Orders of Finite Groups of Matrices

Séminaire AGATA Montpellier 06/08/2006
2^{nd} talk

Martin Lorenz

Temple University

Philadelphia

Overview

- **Two classical results**: Theorems of Minkowski and Schur

Overview

- **Two classical results**: Theorems of Minkowski and Schur
- A "new" proof of Schur's Theorem

Overview

- **Two classical results**: Theorems of Minkowski and Schur
- A "new" proof of Schur’s Theorem
- The Minkowski sequence: two mysteries

Overview

- **Two classical results**: Theorems of Minkowski and Schur
- A "new" proof of Schur's Theorem
- The Minkowski sequence: two mysteries
- Survey of some recent related work

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Here $\lfloor \quad \rfloor$ is the greatest integer ("floor") function

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

The ℓ-factor for $\ell > n+1$ equals 1; so the product is finite. E.g.,

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

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

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Using the identity $(m!)_\ell = \ell^{\left\lfloor \frac{m}{\ell} \right\rfloor + \left\lfloor \frac{m}{\ell^2} \right\rfloor + \cdots}$, one can write the ℓ-factor as

ℓ-part

$$M(n)_\ell = \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor} \left(\left\lfloor \frac{n}{\ell-1} \right\rfloor ! \right)_\ell$$

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Recursion: $M(2n+1) = 2\,M(2n)$

$$M(2n) = 2\,M(2n-1) \prod_{\ell \text{ prime, } \ell-1|2n} \ell n_\ell$$

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Recursion: $M(2n+1) = 2\,M(2n)$

$$M(2n) = 2\,M(2n-1) \underbrace{\prod_{\ell \text{ prime},\ \ell-1|2n} \ell n_\ell}_{= \text{ denominator of } \frac{B_{2n}}{n}}$$

Bernoulli numbers: $\frac{x}{e^x-1} = \sum_{n\geq 0} \frac{B_n x^n}{n!}$

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

More on the Minkowski numbers $M(n)$ later . . .

Large Matrix Groups

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

Large Matrix Groups

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

- Embed the symmetric group $\mathcal{S}_{m+1} \hookrightarrow \mathrm{GL}_m(\mathbb{Z})$ via its action on the "root lattice" (same as in the first talk)

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

Large Matrix Groups

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

- Hence,

$$\mathcal{S}_{m+1}^a \cong \left\{ \begin{pmatrix} \boxed{\mathcal{S}_{m+1}} & & & \\ & \boxed{\mathcal{S}_{m+1}} & & \\ & & \ddots & \\ & & & \boxed{\mathcal{S}_{m+1}} \end{pmatrix}_{a \times a} \right\} \hookrightarrow \mathrm{GL}_{am}(\mathbb{Z})$$

Large Matrix Groups

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

- Furthermore,

$$\mathcal{S}_a \cong \left\{ \left(\begin{array}{c|c|c|c|c|c} & 1_{m\times m} & \cdots & & & \\ \hline & & \cdots & & 1_{m\times m} & \\ \hline & & \ddots & & & \\ \hline & & \cdots & 1_{m\times m} & & \end{array} \right)_{a\times a} \right\} \hookrightarrow \mathrm{GL}_{am}(\mathbb{Z})$$

Large Matrix Groups

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

- $\mathcal{S}_{m+1}^a$ and $\mathcal{S}_a$ together generate a subgroup $\mathcal{G} \cong \mathcal{S}_{m+1} \wr \mathcal{S}_a$ of the desired order inside $\mathrm{GL}_{am}(\mathbb{Z})$, and

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

This completes the construction.

Large Matrix Groups

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

$$\Downarrow$$

Fix a prime $\ell \leq n+1$ and take $m = \ell - 1$ and $a = \left\lfloor \frac{n}{\ell-1} \right\rfloor$.
Get a subgroup $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Z})$ of order $\ell!^{\,a}\, a!$; so

$$|\mathcal{G}|_\ell = \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor} \left(\left\lfloor \frac{n}{\ell-1} \right\rfloor ! \right)_\ell = M(n)_\ell$$

Large Matrix Groups

Hence, the main content of Minkowski's Theorem is:

$M(n)$ is a multiple of the order of any finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{Q})$

Large Matrix Groups

Hence, the main content of Minkowski's Theorem is:

$M(n)$ *is a multiple of the order of any finite subgroup* $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{Q})$

In fact, much more is true . . .

