Contents

1 A Needle in a Haystack

1.1 Haystack

We deal with finite groups, and there is a lot of them.
Indeed, a lot.

Put gnu(k) = ***g**roup **nu**mber* of k, that is the number of pairwise non-isomorphic groups of order k (John Conway's terminology), and define

$$\mathrm{Gnu}(m) = \sum_{k=1}^{m} \mathrm{gnu}(k).$$

Now, let us see
$\mathrm{Gnu}(1) = 1$

$\mathrm{Gnu}(10) = 18$

$\mathrm{Gnu}(100) = 1\ 048$

$\mathrm{Gnu}(1000) = 11\ 758\ 814$

$\mathrm{Gnu}(2000) = 49\ 910\ 529\ 484$

(H. U. Beshe, B. Eick, and E. A. O'Brien, 2001)

1.2 Finding a Needle

How can we recognize the specific group among the others?

How can we find a needle in a haystack?

Clearly, every finite group is completely characterized by its own multiplication table. However, there are two problems here.

- If $|G| = n$ (and large), then the multiplication table of G contains n^3 entries (and huge).
- If we even have the multiplication tables of G and H, how (or how fast) can we determine whether G and H are isomorphic?

Can we choose a substantially smaller set of group parameters to determine the group uniquely (and effectively)?

Or, at least,

can we do this for most valuable groups?

What a magnet is able to retrieve a needle from a haystack?
First of all, what does the phrase "given the group G" mean?

In fact, it always implies that G is represented in some way:

- as a matrix group
- as a permutation group
- as a group of automorphisms of some object (graph, polygon etc.)
- as an abstract group with the list of generators and relations.

At present, if the last representation is used for finite groups, a group G is usually treated as *a black-box group*.

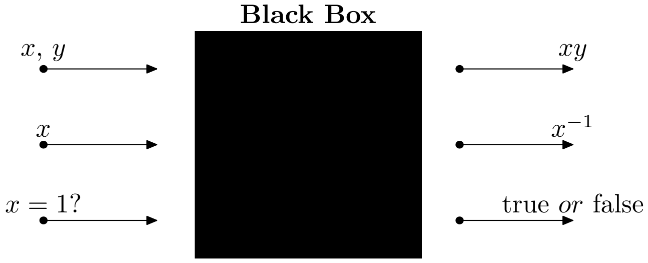
1.3 Black Box

A notion of a black-box group was invented by László Babai in the late 1970'ies and firstly introduced by L. Babai and E. Szemerézdi in "On the complexity of matrix group problems" in 1984. It plays a crucial role in the modern Computational Group Theory and influences the Theoretical Computer Science as well.

Scott Aaronson (MIT), 2010:

"Beautiful mathematical structures (like finite groups) *do useful things* in TCS (like giving natural examples where quantum computing seem to outperform classical). Laci (László Babai) did a quantum stuff before it ever exists..."

A black-box group G is a finite group whose elements are encoded, not necessarily uniquely, by $(0, 1)$-strings of uniform length n, with an oracle to perform group operations on the codewords, including the decision whether or not a string encodes the identity.



A black-box group G (or its subgroup) is *given* if a list of its generators $x_1, \ldots, x_k$ (strings corresponding to generators) is given:

$$G = \langle x_1, \ldots, x_k \rangle.$$

Definition (Babai, Beals, Seress, 2009)**.** *Let G be a finite group. A black-box representation of G with code-length n is a surjection $f : S \to G$ for some subset $S \subseteq \{0, 1\}^n$ of* valid strings*, along with an oracle that performs the group operations: given two valid strings x, y, the oracle produces valid strings z, u such that $f(x)f(y) = f(z)$ and $f(x)^{-1} = f(u)$, and also answers the question whether or not $f(x) = 1$. We say that G is* given *as a black-box group if in addition a list of valid strings $x_1, \ldots, x_k$ is given such that $\langle f(x_1), ..., f(x_k)\rangle = G$.*

Note that $|G| \leqslant 2^n$ where n is the code-length. The complexity of black-box group algorithms is always relative to the input length, which is $|A|n$ if G is given as $G = \langle A \rangle$.

