $\beta' = \beta(v, v)\beta$ is a non-singular hermitian form on V with $\mathrm{Iso}(V, \beta') = \mathrm{Iso}(V, \beta)$. On the other hand, if $\beta(v, v) = 0$ for all $v \in V$ then it is easy to see that $\theta = \mathrm{Id}$ and so β is an alternating bilinear form. Therefore, when studying isometry groups of non-singular hermitian or skew-hermitian forms β on V, it suffices to consider the following cases:

unitary case: β is hermitian with respect to $\theta \neq \mathrm{Id}$;
orthogonal case: β is symmetric bilinear ($\theta = \mathrm{Id}$);
symplectic case: β is alternating bilinear ($\theta = \mathrm{Id}$).

5.5.2. *Twisting modules.* Now assume that V is a finitely generated (left) $\Bbbk[\mathcal{G}]$-module, where $\mathcal{G}$ is a finite group. We let $V^{\theta} = \{v^{\theta} \mid v \in V\}$ denote a copy of V with operations

$$v^{\theta} + w^{\theta} = (v + w)^{\theta}\,, \quad (av)^{\theta} = a^{\theta}v^{\theta} \quad \text{and} \quad gv^{\theta} = (gv)^{\theta}$$

for $v, w \in V$, $a \in \Bbbk$ and $g \in \mathcal{G}$. Then V^{θ} becomes a $\Bbbk[\mathcal{G}]$-module and

$$\mathrm{trace}_{V^{\theta}/\Bbbk}(g) = \big(\mathrm{trace}_{V/\Bbbk}(g)\big)^{\theta} \tag{18}$$

holds for all $g \in \mathcal{G}$. Furthermore, there is an isomorphism of $\Bbbk[\mathcal{G}]$-modules

$$\big(V \otimes_{\Bbbk} V^{\theta}\big)^* \cong \{\text{sesquilinear forms } V \times V \longrightarrow \Bbbk \text{ with respect to } \theta\}\,. \tag{19}$$

The isomorphism sends a linear for $\varphi\colon V \otimes_{\Bbbk} V^{\theta} \longrightarrow \Bbbk$ to the form $\widetilde{\varphi}\colon V \times V \longrightarrow \Bbbk$ given by $\widetilde{\varphi}(v, w) = \varphi(v \otimes w^{\theta})$. The group $\mathcal{S}_2 = \langle\tau\rangle$ acts on the space of sesquilinear forms $\beta\colon V \times V \longrightarrow \Bbbk$ with respect to θ by

$$(\tau\beta)(v, w) = \beta(v, w)^{\theta}$$

for $v, w \in V$. This action commutes with the action of $\mathcal{G}$. Note however that the action is only $\Bbbk$-semilinear: $\tau(a\beta) = a^{\theta}\tau\beta$. Clearly, β is hermitian (resp. skew-hermitian) if and only if $\tau\beta = \beta$ (resp. $\tau\beta = -\beta$).

LEMMA 16. *Let $\sigma\colon \mathcal{G} \longrightarrow \mathrm{GL}(V)$ be an irreducible representation of the finite group $\mathcal{G}$. If $V^* \cong V^{\theta}$ as $\Bbbk[\mathcal{G}]$-modules then $\sigma(\mathcal{G}) \subseteq \mathrm{Iso}(V, \beta)$ for some non-singular form β on V that is hermitian or skew-hermitian with respect to θ.*

PROOF. Since $V^* \cong V^\theta$, we have $V^* \otimes_{\Bbbk} V \cong \left(V \otimes_{\Bbbk} V^\theta\right)^*$ and so

$$\mathrm{End}_{\Bbbk}(V) \cong \{\text{sesquilinear forms } V \times V \to \Bbbk \text{ with respect to } \theta\}$$

as $\Bbbk[\mathcal{G}]$-modules, by (19). The identity $\mathrm{Id}_V \in \mathrm{End}_{\Bbbk}(V)$ therefore corresponds to a non-zero $\mathcal{G}$-invariant sesquilinear form β. Write $\beta = \beta_+ + \beta_-$ with $\beta_\pm = \frac{1}{2}(1 \pm \tau)(\beta)$, where $\mathcal{S}_2 = \langle \tau \rangle$ as above. Then $\tau\beta_\pm = \pm\beta$; so β_+ is hermitian and β_- is skew-hermitian with respect to θ, and at least one of them is non-zero. Moreover, both $\beta_\pm$ are $\mathcal{G}$-invariant, since the actions of τ and $\mathcal{G}$ commute. Finally, any non-zero $\mathcal{G}$-invariant hermitian or skew-hermitian form on V is non-singular, because its radical is a proper $\Bbbk[\mathcal{G}]$-submodule of V, and hence it must be zero because V is assumed simple. □

