Calculations With Matrix Groups Over Rings And Applications To Arithmetic Groups

Alexander Hulpke
Department of Mathematics
Colorado State University
Fort Collins, CO, 80523, USA
www.hulpke.com

Groups St Andrews, Birmingham, August '17

Matrix Group Calculations

Matrix groups over commutative ring (here: $\mathbb{Z}$), given by (finite number) of generating matrices.

What can we say about such groups?

Over finite fields: ***matrix group recognition***

Uses: Divide-and-conquer approach. Data structure ***composition tree***. Reduction to simple groups.

Effective Homomorphisms, recursion to kernel, image.

Matrix Group Calculations

Matrix groups over commutative ring (here: $\mathbb{Z}$), given by (finite number) of generating matrices.

What can we say about such groups?

Finite Quotients key to computability

Over finite fields: ***matrix group recognition***

Uses: Divide-and-conquer approach. Data structure ***composition tree***. Reduction to simple groups.

Effective Homomorphisms, recursion to kernel, image.

Matrix Groups Over $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$

First consider $m=p^2$. ($m=p^a$ ditto iterated.)

Reduction mod p gives hom. φ: $\mathrm{SL}_n(\mathbb{Z}_m) \to \mathrm{SL}_n(\mathbb{Z}_p)$.

Kernel $\{I+pA \mid A \in \mathbb{Z}_p^{n\times n}\}$. Note: $\det(I+pA)=1+p\cdot\mathrm{Tr}(A)$.

Multiplication by addition of the A-parts modulo p.

$(I+pA)(I+pB)=I+p(A+B)+p^2\ldots\equiv I+p(A+B) \bmod m$

(Under map $A\mapsto I+pA$, $\ker\varphi$ is LIE-adjoint module)

Multiple primes: Subdirect product

```
gap> LoadPackage("matgrp"); # available for GAP 4.8.3
    […]
gap> g:=SL(3,Integers mod 1040);
SL(3,Z/1040Z)
gap> ff:=FittingFreeLiftSetup(g);;
gap> Size(g);
849852961151281790976000
gap> Collected(RelativeOrders(ff.pcgs));
[ [ 2, 24 ], [ 3, 1 ] ]
gap> m:=MaximalSubgroupClassReps(g);;time;
24631 #24 seconds
gap> List(m,x->Size(g)/Size(x));
[ 256, 7, 7, 8, 183, 183, 938119, 1476384, 3752476,
  123708, 123708, 123708, 31, 31, 3100, 3875, 4000 ]
```

Arithmetic Groups

Roughly: Discrete subgroup of Lie Group, defined by arithmetic properties on matrix entries(e.g. det=1, preserve form).

Definition: G linear algebraic group, over number field K. An ***arithmetic group*** is $\Gamma < G$, such that for integers $\mathcal{O}_K$ the intersection $\Gamma \cap G(\mathcal{O})$ has finite index in both intersectants.

Prototype: Subgroups of $SL_n(\mathbb{Z})$, $Sp_{2n}(\mathbb{Z})$ of finite index.