1.4 Spectrum and its Apex

If G is given as a black-box group, then for every element x of G we can determine its order $|x|$ that is the least natural number n with $x^n = 1$. Thus, we can determine (or partially determine or with a high probability determine) the set of element orders of G.

For a group G the set $\omega(G) = \{n \in \mathbb{N} \mid \exists x \in G : |x| = n\}$ is called the *spectrum* of G.

If k divides n and $n \in \omega(G)$ then $k \in \omega(G)$. Therefore, the spectrum of G is determined by the set $\mu(G)$ of maximal under divisibility elements of $\omega(G)$. Till now the set $\mu(G)$ was unnamed.

Let us call it the *apex* of spectrum of G or, briefly, the apex of G.

1.5 Groups with a Nontrivial Normal Abelian Subgroup

Is a finite group G uniquely determined by $\omega(G)$?

Generally, the answer is, "No."

It is not determined, even among the groups of the same order.

Indeed, the abelian group $Z_4 \times Z_2$, the dihedral group D_8, and the quaternion group Q_8 have the order 8, the spectrum $\{1, 2, 4\}$, but are pairwise non-isomorphic.

Moreover, now we'll prove the following

Proposition (Shi, Mazurov, 1998)**.** *If the soluble radical (the maximal soluble normal subgroup) K of a finite group G is nontrivial, then there exist infinitely many finite groups H with $\omega(H) = \omega(G)$.*

Lemma. *If V is a nontrivial elementary abelian normal subgroup of G, $G_1 = V \leftthreetimes G$ is the natural semidirect product under the action of G on V by conjugation, then $\omega(G) = \omega(G_1)$.*

Proof. Obviously, $\omega(G) \subseteq \omega(G_1)$.

Suppose $(g, v) \in G_1$, where $g \in G$ and $v \in V$, a prime p is the period of V, and n is the order of Vg in G/V.

If $g^n \neq 1$, then $(g, v)^n = (g^n, v^{g^{n-1}} \dots v^g v)$ and g^n are nontrivial, and so they have the order p. Hence $|(g, v)| = |g| = pn$.

If $g^n = 1$ and $(g, v)^n = 1$, then $|(g, v)| = |g| = n$.

If $g^n = 1$ and $(g, v)^n = (1, v^{g^{n-1}} \dots v^g v) \neq 1$, then $(gv)^n = v^{g^{n-1}} \dots v^g v \neq 1$, so $|(g, v)| = |gv| = pn$.

Anyway, $|(g, v)| \in \omega(G)$, as required.

Proposition (Shi, Mazurov, 1998)**.** *If the soluble radical (the maximal soluble normal subgroup) K of a finite group G is nontrivial, then there exist infinitely many finite groups H with $\omega(H) = \omega(G)$.*

Lemma. *If V is a nontrivial elementary abelian normal subgroup of G, $G_1 = V \leftthreetimes G$ is the natural semidirect product under the action of G on V by conjugation, then $\omega(G) = \omega(G_1)$.*

Proof of Proposition. Since $K \neq 1$, there is an elementary abelian normal subgroup V of G. By lemma the spectrum of every group from infinite series $G = G_0, G_1, G_2 \dots$, where $G_{i+1} = V \leftthreetimes G_i$, coincides with $\omega(G)$.

1.6 Determination of Simple Groups

Does it mean that the spectrum is useless?

Must a magnet attract every straw in a haystack?

What about simple groups, building stones of the Group Theory?

Can we recognize them using their spectra?

It turns out that the answer is, "Yes."

At least, if we search among the groups of the same order.