5.5.3. *Isometry groups over finite fields.* We will now concentrate on the case of a finite field $\Bbbk = \mathbb{F}_q$ of order $q = p^f$ for some odd prime p. Let β be a non-singular hermitian or skew-hermitian form on $V \cong \mathbb{F}_q^n$. Since we are only interested in the group of isometries $\mathrm{Iso}(V, \beta)$, we may assume that β is unitary, orthogonal or symplectic. The orders of these groups are classical; see Dieudonné [14] or Artin [1, Section III.6], for example. The original sources are Minkowski's dissertation [32] and Dickson [13].

unitary case: Since θ has order 2 in this case, f must be even. Moreover, β is unique up to equivalence, and so $\mathrm{Iso}(V, \beta)$ is determined up to conjugation. The order of $\mathrm{Iso}(V, \beta)$ is

$$|\,\mathrm{Iso}(V,\beta)| = p^{fn(n-1)/4} \prod_{i=1}^{n} (p^{fi/2} - (-1)^i)\,. \tag{20}$$

symplectic case: Again, β is unique up to equivalence. The dimension n must be even. One has

$$|\,\mathrm{Iso}(V,\beta)| = q^{n^2/4} \prod_{i=1}^{n/2} (q^{2i} - 1)\,. \tag{21}$$

orthogonal case: Here, the order of $\mathrm{Iso}(V, \beta)$ is given by

$$|\,\mathrm{Iso}(V,\beta)| = \begin{cases} 2q^{(n-1)^2/4} \displaystyle\prod_{i=1}^{(n-1)/2} (q^{2i} - 1) & \text{if } n \text{ is odd,} \\ 2q^{n(n-2)/4}(q^{n/2} - \varepsilon) \displaystyle\prod_{i=1}^{(n-2)/2} (q^{2i} - 1) & \text{if } n \text{ is even,} \end{cases} \tag{22}$$

where $\varepsilon = \pm 1$ depends on the form β. The detailed description of ε will not matter for us.

LEMMA 17. *Let K be an algebraic number field contained in $\mathbb{Q}(\mu_{2^\infty})$ (so K is Galois over $\mathbb{Q}$ and in particular stable under complex conjugation). If $K \not\subseteq \mathbb{R}$ then assume that $t(K, 2) = 1$. There are infinitely many odd primes $\mathfrak{p}$ of the ring of algebraic integers $\mathcal{O}_K$ satisfying the following two conditions:*

(i) *$\mathfrak{p}$ is stable under complex conjugation, and*
(ii) *If β is any non-singular hermitian or skew-hermitian form on $V = \mathbb{F}_q^n$ with respect to the automorphism θ of $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$ that is afforded by complex conjugation then $|\,\mathrm{Iso}(V, \beta)|_2$ divides $S(n, K)_2$.*

PROOF. We will need the following elementary observation. If p is a prime satisfying $p \equiv -1 + 2^k \mod 2^{k+1}$ for some $k \geq 2$ then, for all positive integers i,

$$(p^i - (-1)^i)_2 = 2^k i_2 \,. \tag{23}$$

To see this, we remark first that $(p^i - 1)_2 = 2$ holds for odd$i$, because the residue class of p modulo 4 is the nonidentity element of $(\mathbb{Z}/4\mathbb{Z})^*$, and hence the same holds for all odd powers of p. Moreover, since $p^2 \equiv 1 \mod 2^{k+1}$, we have $p^i \equiv 1 \mod 2^{k+1}$ for all even i, and hence $(p^i + 1)_2 = 2$. Now, to prove (23), assume first that i is odd, say $i = 2j + 1$. Then the foregoing implies that $p^i - (-1)^i = p^{2j}p + 1 \equiv p + 1 \equiv 2^k \mod 2^{k+1}$, and so $(p^i - (-1)^i)_2 = 2^k$, proving (23) for odd values of i. Finally, assume that $i = 2j$. Then $p^i - (-1)^i = (p^j - 1)(p^j + 1)$. If j is odd then we know that $(p^j + 1)_2 = 2^k$ and $(p^j - 1)_2 = 2$, and hence $(p^i - (-1)^i)_2 = 2^{k+1}$, as desired. When j is even then $(p^j - 1)_2 = 2^k j_2$, by induction, and $(p^j + 1)_2 = 2$, as we remarked earlier. Thus, (23) is proved in all cases.