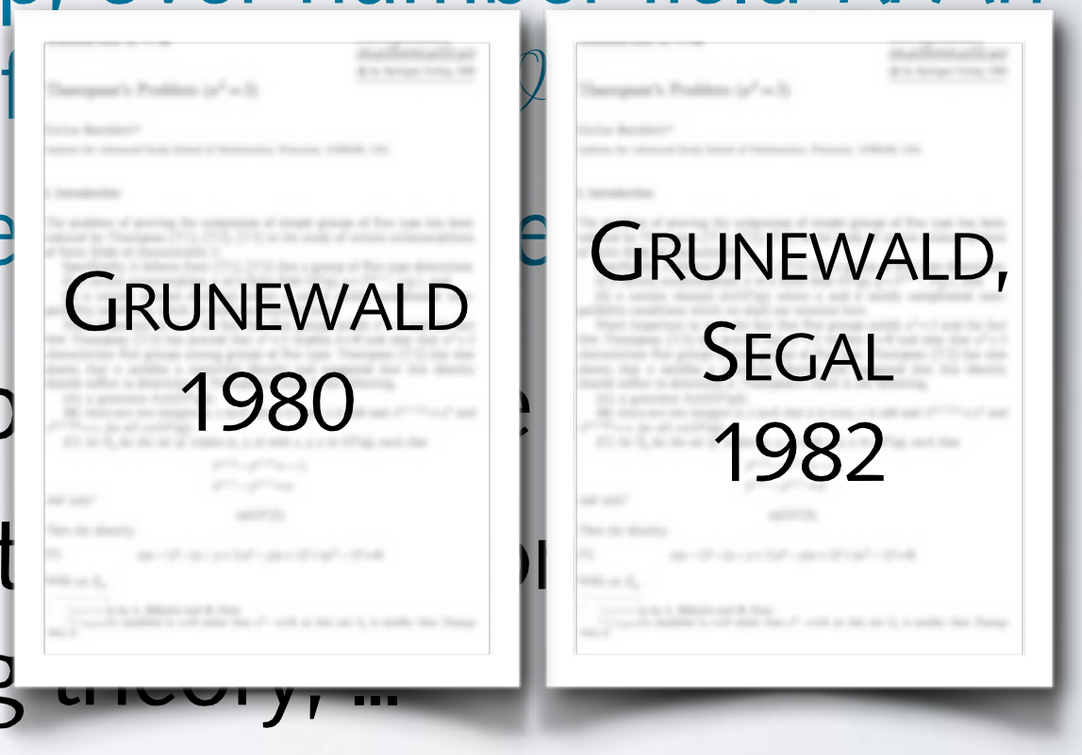
Applications: Number Theory (Automorphic Forms), Topology, Expander Graphs, String theory, ...

Theoretical algorithms for problems, such as conjugacy, known, but infeasible in practice.

Arithmetic Groups

Roughly: Discrete subgroup of Lie Group, defined by arithmetic properties on matrix entries(e.g. det=1, preserve form).

Definition: G linear algebraic group, over number field K. An *arithmetic group* is $\Gamma < G$, such that f… intersection $\Gamma \cap G(\mathcal{O})$ has finite inde…



Prototype: Subgroups of $SL_n(\mathbb{Z})$, Sp…

Applications: Number Theory (Aut… Topology, Expander Graphs, String theory, …

Theoretical algorithms for problems, such as conjugacy, known, but infeasible in practice.

Subgroups Of $SL_n(\mathbb{Z})$, $Sp_{2n}(\mathbb{Z})$

Take subgroup $G < SL_n(\mathbb{Z})$ (or Sp_{2n}) given by finite set of generators. G is arithmetic if it has finite index.

- Can we determine whether G has finite index?
- If G has finite index, can we determine it?

Here: Only SL case. SP similar. Others in work.

Joint work with ALLA DETINKO,
DANE FLANNERY
(St. Andrews / NUI Galway).

Subgroups Of $SL_n(\mathbb{Z})$, $Sp_{2n}(\mathbb{Z})$

Free subgroups, in general impossible, but Coset Enumeration may succeed in unbounded time.

- Can we determine whether G has finite index?
- If G has finite index, can we determine it?

Here: Only SL case. SP similar. Others in work.

Joint work with Alla Detinko,
Dane Flannery
(St. Andrews / NUI Galway).

Subgroups Of $SL_n(\mathbb{Z})$, $Sp_{2n}(\mathbb{Z})$

Take subgroup $G < SL_n(\mathbb{Z})$ (or Sp_{2n}) given by finite set of generators. G is arithmetic if it has finite index.

- Can we determine whether G has finite index?
- If G has finite index, can we determine it?

Here: Only SL case. SP similar. Others in work.

Joint work with ALLA DETINKO,
DANE FLANNERY
(St. Andrews / NUI Galway).

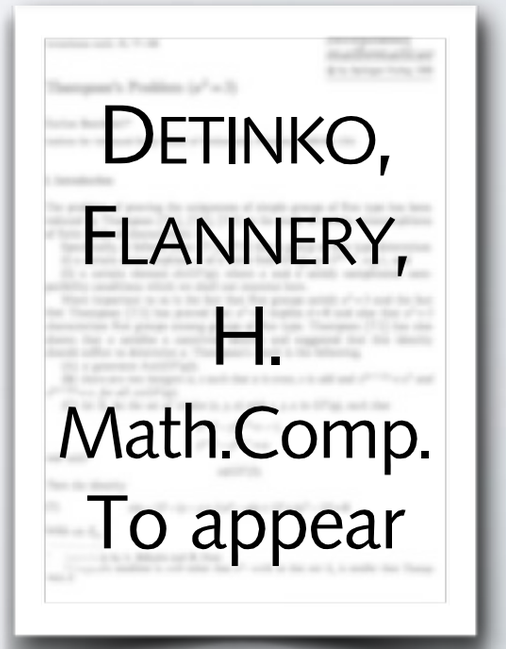
Subgroups Of $SL_n(\mathbb{Z})$, $Sp_{2n}(\mathbb{Z})$