Schur's Theorem

Schur (1905): $M(n)$ *is also a multiple of the order of any finite subgroup* $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ *such that* $\mathrm{tr}(g) \in \mathbb{Q}$ *for all* $g \in \mathcal{G}$*.*

Schur's Theorem

Schur (1905): $M(n)$ *is also a multiple of the order of any finite subgroup* $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ *such that* $\mathrm{tr}(g) \in \mathbb{Q}$ *for all* $g \in \mathcal{G}$.

Remark 1 Schur's Theorem covers a much wider class of groups than Minkowski's:

there are many finite subgroups $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(g) \in \mathbb{Q}$ holds for all $g \in \mathcal{G}$ yet no conjugate of $\mathcal{G}$ is even contained in $\mathrm{GL}_n(\mathbb{R})$. $\rightsquigarrow$ "Frobenius-Schur indicator"

Schur's Theorem

Schur (1905): $M(n)$ *is also a multiple of the order of any finite subgroup* $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ *such that* $\mathrm{tr}(g) \in \mathbb{Q}$ *for all* $g \in \mathcal{G}$*.*

Remark 2 Schur's proof is completely different from Minkowski's:

- Schur uses the theory of characters and induced representations (Blichfeldt).
- Minkowski relies on basic facts from number theory and quadratic forms.

Proof of Schur's Theorem

with **Bob Guralnick**

arXiv: math.GR/0511191

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Want: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$ for all primes ℓ

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Preliminary observations:

- Actually, $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Z}$ since traces are algebraic integers.

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Preliminary observations:

- Actually, $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Z}$ since traces are algebraic integers.
- Replacing $\mathcal{G}$ by a conjugate in $\mathrm{GL}_n(\mathbb{C})$, we can assume

$$\mathcal{G} \subseteq \mathrm{GL}_n(F)$$

for some algebraic number field F: any splitting field for $\mathcal{G}$ that is finite over $\mathbb{Q}$ will do.

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Preliminary observations: algebraic integers of F

- If $a \in \mathcal{O} = \mathcal{O}_F$ is a common denominator for all matrix entries of all elements of $\mathcal{G}$ then $\mathcal{G} \subseteq \mathrm{GL}_n(\mathcal{O}[1/a])$; so

$$\mathcal{G} \subseteq \mathrm{GL}_n(\mathcal{O}_{\mathfrak{p}})$$

for any prime $\mathfrak{p}$ of $\mathcal{O}$ not containing a.

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus:

- $\mathcal{G} \subset \mathrm{GL}_n(\mathcal{O}_{\mathfrak{p}})$ for some ring of algebraic integers $\mathcal{O}$ and almost all primes $\mathfrak{p}$ of $\mathcal{O}$
- $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Z}$

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus:

- $\mathcal{G} \subset \mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ for some ring of algebraic integers $\mathcal{O}$ and almost all primes $\mathfrak{p}$ of $\mathcal{O}$
- $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Z}$

Easy: If $0 \neq \mathfrak{p}$ with $|\mathcal{G}| \notin \mathfrak{p}$ then the **reduction map** $\mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathbb{F}_q$ for GL_n yields

$q = \mathcal{N}(\mathfrak{p}) = p^f$

$$\rho \colon \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{F}_q) \quad \text{(mono!)}$$

$$\mathrm{tr} \circ \rho \colon \mathcal{G} \to \mathbb{F}_p \subset \mathbb{F}_q$$

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus, for almost all primes $\mathfrak{p}$ of $\mathcal{O}$,

- $\rho\colon \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{F}_q)$
- $\mathrm{tr} \circ \rho\colon \mathcal{G} \longrightarrow \mathbb{F}_p \subset \mathbb{F}_q$

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus, for almost all primes $\mathfrak{p}$ of $\mathcal{O}$,

- $\rho\colon \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{F}_q)$
- $\mathrm{tr} \circ \rho\colon \mathcal{G} \to \mathbb{F}_p \subset \mathbb{F}_q$

Lemma: *Let $\mathcal{H} \subset \mathrm{GL}_n(\mathbb{F}_q)$, where $q = p^f$, $p \nmid |\mathcal{H}|$ and $p > n$. If $\mathrm{tr}(\mathcal{H}) \subset K \subset \mathbb{F}_q$ then $\mathcal{H} \subset \mathrm{GL}_n(K)$ up to conjugation.*