Theorem (2009)**.** *If L is a finite simple group, and G is a finite group with $|G| = |L|$ and $\omega(G) = \omega(L)$, then $G \simeq L$.*

This result has a long history that we'll discuss later. Now let us prove it. A little bit of it, for a start.
Let L be a finite simple group, and G be a finite group with $|G| = |L|$ and $\omega(G) = \omega(L)$.

If L is a group of the prime order, then obviously $G \simeq L$. So we assume further that L is nonabelian.

Let L be the smallest nonabelian simple group. L can be considered as

- alternating group Alt_5 of permutations on 5 letters
- special linear group $SL_2(4)$ over the field of order 4
- projective linear group $PSL_2(5)$, that is the factor group of $SL_2(5)$ by its center of order 2.

We have

- $\omega(L) = \{1, 2, 3, 5\}$
- $|L| = 60 = 2^2 \cdot 3 \cdot 5$
- $\mathrm{gnu}(60) = 13$

Our nearest goal is to prove that $G \simeq L$ in this case.

1.7 Graphs and Cocliques

- G is a finite group
- $\pi(G)$ is the set of prime divisors of $|G|$
- $GK(G)$ is the *prime graph* of G with the vertex set $\pi(G)$ and $p \sim q \Leftrightarrow pq \in \omega(G)$
- A *coclique* is a subset ρ of the graph vertex set which vertices are pairwise non-adjacent.

Lemma. *Suppose that a finite group G has a normal series of subgroups $1 \leqslant K \leqslant M \leqslant G$, and primes p, q and r are such that p divides $|K|$, q divides $|M/K|$ and r divides $|G/M|$. Then $\{p, q, r\}$ cannot be a coclique in $GK(G)$.*

Proof. Assume G is a minimal counterexample (by order). Using the Frattini argument, we show that K is a p-group, and M/K is a q-group, and then consider the action of element of order r on the $\{p, q\}$-group M.

Let P be a Sylow p-subgroup of K, and $N = N_G(P)$.

By the Frattini argument, $G = KN$ and $N/(N \cap K) \simeq G/K$. So $1 \leqslant P \leqslant N \cap M \leqslant N$ is the normal series of N, and its factors satisfy the conditions of the lemma. The set $\{p, q, r\}$ is the coclique in $GK(G) \Rightarrow$ it is the coclique in $GK(N)$.

G is a minimal counterexample $\Rightarrow G = N$, $M = N \cap M$, $K = P$.

Put $\overline{G} = G/K$, $\overline{M} = M/K$, $\overline{Q} \in \mathrm{Syl}_q(\overline{M})$, and $\overline{N} = N_{\overline{G}}(\overline{Q})$.

By the Frattini argument, $\overline{N}/(\overline{N} \cap \overline{M}) \simeq \overline{G}/\overline{M}$, so r divides $|\overline{N}/\overline{Q}|$.

Let Q and N denote the preimages of $\overline{Q}$ and $\overline{N}$ in G. Then N has the normal series $1 \leqslant K \leqslant Q \leqslant N$, and its factors satisfy the conditions of the lemma. Hence $G = N$, and $M = Q$.

Let x be an element of order r in G. Since G does not contain elements of order pr and qr, the element x induces a fixed-point-free automorphism of order r of M. By the Thompson Theorem, M is nilpotent. Therefore, it contains an element of order pq; a contradiction.

Corollary. *Suppose that G is a finite group, and ρ is a coclique in $GK(G)$ of size at least 3. Then at most one prime from ρ can divide the order of the soluble radical K of G. In particular, G is insoluble.*

Proof. Assume to the contrary that two distinct primes p, q lie in $\rho \cap \pi(K)$. $|\rho| \geqslant 3 \Rightarrow$ the coclique ρ contains a third prime r.

Let $R \in \mathrm{Syl}_r(G)$, and put $H = \langle K, R \rangle$. H/K is a r-group $\Rightarrow$ H is soluble $\Rightarrow$ there is a chief series of H, whose factors are elementary abelian. It follows that H satisfies the conditions of the lemma, so $\{p, q, r\}$ cannot be a coclique; a contradiction.