Take subgroup $G < SL_n(\mathbb{Z})$ (or Sp_{2n}) given by finite set of generators. G is arithmetic if it has finite index.

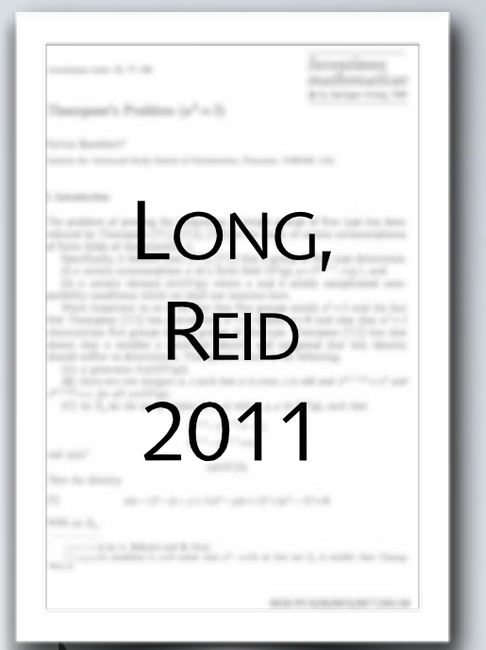
- Can we determine whether G has finite index?
- If G has finite index, can we determine it?

Here: Only SL case. SP similar. Others in work.

Joint work with ALLA DETINKO,
DANE FLANNERY
(St. Andrews / NUI Galway).



Easy Example

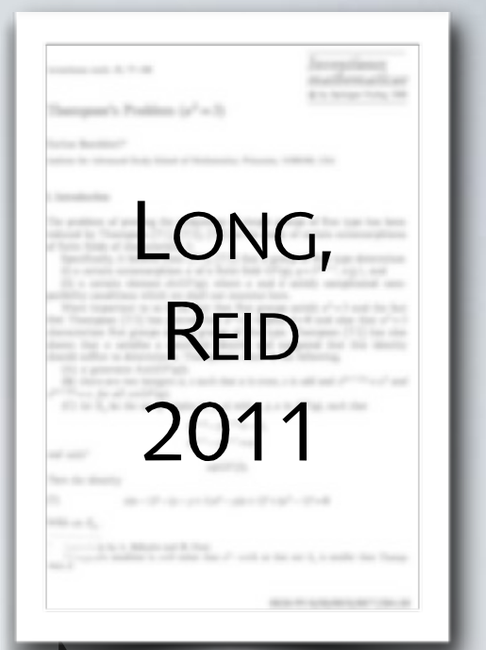


Let $SL_3(\mathbb{Z}) \geqq \beta_T =$

$$\left\langle \begin{pmatrix} -1+T^3 & -T & T^2 \\ 0 & -1 & 2T \\ -T & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ -T^2 & 1 & -T \\ T & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & T^2 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle,$$

then $[SL_3(\mathbb{Z}): \beta_{-2}]=3670016$.

Easy Example



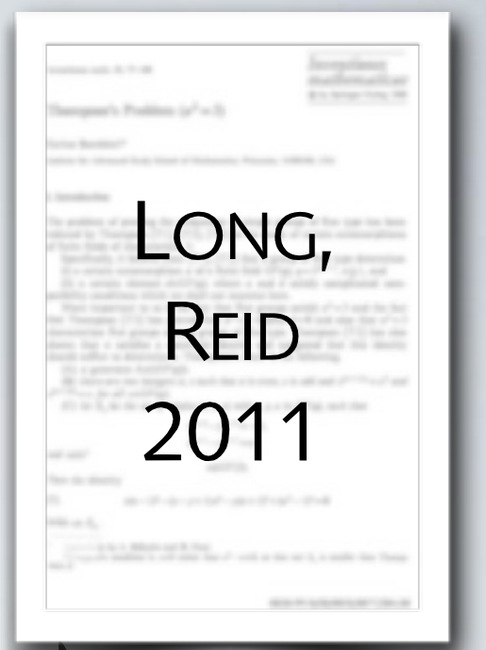
Let $SL_3(\mathbb{Z}) \trianglerighteq \beta_T =$