Turning to the proof of the lemma, note that $K/\mathbb{Q}$ is Galois, being a subextension of the abelian extension $\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}$. Put $m = m(K,2)$, $t = t(K,2)$ and $\zeta = \zeta_{2^m}$. Then (15) becomes

$$S(n,K)_2 = [K : \mathbb{Q}]^{\lfloor n/t \rfloor} 2^n (n!)_2$$

and K is one of the fields $\mathbb{Q}(\zeta)$ or $\mathbb{Q}(\zeta + \zeta^{-1})$; see §5.3. We will deal with each of these cases separately. Throughout, $\mathfrak{p}$ will denote a prime ideal of $\mathcal{O}_K$ and we put $q = \mathcal{N}(\mathfrak{p})$ and $(p) = \mathfrak{p} \cap \mathbb{Z}$.

First consider the case where K is real. Then property (i) is automatic and $\operatorname{Iso}(V,\beta)$ is symplectic or orthogonal. Replacing the factor $(q^{n/2} - \varepsilon)$ in formula (22) for even n by its multiple $(q^{n/2} - \varepsilon)(q^{n/2} + \varepsilon)/2 = (q^n - 1)/2$ and deleting q-factors (which are odd) we obtain the expression $\prod_{i=1}^{n/2}(q^{2i} - 1)$ that only depends on n and q and is identical to (21) stripped of its q-factors. Put

$$\mathfrak{o}(n,q) = \begin{cases} 2\displaystyle\prod_{i=1}^{(n-1)/2}(q^{2i} - 1) & \text{if } n \text{ is odd,} \\ \displaystyle\prod_{i=1}^{n/2}(q^{2i} - 1) & \text{if } n \text{ is even.} \end{cases}$$

Now $q = p^f$, where $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$ is a divisor of $[K : \mathbb{Q}]$; so f is a power of 2. Choose $\mathfrak{p}$ to lie over any rational prime p with $p \equiv 3 \mod 8$. Then (23) with $k = 2$ implies that the 2-part of $q^{2i} - 1$ for $i \geq 1$ is given by $\left(q^{2i} - 1\right)_2 = 8fi_2$. It follows that the 2-part of $\mathfrak{o}(n,q)$ can be written as $\mathfrak{o}(n,q)_2 = f^{\lfloor n/2 \rfloor} 2^n (n!)_2$ in both cases. Since f is a divisor of $[K : \mathbb{Q}]$ and t equals 1 or 2, we see that $\mathfrak{o}(n,q)_2$ divides $S(n,K)_2$ which settles the symplectic and orthogonal cases.

Next, let $K = \mathbb{Q}(\zeta)$ with $m \geq 2$. Choose $\mathfrak{p}$ to lie over any rational prime p satisfying $p \equiv -1 + 2^m \mod 2^{m+1}$. The $\mathfrak{p}$ is stable under complex conjugation. Indeed, the decomposition group of $\mathfrak{p}$ is generated by the automorphism of K sending ζ to ζ^p (cf., e.g., [**19**, Corollary on p. 197]), and our choice of p implies that $\zeta^p = \zeta^{-1} = \overline{\zeta}$. Thus, complex conjugation $\bar{\ }$ belongs to the decomposition group of $\mathfrak{p}$, and it must in fact generated the decomposition group, because $\bar{\ }$ is not a square in $\operatorname{Gal}(K/\mathbb{Q})$. Since $\mathfrak{p}$ is unramified over $\mathbb{Q}$, its relative degree over $\mathbb{Q}$ equals $f = 2$; so $q = p^2$. Therefore, (20) and (23) give

$$|\operatorname{Iso}(V,\beta)|_2 = \prod_{i=1}^{n}(p^i - (-1)^i)_2 = 2^{mn}(n!)_2 = 2^{(m-1)n}2^n(n!)_2 \,.$$

Since $[K:\mathbb{Q}] = 2^{m-1}$ and $t = 1$, the last expression is equal to $S(n,K)_2$, thereby completing the proof of the lemma. $\square$

The lemma fails in the excluded case $K \not\subseteq \mathbb{R}$, $t(K,2) = 2$. For example, let $K = \mathbb{Q}(\sqrt{-2})$. Then $m(K,2) = 3$ and $t(K,2) = 2$ and so $S(n,K)_2 = 2^{\lfloor \frac{n}{2} \rfloor} 2^n (n!)_2$. On the other hand, if $\mathfrak{p}$ is an odd prime of $\mathcal{O}_K$ that is stable under complex conjugation, then $f(\mathfrak{p}/\mathbb{Q}) = 2$ and $p \equiv -1 \mod 8$. It follows that $|\operatorname{Iso}(V,\beta)|_2 = \prod_{i=1}^n (p^i - (-1)^i)_2$ is divisible by 2^{3n} which is too big.