Corollary. *Suppose that G is a finite group, and ρ is a coclique in $GK(G)$ of size at least 3. Then at most one prime from ρ can divide the order of the soluble radical K of G. In particular, G is insoluble.*

Return to $L \simeq \mathrm{Alt}_5$ and G with $\omega(G) = \omega(L)$ and $|G| = |L|$.

$\omega(G) = \omega(L) = \{1, 2, 3, 5\} \Rightarrow GK(G) = GK(L)$ is the coclique.
So a composition series of G must contain a nonabelian factor S.

$|L| \leqslant |S| \leqslant |G|$ and $|G| = |L| \Rightarrow G = S \simeq L$.

Now we understood why L is uniquely determined by its spectrum among the groups of order 60.
Modulo two facts:

- the smallest nonabelian simple group is unique and isomorphic to Alt_5.
- the Thompson Theorem on nilpotency of a group admitting a fixed-point-free automorphism of prime order

Who can prove the Thompson Theorem here and now?
Is it necessary to use here so powerful resource as the Thompson Theorem? The choice among 13 groups seems easy and regardless.

Let's take the simple group $L = GL_5(2)$.

- the apex $\mu(L) = \{8, 12, 14, 15, 21, 31\}$
  (recall $\omega(L)$ is the set of all divisors of elements from $\mu(L)$)
- $|L| = 9\,999\,360 = 2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$

- gnu(9 999 360) > 100 000 000 000

The last inequality holds, since $gnu(2^{10}) = 49\,487\,365\,422$

The prime graph $GK(L)$ includes the coclique $\{5, 7, 31\}$, so a group G with the same prime graph is insoluble. It follows that a composition series of G contains a nonabelian factor S with $\pi(S) \subseteq \pi(L)$. There are finitely many simple groups that can be isomorphic to S (in fact, there are 24 such groups). This observation does not solve the problem, but obviously allows to restrict a selection field. Later, we'll see how one can use such restriction to recognize a simple group.

1.8 Infinite Haystack

Returning to a determination of $L \simeq \mathrm{Alt}_5$, what happens if we omit the condition $|L| = |G|$?

What can we say about G with $\omega(G) = \omega(L)$?

$\omega(G) = \omega(L) = \{1, 2, 3, 5\} \Rightarrow G$ insoluble.

Let K be the soluble radical of G, then $\overline{G} = G/K$ is nontrivial. If M is the minimal normal subgroup of $\overline{G}$, then M is a direct product $S_1 \times \ldots \times S_k$ of nonabelian simple groups. If $k > 1$, then $GK(G)$ cannot be a coclique, which is impossible. Thus, there is a nonabelian simple group S such that

$$S \simeq \mathrm{Inn}(S) \leqslant \overline{G} \leqslant \mathrm{Aut}(S).$$

Such configuration arises for most of simple groups L (see soon)

$\omega(S) \subseteq \omega(L) \Rightarrow \pi(S) = \{2, 3, 5\}$.

There are only three such nonabelian simple groups, and two of them, non-isomorphic to L, contain an element of order 4.

So $S \simeq L \Rightarrow L \leqslant \overline{G} \leqslant \mathrm{Aut}(L)$.
Thus, $L \leqslant \overline{G} \leqslant \mathrm{Aut}(L)$.

$L \simeq \mathrm{Alt}_5 \Rightarrow \mathrm{Aut}(L) \simeq \mathrm{Sym}_5$.

$4 \in \omega(\mathrm{Sym}_5) \Rightarrow \overline{G} = L$.

$\rho = \{2, 3, 5\}$ is the coclique of $GK(G) \Rightarrow$ at most one prime from ρ can divide $|K|$.