$$\left\langle \begin{pmatrix} -1+T^3 & -T & T^2 \\ 0 & -1 & 2T \\ -T & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ -T^2 & 1 & -T \\ T & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & T^2 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle,$$

then $[SL_3(\mathbb{Z}): \beta_{-2}] = 3670016$.

(Barely) doable.

Easy Example



Let $SL_3(\mathbb{Z}) \trianglerighteq \beta_T =$

$$\left\langle \begin{pmatrix} -1+T^3 & -T & T^2 \\ 0 & -1 & 2T \\ -T & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ -T^2 & 1 & -T \\ T & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & T^2 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle,$$

then $[SL_3(\mathbb{Z}): \beta_{-2}] = 3670016$. (Barely) doable.

But $[SL_3(\mathbb{Z}): \beta_7] = 24193282798937316960$

$= 2^5 3^4 5 \cdot 7^{10} 19 \cdot 347821 \sim 2^{64}$. Hopeless.

New Approach

A subgroup of finite index defines a finite permutation quotient.

Use finite quotients, in particular congruence quotients, to determine the index?

Congruence Subgroups

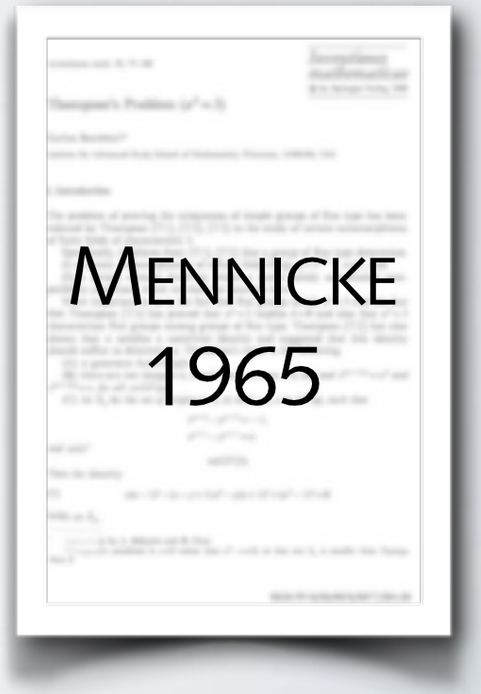
The m-th congruence subgroup $\Gamma_m \leq \mathrm{SL}_n(\mathbb{Z})$ is the kernel of the reduction φ_m modulo m. Image is $\mathrm{SL}_n(\mathbb{Z}_m)$.

If $G \leq \mathrm{SL}_n(\mathbb{Z})$ has finite index, there exists integer l such that $\Gamma_l \leq G$. The smallest such l is called the *level* of G.

Then $[\mathrm{SL}_n(\mathbb{Z}) : G] = [\mathrm{SL}_n(\mathbb{Z}_l) : \varphi_l(G)]$.

Calculate this second index from generators of G modulo l.

Thus sufficient to find level to get index.



Strategy

Consider congruence images $\varphi_m(G) < SL_n(\mathbb{Z}_m)$ for increasing values of m to find level l of G.