5.6. The prime $\ell = 2$. The following proposition complements Proposition 15. It would be nice to remove the restrictions $K' = K \cap \mathbb{Q}(\mu_{2^\infty}) \subseteq \mathbb{R}$ or $t(K,2) = 1$ on K. This would require replacing the isometry groups $\operatorname{Iso}(V,\beta)$ by suitable subgroups.

PROPOSITION 18. *Let $\mathcal{G}$ be a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ such that the traces of all elements of $\mathcal{G}$ belong to some fixed algebraic number field K. Assume that $K' = K \cap \mathbb{Q}(\mu_{2^\infty}) \subseteq \mathbb{R}$ or $t(K,2) = 1$. Then $|\mathcal{G}|_2$ divides $S(n,K)$.*

PROOF. We may assume that $\mathcal{G}$ is a 2-group. Therefore, $\operatorname{trace}(g) \in \mathcal{O}_{K'}$ for all $g \in \mathcal{G}$. Replacing K by K', we may assume that $K = K' \subseteq \mathbb{Q}(\mu_{2^\infty})$; see (17). Choose a prime $\mathfrak{p}$ of $\mathcal{O}_K$ as in Lemma 17 and put $q = \mathcal{N}(\mathfrak{p})$. As in the proof of Proposition 15, we can arrange that $\mathcal{G} \subseteq \mathrm{GL}_n(F)$ for some algebraic number field F containing K. Choose a prime $\mathfrak{P}$ of $\mathcal{O} = \mathcal{O}_F$ lying over $\mathfrak{p}$ and put $\Bbbk = \mathcal{O}/\mathfrak{P}$; so $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{p} \subseteq \Bbbk$. We may assume $\mathcal{G} \subseteq \mathrm{GL}_n(\mathcal{O}_\mathfrak{P})$ and that $(p) = \mathfrak{P} \cap \mathbb{Z}$ satisfies $p > n$. By Lemma 9, the reduction homomorphism $\mathrm{GL}_n(\mathcal{O}_\mathfrak{P}) \to \mathrm{GL}_n(\Bbbk)$ is injective on $\mathcal{G}$. We will write the restriction of this map to $\mathcal{G}$ as

$$\rho\colon \mathcal{G} \hookrightarrow \mathrm{GL}_n(\Bbbk)\,.$$

Then $\operatorname{trace}\rho(g) = \operatorname{trace} g \mod \mathfrak{p} \in \mathbb{F}_q \subseteq \Bbbk$ for $g \in \mathcal{G}$, and $\operatorname{trace}\rho(g^{-1}) = (\operatorname{trace}\rho(g))^\theta$, where θ denotes the automorphism of $\mathbb{F}_q$ that is afforded by complex conjugation, as in Lemma 17. Now Lemma 8 implies that $\rho(\mathcal{G})^v = v^{-1}\rho(\mathcal{G})v \subseteq \mathrm{GL}_n(\mathbb{F}_q)$ for some $v \in \mathrm{GL}_n(\Bbbk)$; so we may consider the representation

$$\sigma = (\,.\,)^v \circ \rho\colon \mathcal{G} \hookrightarrow \mathrm{GL}(V)\,,$$

where $V = \mathbb{F}_q^n$. Note that $\operatorname{trace}\sigma(g) = \operatorname{trace}\rho(g)$ for all $g \in \mathcal{G}$. We will write V as a direct sum of $\mathbb{F}_q[\mathcal{G}]$-submodules U_i on which $\mathcal{G}$ acts as a subgroup of $\operatorname{Iso}(U_i,\beta_i)$ for some non-singular hermitian or skew-hermitian form β_i with respect to θ on U_i. This will imply that $|\mathcal{G}|$ divides $\prod_i |\operatorname{Iso}(U_i,\beta_i)|_2$, and hence $|\mathcal{G}|$ divides $\prod_i S(\dim U_i, K)$ by Lemma 17. Since $\prod_i S(\dim U_i, K)$ is a divisor of $S(\sum_i \dim U_i, K) = S(n,K)$, by (16), the theorem will follow.