So K is a p-group for $p \in \rho$. For the Frattini subgroup $\Phi(K)$ put $\widetilde{K} = K/\Phi(K)$ and $\widetilde{G} = G/\Phi(K)$. Then $\widetilde{G}$ is an extension of an elementary abelian p-group $\widetilde{K}$ by L. Since $C = C_{\widetilde{G}}(\widetilde{K}) \lhd \widetilde{G}$, we have $C = \widetilde{K}$ or $C = \widetilde{G}$. In the last case $GK(G)$ is not a coclique; a contradiction. Thus, L acts faithfully on $\widetilde{K}$ by conjugation, and we can consider $\widetilde{G}$ as a faithful L-module over $\mathbb{F}_p$. Using the linear representation theory, one can show (and we'll do that later) that $2p \in \omega(\widetilde{G}) \subseteq \omega(G) = \omega(L)$; a final contradiction. Thus, $G \simeq L$.

We say that L is *recognizable by spectrum* in that case.

It turns out that many finite simple groups are recognizable by spectrum.

1.9 Recognition by Spectrum: Problem Statement

- G is a finite group
- $h(G)$ is the number of pairwise non-isomorphic finite groups H with $\omega(H) = \omega(G)$
- G is *recognizable* (by spectrum) if $h(G) = 1$
- G is almost recognizable if $h(G) < \infty$
- G is non-recognizable if $h(G) = \infty$

Recognition Problem
Given a finite group G, find $h(G)$. If $h(G)$ is finite, describe finite groups H with $\omega(H) = \omega(G)$.

2 Visit to the Zoo

2.1 Classification Theorem

Every finite group G has a composition series

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_{t-1} \leqslant G_t = G,$$

where $G_{i-1} \trianglelefteq G_i$ and G_i/G_{i-1} is a simple group for $i = 1, \ldots, t$.

Thus every finite group can be constructed from simple groups.

The fact that we have the classification of finite simple groups (CFSG) is quite overwhelming. It is one of the Wonders of the mathematical World.

Since simple groups are highlights of our discussion we'll consider them and their classification today.

This does not pretend to be a serious investigation, it's rather a visit.

Visit to the Zoo
The Classification Theorem asserts

Finite Simple Groups:

- groups of prime order
- alternating groups
- groups of Lie type
  - classical
  - exceptional
- 26 sporadic groups

If G is a group of prime order, then it is uniquely determined by its order. On the other hand, it is obvious that there are infinitely many finite group with the same spectrum as spectrum of G.

Further, *simple* means *nonabelian simple.*

2.2 Sporadic groups

Sporadic Groups
In fact we skip sporadic groups at the present visit. There are two reasons.

First, for all sporadic groups the recognition problem has been completely solved. Namely,

Shi, 1988, ..., Shi-Mazurov, 1998

Let L be a sporadic simple group.

- If $L \neq J_2$, then $h(L) = 1$.
- If $L = J_2$, then $\omega(L) = \omega(V \leftthreetimes GL_4(2))$, where V is the elementary abelian group of order 2^6, and $h(L) = \infty$.

Second, every sporadic group requires a special sporadic approach to be presented. Unfortunately, we have not enough time for this.

2.3 Permutation Groups

Permutation Groups
Alt_n is the subgroup of all even permutations of the group Sym_n of all permutations on n letters.

Evariste Galois:

The groups Alt_n are solvable for $n \leqslant 4$ and nonabelian simple for $n \geqslant 5$.

So a general polynomial equation of degree n in one variable is solvable by radicals $\Leftrightarrow n \leqslant 4$.
Spectra of permutation groups
Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, $k = p_1^{\alpha_1} + \dots + p_s^{\alpha_s}$, where p_i are primes, and α_i are positive integers.

If $G = \mathrm{Sym}_n$, then $m \in \omega(G) \Leftrightarrow k \leqslant n$.