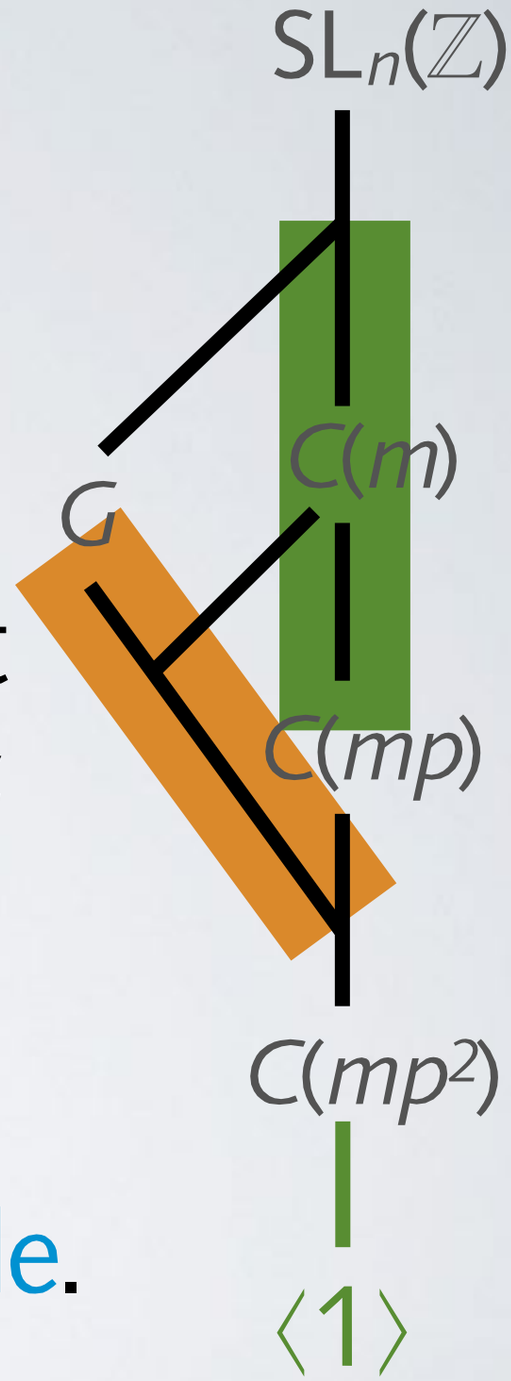
- Find the primes dividing l
- Find the prime powers dividing l
- Criterion on whether $I_m = [SL_n(\mathbb{Z}_m) : \varphi_m(G)]$ increases.

Same Index

Let $G \leq \mathrm{SL}_n(\mathbb{Z})$ and $C(m) = \ker \varphi_m$.

If for a given m and prime p we have that $I_m = I_{mp}$ but $I_{mp} \neq I_{mp^2}$, then (modulo mp^2) G contains a supplement to $C(mp)$.

We show such supplements typically do not exist, thus a stable index remains stable.



Kernel Supplements

Let p be prime, $a \geq 2$, $m=p^a$ and $H=\mathrm{SL}(n,\mathbb{Z}_m)$ for $n \geq 2$ (or $H=\mathrm{Sp}(2n, \mathbb{Z}_m)$ for $n \geq 1$). Let $C(k) \triangleleft H$ kernel mod k.

Theorem: (D-F-H.) $C(p^{a+1})$ has no proper supplement in $C(p^a)$.

Theorem: (Beisiegel 1977, Weigel 1995, …,D-F-H.)

Let $a=2$. $C(p)$ has a supplement in H if and only if

(a) $H=\mathrm{SL}(2,\mathbb{Z}_4)$, $\mathrm{SL}(2,\mathbb{Z}_9)$, $\mathrm{SL}(3,\mathbb{Z}_4)$, or $\mathrm{SL}(4,\mathbb{Z}_4)$.

(b) $H=\mathrm{Sp}(2,\mathbb{Z}_4)$, $\mathrm{Sp}(2,\mathbb{Z}_9)$.

Proof: Small cases/counterexample by explicit calculation. Use nice elements to show supplement contains kernel.

Index Algorithm

Assume that G has (unknown) finite index and level l. Assume we know the set $\mathscr{P}$ of primes dividing l.

1. Set $m=\mathrm{lcm}(4,\prod \mathscr{P})$.
2. While for any $p \in \mathscr{P}$ we have

   $[\mathrm{SL}_n(\mathbb{Z}_m):\varphi_m(G)]<[\mathrm{SL}_n(\mathbb{Z}_{pm}):\varphi_{pm}(G)]$, set $m:=pm$.
3. Repeat until index is stable, level divides m.

Show also that one can work prime-by-prime.

Index Algorithm

Assume that G has (unknown) finite index and level l. Assume we know the set $\mathscr{P}$ of primes dividing l.

1. Set $m=\mathrm{lcm}(4,\prod \mathscr{P})$.
2. While for any $p \in \mathscr{P}$ we have

   $[SL_n(\mathbb{Z}_m):\varphi_m(G)]<[SL_n(\mathbb{Z}_{pm}):\varphi_{pm}(G)]$, set $m:=pm$.
3. Repeat until index is stable, level divides m.