To achieve the decomposition of V, recall that $\operatorname{trace}\sigma(g^{-1}) = (\operatorname{trace}\sigma(g))^\theta$ for all $g \in \mathcal{G}$. By (18), this says that the $\mathbb{F}_q[\mathcal{G}]$-modules V^* and V^θ have the same character, and hence they are isomorphic; see the proof of Lemma 8. Write $V \cong \bigoplus_i V_i^{(n_i)}$ with non-isomorphic irreducible $\mathbb{F}_q[\mathcal{G}]$-modules V_i. Then $V^* \cong \bigoplus_i (V_i^*)^{(n_i)}$ and $V^\theta \cong \bigoplus_i \left(V_i^\theta\right)^{(n_i)}$. For each i, there is an i' so that $V_i^* \cong V_{i'}^\theta$. If $i = i'$ then Lemma 16 says that $\mathcal{G}$ acts on V_i as a subgroup of $\operatorname{Iso}(V_i,\beta_i)$ for some non-singular hermitian or skew-hermitian form β_i on V_i. Now assume that $i \neq i'$. Then $V_i^* \oplus V_i^\theta$ is a direct summand of V^θ, and hence $\widetilde{V}_i = (V_i^*)^\theta \oplus V_i$ is a direct summand of V. Defining

$$\beta_i(f^\theta + v, f'^\theta + v') = f(v')^\theta + f'(v)$$

for $f, f' \in V_i^*$ and $v, v' \in V_i$ we obtain a non-singular hermitian form on $\widetilde{V}_i$ that is preserved by the action of $\mathcal{G}$. This yields the desired decomposition of V and completes the proof of the theorem. □

6. Outlook

We conclude by surveying, without proofs, a number of topics that are related to the foregoing.

6.1. The largest groups and recent work on the Jordan bound.

6.1.1. The group $\mathcal{G}$ constructed in Proposition 4 is isomorphic to the so-called wreath product

$$\mathcal{S}_{m+1} \wr \mathcal{S}_a .$$

By definition, $\mathcal{S}_{m+1} \wr \mathcal{S}_a$ is the semidirect product of $\mathcal{S}_{m+1}^a \rtimes \mathcal{S}_a$, where $\mathcal{S}_a$ acts on $\mathcal{S}_{m+1}^a = \mathcal{S}_{m+1} \times \cdots \times \mathcal{S}_{m+1}$ by permuting the a factors $\mathcal{S}_{m+1}$. The special case $m = 1$ yields the group $\{\pm 1\} \wr \mathcal{S}_n$, a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ order $2^n n!$ which is also known as the automorphism group $\mathrm{Aut}(B_n)$ of the root system of type B_n; see **[3]**. For almost all values of n, these particular groups turn out to be the largest finite groups that can be found inside $\mathrm{GL}_n(\mathbb{Z})$, and even inside $\mathrm{GL}_n(\mathbb{Q})$ (see §5.2). Indeed, Feit **[16]** has shown that, for all $n > 10$ and for $n = 1, 3, 5$, the finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ of largest order are precisely the conjugates of $\mathrm{Aut}(B_n)$. For the remaining values of n, Feit also characterizes the largest finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ and shows that they are unique up to conjugacy. Feit's proof depends in an essential way on an unfinished manuscript of Weisfeiler **[46]** which establishes an estimate for the so-called Jordan bound; see § 6.1.2 below. An alternative proof of Feit's theorem for sufficiently large values of n has been given by Friedland **[18]** who relies on another (published) article of Weisfeiler's, **[47]**. Both **[46]** and **[47]** depend crucially on the classification of finite simple groups.

Sadly, the two protagonists of the developments sketched above are no longer with us: Walter Feit passed away on July 29, 2004 while Boris Weisfeiler disappeared in January 1985 during a hiking trip in the Chilean Andes. The present status of the investigation into Weisfeiler's disappearance is documented on the web site *http://www.weisfeiler.com/boris/*. For further information on the subject of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ and of $\mathrm{GL}_n(\mathbb{Q})$, especially maximal ones, see, e.g., Nebe and Plesken **[34]**, Plesken **[37]**, the first chapter of **[31]** and, at a more elementary level, the article **[27]** by Kuzmanovich and Pavlichenkov.