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus, for almost all primes $\mathfrak{p}$ of $\mathcal{O}$,

- $\rho \colon \mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{F}_q)$
- $\mathrm{tr} \circ \rho \colon \mathcal{G} \longrightarrow \mathbb{F}_p \subset \mathbb{F}_q$

Lemma: *Let* $\mathcal{H} \subset \mathrm{GL}_n(\mathbb{F}_q)$*, where* $q = p^f$, $p \nmid |\mathcal{H}|$ *and* $p > n$*. If* $\mathrm{tr}(\mathcal{H}) \subset K \subset \mathbb{F}_q$ *then* $\mathcal{H} \subset \mathrm{GL}_n(K)$ *up to conjugation.*

This follows from

- Wedderburn's thm on finite division rings, or
- Hilbert's Thm 90 for GL_n (Speiser 1919), or
- Lang's thm on algebraic groups over finite fields.

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus, for almost all rat'l primes p,

$$\boxed{\mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)}$$

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus, for almost all rat'l primes p,

$$\boxed{\mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)}$$

Minkowski: *Let $\ell \neq 2$ be prime. Then $|\,\mathrm{GL}_n(\mathbb{F}_p)|_\ell = M(n)_\ell$ holds for infinitely many primes p.*

Sketch: The unit group $(\mathbb{Z}/\ell^2\mathbb{Z})^*$ is cyclic. Moreover, by Dirichlet's theorem on primes in arithmetic progression, the residue class modulo ℓ^2 of any generator of $(\mathbb{Z}/\ell^2\mathbb{Z})^*$ contains infinitely many primes p. Any such prime will work.

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

Thus, for almost all rat'l primes p,

$$\boxed{\mathcal{G} \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)}$$

Minkowski: *Let $\ell \neq 2$ be prime. Then $|\mathrm{GL}_n(\mathbb{F}_p)|_\ell = M(n)_\ell$ holds for infinitely many primes p.*

$$\Downarrow$$

$|\mathcal{G}|_\ell$ divides $M(n)_\ell$, as desired

Proof of Schur's Theorem

Given: a finite subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{C})$ such that $\mathrm{tr}(\mathcal{G}) \subset \mathbb{Q}$.

- The prime $\ell = 2$ needs more work: $\mathrm{GL}_n(\mathbb{F}_p)$ is too big and must be replaced by suitable orthogonal and symplectic groups.
- A similar argument works for a number field K rather than $\mathbb{Q}$, with $M(n)$ replaced by a constant $S(n, K)$ defined by Schur.

Minkowski's sequence $M(n)$

Next: Two mysteries . . .

Minkowski's sequence $M(n)$

Entering the first six terms of $M(n)$,

$$2, 24, 48, 5760, 11520, 2903040$$

into Sloane's *On-Line Encyclopedia of Integer Sequences* brings up sequence **A053657**.

Minkowski's sequence $M(n)$

A053657 has two alternative descriptions . . .

Sequence $M(n)$ – First Alternative

- **Chabert et. al. (1997):** Consider polynomials $f(x) \in \mathbb{Q}[x]$ of degree at most n such that $f(p) \in \mathbb{Z}$ holds for all primes p.

Sequence $M(n)$ – First Alternative

- **Chabert et. al. (1997):** Consider polynomials $f(x) \in \mathbb{Q}[x]$ of degree at most n such that $f(p) \in \mathbb{Z}$ holds for all primes p.

The leading coefficients of these polynomials form a fractional ideal of the form $\frac{\mathbb{Z}}{a(n)}$ for suitable $a(n) \in \mathbb{Z}_{>0}$.

Sequence $M(n)$ – First Alternative

- **Chabert et. al. (1997):** Consider polynomials $f(x) \in \mathbb{Q}[x]$ of degree at most n such that $f(p) \in \mathbb{Z}$ holds for all primes p.

The leading coefficients of these polynomials form a fractional ideal of the form $\frac{\mathbb{Z}}{a(n)}$ for suitable $a(n) \in \mathbb{Z}_{>0}$.

Minkowski's formula is identical with the one **proved** for $a(n+1)$; so

$$a(n+1) = M(n) \ .$$

Sequence $M(n)$ – First Alternative

- **Chabert et. al. (1997):** Consider polynomials $f(x) \in \mathbb{Q}[x]$ of degree at most n such that $f(p) \in \mathbb{Z}$ holds for all primes p.