Show also that one can wor

because we start with 4

Index Algorithm

Assume that G has (unknown) finite index and level l. Assume we know the set $\mathscr{P}$ of primes dividing l.

1. Set m=lcm(4,$\prod \mathscr{P}$).
2. While for any $p \in \mathscr{P}$ we have $[G:G^{(m)}] = [\mathrm{PSL}_n(\mathbb{Z}):\mathrm{PSL}_n(p)]$, set $m:=pm$.
3. Repeat until index is stable, level divides m.

A group projecting onto $\mathrm{PSL}_n(p)$ has only trivial subdirect products with subgroups of $\mathrm{PSL}_n(q)$

Show also that one can work prime-by-prime.

The Set Of Primes

Theorem: Let $n \geq 3$ and suppose G has finite index. The set $\mathscr{P}$ of primes dividing the level l of G consists of those primes p for which

1. $p>2$ and $G \bmod p \neq \mathrm{SL}_n(\mathrm{p})$, or

2. $p=2$ and $G \bmod 4 \neq \mathrm{SL}_n(\mathbb{Z}_4)$

Proof: If other primes divided the level, there would be a supplement modulo p^2 (or 8).

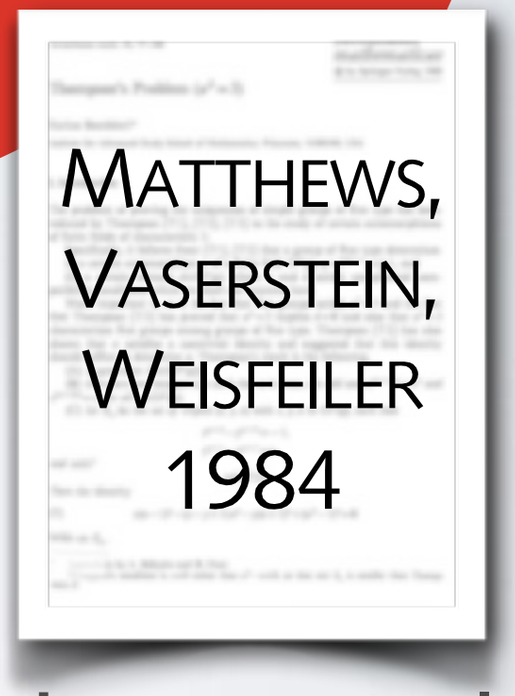
The Set Of Primes

Theorem: Let $n \geq 3$ and suppose G has fini

The set $\mathscr{P}$ of primes dividing the leve sts of those primes p for which

1. $p > 2$ and $G \bmod p \neq \mathrm{SL}_n(\mathrm{p})$, or
2. $p = 2$ and $G \bmod 4 \neq \mathrm{SL}_n(\mathbb{Z}_4)$

Zariski - density



Proof: If other primes divided the level, there would be a supplement modulo p^2 (or 8).

Finding Primes

We want primes for which $\varphi_p(G) \neq \mathrm{SL}_n(p)$. Methods:

a) Odd n, have ***transvection*** $t \in G$ (i.e. rk $(t-1)=1$).
   Let $N = \langle t \rangle^G$ normal closure. Primes for which $\varphi_p(t)$ not transvection or $\varphi_p(N)$ not abs. irr.

b) Test suitable set (possible b/c Steinberg rep.) of representations to remain abs. irr.

c) Eliminate possibilities of $\varphi_p(G)$ to lie in maximal subgroups of Aschbacher classes.
   So far done for small (prime) degrees.

Take $\mathbb{Z}$-lattice $L \leq \mathbb{Z}^{n\times n}$ spanned by G, rank n^2
Primes divide discriminant of L.

V

a) Odd n, have ***transvection*** $t \in G$ (i.e. rk $(t - 1)=1$).
   Let $N = \langle t \rangle^G$ normal closure. Primes for which $\varphi_p(t)$ not transvection or $\varphi_p(N)$ not abs. irr.

b) Test suitable set (possible b/c Steinberg rep.) of representations to remain abs. irr.

c) Eliminate possibilities of $\varphi_p(G)$ to lie in maximal subgroups of Aschbacher classes.
   So far done for small (prime) degrees.