6.1.2. The Jordan bound comes from the following classical result **[24]**.

THEOREM 19 (Jordan 1878). *There exists a function $j \colon \mathbb{N} \to \mathbb{N}$ such that every finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ contains an abelian normal subgroup of index at most $j(n)$.*

Early estimates for the optimal function $j(n)$ were quite astronomical. Until fairly recently, the best known result was due to Blichfeldt: $j(n) \leq n!\, 6^{(n-1)(\pi(n+1)+1)}$, where $\pi(n+1)$ denotes the number of primes $\leq n+1$; see **[15**, Theorem 30.4**]**. Since $\mathcal{S}_{n+1} \subseteq \mathrm{GL}_n(\mathbb{C})$, as explained in the proof of Proposition 4, one must certainly have $j(n) \geq (n+1)!$ for $n \geq 4$. In his near-complete manuscript **[46]**, Weisfeiler comes close to proving that equality holds for large enough n: he shows that if $n > 63$ then $j(n) \leq (n+2)!$. In **[47]**, Weisfeiler announces the weaker upper bound $j(n) \leq n^{a \log n + b} n!$. Quite recently, Michael Collins **[11]** was able to settle the problem by showing that for $n \geq 71$ we do indeed have $j(n) = (n+1)!$ and, if this bound is achieved by $\mathcal{G}$, then $\mathcal{G}$ modulo its center is isomorphic to $\mathcal{S}_{n+1}$.

6.1.3. Analogs of Jordan's Theorem for linear groups in characteristics $p > 0$ were established by Weisfeiler [**46**], [**47**], Larsen and Pink [**30**], and Collins [**10**]. While both Weisfeiler and Collins rely on the classification theorem, Larsen and Pink prove a noneffective version of Jordan's theorem, without explicit index and degree bounds, by using methods from algebraic geometry and the theory of linear algebraic groups instead. We will explain Collins' modular version of Jordan's Theorem. As usual, $O_p(\mathcal{G})$ denotes the maximal normal p-subgroup of the finite group $\mathcal{G}$. Furthermore, a group is called *quasisimple* if it is perfect and simple modulo its center. Collins' result then reads as follows.

THEOREM 20 (Collins 2005). *Let F be a field of positive characteristic p and let $\mathcal{G}$ be a finite subgroup of* $\mathrm{GL}_n(F)$*, where $n \geq 71$. Put $G = \mathcal{G}/O_p(\mathcal{G})$. Then G has a normal subgroup N such that*

(a) *$N = A\,Q_1 \dots Q_m$, a central product with A abelian and the Q_i (quasi)simple Chevalley groups in characteristic p.*

(b) $[G : N] \leq \begin{cases} (n+2)! & \text{if } p \text{ divides } n+2, \\ (n+1)! & \text{otherwise.} \end{cases}$

6.2. The Minkowski sequence $M(n)$**.** A search of Sloane's *On-Line Encyclopedia of Integer Sequences* [**43**], by entering the first six terms $2, 24, 48, 5760, 11520, 2903040$ of $M(n)$, turns up a sequence labeled A053657. This sequence has two additional descriptions besides Minkowski's description of $M(n)$ as the least common multiple of the orders of all finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$; the other two will be given below. We know of no direct argument explaining the (proven) equivalence of $M(n)$ to the first sequence below. The equivalence of the second sequence to $M(n)$ is currently supported only by empirical evidence.

- By Chabert et. al. [**8**], the collection of all leading coefficients of polynomials $f(x) \in \mathbb{Q}[x]$ of degree at most n such that $f(p) \in \mathbb{Z}$ holds for all primes p is a fractional ideal of the form $\frac{1}{a(n)}\mathbb{Z}$ for suitable positive integers $a(n)$. It turns out that formula (1) is identical with the formula given in [**8**, Proposition 4.1] for $a(n+1)$. Thus $M(n-1) = a(n)$.
- Following Paul Hanna [**43**, A075264], we let $P(n,z)$ denote the coefficient of x^n in the Taylor series for $(\frac{-\ln(1-x)}{x})^z$ at $x = 0$. Thus, $\sum_{m=1}^{\infty} \binom{z}{m}\xi^m = \sum_{n=1}^{\infty} P(n,z)x^n$ with $\xi = \frac{-\ln(1-x)}{x} - 1 = \sum_{k=1}^{\infty} \frac{x^k}{k+1}$ and $\binom{z}{m} = \frac{z\dots(z-m+1)}{m!}$. For example, $P(1,z) = \frac{z}{2}$, $P(2,z) = \frac{5z+3z^2}{24}$, $P(3,z) = \frac{6z+5z^2+z^3}{48}$. In general, $P(n,z) \in z\mathbb{Q}[z]$; the polynomials $P(n,z)$ for $n \leq 8$ are listed in sequence A075264 of OEIS [**43**]. Paul Hanna has noted that the denominator of $P(n,z)$, that is, the positive generator of the ideal $\{q \in \mathbb{Z} \mid qP(n,z) \in \mathbb{Z}[z]\}$, appears to coincide with $M(n)$.