The leading coefficients of these polynomials form a fractional ideal of the form $\frac{\mathbb{Z}}{a(n)}$ for suitable $a(n) \in \mathbb{Z}_{>0}$.

Minkowski's formula is identical with the one **proved** for $a(n+1)$; so

$$a(n+1) = M(n) \ .$$

I know of no direct argument explaining this equality.

Sequence $M(n)$ – Second Alternative

- **Paul Hanna (2002):** Let $P(n,z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $(\frac{-\ln(1-x)}{x})^z$.

Sequence $M(n)$ – Second Alternative

- **Paul Hanna (2002):** Let $P(n,z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $(\frac{-\ln(1-x)}{x})^z$.

OEIS, sequence **A075264**:

$$P(1,z) = \frac{z}{2}$$

$$P(2,z) = \frac{5z+3z^2}{24}$$

$$P(3,z) = \frac{6z+5z^2+z^3}{48}$$

$$\ldots$$

Sequence $M(n)$ – Second Alternative

- **Paul Hanna (2002):** Let $P(n, z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $(\frac{-\ln(1-x)}{x})^z$.

Experimental evidence suggests that always

$$\text{denominator of } P(n, z) = M(n)$$

Sequence $M(n)$ – Second Alternative

- **Paul Hanna (2002):** Let $P(n, z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $(\frac{-\ln(1-x)}{x})^z$.

Experimental evidence suggests that always

$$\text{denominator of } P(n, z) = M(n)$$

No proof has been worked out yet!

Survey: large matrix groups (again)

$\mathrm{GL}_n(\mathbb{Z})$ contains the group of "monomial matrices", a special case of the construction explained earlier:

$$\mathcal{W}(B_n) = \mathbf{O}_n(\mathbb{Z}) = \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} \rtimes \mathcal{S}_n$$

Survey: large matrix groups (again)

$\mathrm{GL}_n(\mathbb{Z})$ contains the group of "monomial matrices", a special case of the construction explained earlier:

$$\mathcal{W}(B_n) = \mathbf{O}_n(\mathbb{Z}) = \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} \rtimes \mathcal{S}_n$$

Feit (unpubl., $\approx$ 1998): $|\mathcal{W}(B_n)| = 2^n n!$ *is the largest order of any finite subgroup of* $\mathrm{GL}_n(\mathbb{Q})$ *for* $n > 10$ *and for* $n = 1, 3, 5$*.*

Moreover, $\mathcal{W}(B_n)$ *is the unique subgroup of that order, up to conjugacy.*

Survey: large matrix groups (again)

Feit relies on an unfinished manuscript of **Weisfeiler** on the "Jordan bound" (based on the Classification Theorem).

Survey: large matrix groups (again)

Feit relies on an unfinished manuscript of **Weisfeiler** on the "Jordan bound" (based on the Classification Theorem).

Walter Feit
July 29, 2004

Survey: large matrix groups (again)

Feit relies on an unfinished manuscript of **Weisfeiler** on the "Jordan bound" (based on the Classification Theorem).

Boris Weisfeiler has been missing in Chile since January 4, 1985 (`http://boris.weisfeiler.com`)

Survey: Jordan bound

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

Survey: Jordan bound

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

Until fairly recently, the best known estimate was due to Blichfeldt ($\approx$ 1917):

$$j(n) \leq n!\, 6^{(n-1)(\pi(n+1)+1)}$$

the number of primes $\leq n+1$

Survey: Jordan bound

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

On the other hand, since $\mathcal{S}_{n+1} \hookrightarrow \mathrm{GL}_n(\mathbb{C})$,

$$j(n) \geq (n+1)!$$

Survey: Jordan bound

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

Weisfeiler's aforementioned manuscript shows

$$j(n) \leq (n+2)! \quad \text{if } n > 63$$

Survey: Jordan bound

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

The problem of determining $j(n)$ now has been settled:

Michael Collins (preprint 2005): $j(n) = (n+1)!$ *provided* $n \geq 71$*. Moreover, if this bound is achieved by* $\mathcal{G}$ *then* $\mathcal{G}$ *modulo its center is isomorphic to* $\mathcal{S}_{n+1}$*.*

Survey: Jordan bound