Finding Primes

We want primes for which $\varphi_p(G) \neq \mathrm{SL}_n(p)$. Methods:

a) Odd n, have ***transvection*** $t \in G$ (i.e. rk $(t-1)=1$).
   Let $N = \langle t \rangle^G$ normal closure. Primes for which $\varphi_p(t)$ not transvection or $\varphi_p(N)$ not abs. irr.

b) Test suitable set (possible b/c Steinberg rep.) of representations to remain abs. irr.

c) Eliminate possibilities of $\varphi_p(G)$ to lie in r
   subgroups of Aschbacher classes.
   So far done for small (prime) degrees.

E.g:. find suitable elements $a \in G$, whose image cannot lie in particular class:

- $|a| = \infty$, then $|\varphi_p(a)|$ divides m iff $a^m \equiv 1 \pmod{p}$
- $[a^m, b^m] \neq 1$ for $m = \exp(S_n)$, then $\varphi_p(G)$ monomial, iff $\varphi_p([a^m, b^m]) \equiv 1 \pmod{p}$

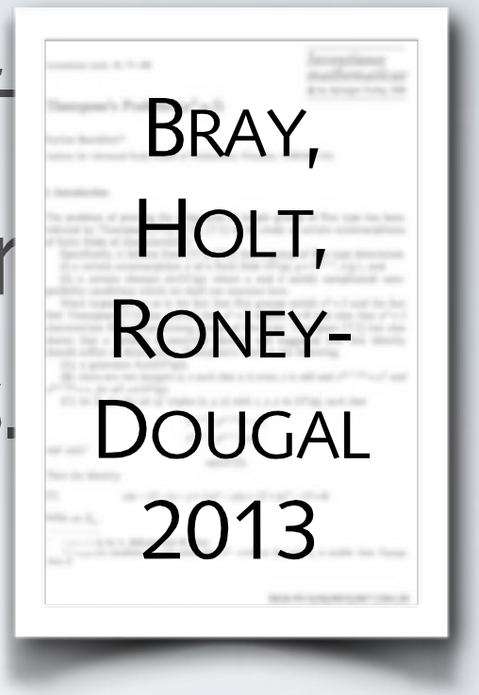
). Methods:

x (*t*-

for

abs.

erg



c) Eliminate possibilities of $\varphi_p(G)$ to lie in maximal subgroups of Aschbacher classes.
So far done for small (prime) degrees.

```
gap> g:=BetaT(7);
<matrix group with 3 generators>
gap> t:=b1beta(g); # transvection from Long/Reid paper
[ [-685,14,-98], [-16807,344,-2401], [2401,-49,344] ]
gap> IsTransvection(t);
1
gap> PrimesForDenseT(g,t,SL);time;
[ 7, 1021 ]
60
gap> MaxPCSPrimes(g,[7,1021],SL);time;
Try 7 7
Try 49 7
Try 343 7
Try 343 1021
Try 350203 1021
[350203, 2419328279893731696O ] #Proven Index in SL
291395 # about 5 minutes
```

```
gap> g:=Group([[778,2679,665],[323,797,665],
>       [6674504920,-1557328,340623049 49]],
>  [[-274290687,140904793,1960070592 ],[853,4560,294],
>       [151,930,209]]);;

gap> PrimesNonSurjective(g);  # about 2 sec.
#I  irrelevant prime 7
#I  Absolute irreducibility - found: [ 3, 5, 19 ] new:[ 19
#I  Monomial - found: [ 2, 3, 53 ] new:[ 53 ]
#I  Preserve a form - found: [ 3, 5 ] new:[  ]
#I  Element Order - found: [ 2, 3, 5, 19 ] new:[  ]
#I  Solvable - found: [ 2, 3, 5, 19, 53 ] new:[  ]
[ 2, 3, 5, 19, 53 ]

gap> MaxPCSPrimes(g,[2,3,5,19,53]); # about 25 sec.
Try 2,4,3,9,5,25,19,19^2,53, 53^2,30210 w. all primes
Index is 586082624189853029990 4=[ [ 2,13 ], [ 3,4 ],
 [ 13,3 ], [ 19,3 ], [ 31,1 ], [ 53,3 ], [ 127,1 ] ]
[ 30210, 586082624189853029990 4 ]
```

Talk to me for more details!