In [**33**], Minkowski states the following recursion for the sequence $M(n)$; the recursion is easy to check from (1):

$$M(2n+1) = 2\,M(2n) \qquad \text{and} \qquad M(2n) = 2\,M(2n-1) \prod_{p:\; p-1|2n} p n_p\,. \tag{24}$$

The product in (24) ranges over all primes p such that $p-1$ divides $2n$, and n_p denotes the p-part of n, as usual. This product has an interpretation in terms of the familiar *Bernoulli numbers* B_n which are defined by $\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$. In fact, $B_n = 0$ for odd $n > 1$ while B_{2n} is a rational number whose denominator, when written in lowest terms, is given by the von Staudt-Clausen theorem: it is equal to $\prod_{p:\; p-1|2n} p$; cf. [**7**, Theorem 1].

Moreover, for each prime p such that $p-1$ does not divide $2n$, the numerator of B_{2n} is divisible by the p-part n_p ; see [7, Theorem 5]. Consequently, the product $\prod_{p:\ p-1|2n} pn_p$ in (24) is equal to the denominator of $\frac{B_{2n}}{n}$. This was already pointed out by Minkowski in [33]. Finally, the asymptotic order of M_n has been determined by Katznelson [25]: $\lim_{n\to\infty}(M(n)/n!)^{1/n} = \prod_p p^{1/(p-1)^2} \approx 3.4109$.

ACKNOWLEDGMENT. The authors wish to thank Boris Datskovsky, Ed Letzter and Jean-Pierre Serre for their comments on a preliminary version of this article, and Michael Collins for making drafts of [9],[10],[11] available to them.

References

[1] Emil Artin, *Geometric algebra*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1988, Reprint of the 1957 original, A Wiley-Interscience Publication. MR 90h:51003

[2] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR 92d:20001

[3] Nicolas Bourbaki, *Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968. MR 39 #1590

[4] ———, *Éléments de mathématique. Fasc. XXXVII. Groupes et algèbres de Lie. Chapitre II: Algèbres de Lie libres. Chapitre III: Groupes de Lie*, Hermann, Paris, 1972, Actualités Scientifiques et Industrielles, No. 1349. MR 58 #28083a

[5] ———, *Éléments de mathématique, Fasc. XXIII*, Hermann, Paris, 1973, Livre II: Algèbre. Chapitre 8: Modules et anneaux semi-simples, Nouveau tirage de l'édition de 1958, Actualités Scientifiques et Industrielles, No. 1261. MR 54 #5282

[6] W. Burnside, *Theory of groups of finite order*, Dover Publications Inc., New York, 1955, 2d ed. MR 16,1086c

[7] Leonard Carlitz, *Bernoulli numbers*, Fibonacci Quart **6** (1968), no. 3, 71–85. MR 38 #1071

[8] Jean-Luc Chabert, Scott T. Chapman, and William W. Smith, *A basis for the ring of polynomials integer-valued on prime numbers*, Factorization in integral domains (Iowa City, IA, 1996), Lecture Notes in Pure and Appl. Math., vol. 189, Dekker, New York, 1997, pp. 271–284. MR 99d:13008

[9] Michael Collins, *Bounds for finite primitive complex linear groups*, preprint, University of Oxford, 30 pages, 2005.

[10] ———, *Modular analogues of Jordan's theorem for finite linear groups*, preprint, University of Oxford, 43 pages, 2005.

[11] ———, *On Jordan's theorem for complex linear groups*, preprint, University of Oxford, 18 pages, 2005.

[12] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons Inc., New York, 1981, With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication. MR 82i:20001

[13] Leonard Eugene Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publications Inc., New York, 1958, unaltered republication of the first edition [Teubner, Leipzig, 1901] with a new introduction by Wilhelm Magnus. MR 21 #3488

[14] Jean A. Dieudonné, *La géométrie des groupes classiques*, Springer-Verlag, Berlin, 1971, Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5. MR 46 #9186

[15] Larry Dornhoff, *Group representation theory. Part A: Ordinary representation theory*, Marcel Dekker Inc., New York, 1971, Pure and Applied Mathematics, 7. MR 50 #458a

[16] Walter Feit, *Orders of finite linear groups*, unpublished preprint, approx. 1998.

[17] Walter Feit, *Finite linear groups and theorems of Minkowski and Schur*, Proc. Amer. Math. Soc. **125** (1997), no. 5, 1259–1262. MR 97g:20007

[18] Shmuel Friedland, *The maximal orders of finite subgroups in* $\mathrm{GL}_n(\mathbf{Q})$, Proc. Amer. Math. Soc. **125** (1997), no. 12, 3519–3526. MR 98b:20064

[19] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 92e:11001

[20] I. Martin Isaacs, *Character theory of finite groups*, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976, Pure and Applied Mathematics, No. 69. MR 57 #417

[21] Nathan Jacobson, *Basic algebra. I*, second ed., W. H. Freeman and Company, New York, 1985. MR 86d:00001

[22] ———, *Basic algebra. II*, second ed., W. H. Freeman and Company, New York, 1989. MR 90m:00007

[23] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR 96j:11137

[24] Camille Jordan, *Mémoire sur les équations différentielles linéaires à intégrale algébrique*, J. Reine Angew. Math. **84** (1878), 89–215.

[25] Yonatan R. Katznelson, *On the orders of finite subgroups of* $\mathrm{GL}(n, \mathbb{Z})$, Exposition. Math. **12** (1994), 453–457.

[26] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits. MR 2000a:16031

[27] James Kuzmanovich and Andrey Pavlichenkov, *Finite groups of matrices whose entries are integers*, Amer. Math. Monthly **109** (2002), no. 2, 173–186. MR 2003c:20057

[28] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR 19,174a

[29] ———, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 2003e:00003

[30] Michael Larsen and Richard Pink, *Finite subgroups of algebraic groups*, preprint, 61 pages, 1998.

[31] Martin Lorenz, *Multiplicative invariant theory*, Encyclopaedia of Mathematical Sciences, vol. 135, Springer-Verlag, Berlin, 2005, Invariant Theory and Algebraic Transformation Groups, VI.

[32] Hermann Minkowski, *Untersuchungen über quadratische Formen. Bestimmung der Anzahl verschiedener Formen, welche ein gegebenes Genus enthält*, Acta Mathematica **7** (1885), 201–258.

[33] ———, *Zur Theorie der positiven quadratische Formen*, J. reine angew. Math. **101** (1887), 196–202.

[34] Gabriele Nebe and Wilhelm Plesken, *Finite rational matrix groups*, Mem. Amer. Math. Soc. **116** (1995), no. 556, viii+144. MR 95k:20081

[35] Donald S. Passman, *Infinite group rings*, Marcel Dekker Inc., New York, 1971, Pure and Applied Mathematics, 6. MR 47 #3500

[36] ———, *The algebraic structure of group rings*, Wiley-Interscience [John Wiley & Sons], New York, 1977, Pure and Applied Mathematics. MR 81d:16001

[37] Wilhelm Plesken, *Some applications of representation theory*, Representation theory of finite groups and finite-dimensional algebras (Bielefeld, 1991), Progr. Math., vol. 95, Birkhäuser, Basel, 1991, pp. 477–496. MR 92k:20019

[38] Joseph J. Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR 95m:20001

[39] Issai Schur, *Über eine Klasse von endlichen Gruppen linearer Substitutionen*, Sitzungsber. Preuss. Akad. Wiss. (1905), 77–91.

[40] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7. MR 49 #8956

[41] ———, *Arithmetic groups*, Homological group theory (Proc. Sympos., Durham, 1977), London Math. Soc. Lecture Note Ser., vol. 36, Cambridge Univ. Press, Cambridge, 1979, pp. 105–136. MR 82b:22021

[42] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 82e:12016

[43] Neil J. A. Sloane, *The on-line encyclopedia of integer sequences*, 2005, published electronically at `http://www.research.att.com/~njas/sequences/`.

[44] Andreas Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Zeitschrift **5** (1919), 1–6.

[45] Joseph H. M. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), 349–352.

[46] Boris Weisfeiler, *On the size and structure of finite linear groups*, unfinished manuscript.

[47] ———, *Post-classification version of Jordan's theorem on finite linear groups*, Proc. Nat. Acad. Sci. U.S.A. **81** (1984), no. 16, Phys. Sci., 5278–5279. MR 85j:20041

DEPT. OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-1113
E-mail address: `guralnick@usc.edu`

DEPT. OF MATHEMATICS, TEMPLE UNIVERSITY, PHILADELPHIA, PA 19122-6094
E-mail address: `lorenz@temple.edu`