Let $G = \mathrm{Alt}_n$.
If m is odd, then $m \in \omega(G) \Leftrightarrow k \leqslant n$.
If m is even, $m \in \omega(G) \Leftrightarrow k \leqslant n - 2$.
Put $\Omega = \{1, \dots, n\}$. Any subgroup G of the symmetric group $\mathrm{Sym}(\Omega) = \mathrm{Sym}_n$ is called a permutation group of Ω.

An arbitrary group G *acts* on a set Ω if there is a homomorphism φ from G to $\mathrm{Sym}(\Omega)$. The image αg of $\alpha \in \Omega$ under action of $g \in G$ is an element $\beta \in \Omega$ such that $\beta = \alpha(g\varphi)$.

G acts *faithfully* on Ω iff $\ker(\varphi) = 1$.

G acts *k-transitively* on Ω if for every two k-tuples of elements of Ω there is an element $g \in G$ transferring one of them to another. 1-transitive group G is said to be *transitive* (on Ω).

If G acts on Ω, $\alpha \in \Omega$, then the subgroup $H = G_\alpha = = \{g \in G \mid \alpha g = \alpha\}$ is *a point stabilizer*, and $|G : H|$ is equal to the size of the orbit $\alpha G = \{\alpha g \mid g \in G\}$. If G is a transitive permutation group on Ω then $\alpha G = \Omega$ and all point stabilizers H are conjugate in G. The action of G on the factor set G/H by right multiplication, that is, $(Hx)g = H(xg)$ for all right cosets Hx of G/H and elements $g \in G$, is similar to the natural action of G on Ω.
If G acts on Ω (of size at least 3) such that it preserves some nontrivial partition of G, then this partition is called a *system of imprimitivity* for G, and G is called *imprimitive.* If G is not imprimitive, it is called *primitive.*

G is 2-transitive $\Rightarrow$ G is primitive $\Rightarrow$ G is transitive

If G is transitive, then
G is primitive $\Leftrightarrow$ a point stabilizer is a maximal subgroup of G

If $n \geqslant 5$, and $n \neq 6$, then every subgroup H of $G = \mathrm{Alt}_n$ isomorphic to Alt_{n-1} must be a point stabilizer. It follows that there is a one-to-one correspondence between the set M of these subgroups and letters from Ω. Every automorphism of G permutes subgroups of M, so it permutes letters from Ω. Therefore, there is a homomorphism from G to Sym_n. On the other hand, $\mathrm{Sym}_n \leqslant \mathrm{Aut}(G)$. Thus, $\mathrm{Sym}_n = \mathrm{Aut}(G)$.

2.4 Groups of Lie type

Groups of Lie type
Simple groups of Lie type arise as a groups of automorphisms (of special form) of simple Lie algebras over finite fields. Thus their classification is connected with the classification of simple Lie algebras.

There are four infinite series of such algebras: A_n, B_n, C_n, D_n,
and five exceptional algebras: G_2, F_4, E_6, E_7, E_8.

Groups corresponding to infinite series of simple algebras have a natural matrix presentations and are called *classical.*
Groups corresponding to exceptional algebras form series of *exceptional* groups of Lie type.

Thus, we have the following classification of simple groups of Lie type.

Classical groups:

- linear: $A_{n-1}(q) \simeq PSL_n(q)$, $n \geqslant 2$, $(n, q) \neq (2, 2), (2, 3)$;
- unitary: ${}^2A_{n-1}(q) \simeq PSU_n(q)$, $n \geqslant 3$, $(n, q) \neq (3, 2)$;
- symplectic: $C_n(q) \simeq PSp_{2n}(q)$, $n \geqslant 2$, $(n, q) \neq (2, 2)$;
- orthogonal: $B_n(q) \simeq P\Omega_{2n+1}(q)$, $n \geqslant 3$, q odd;
- orthogonal: $D_n(q) \simeq P\Omega_{2n}^+(q)$, $n \geqslant 4$;

- orthogonal: ${}^2D_n(q) \simeq P\Omega^-_{2n}(q)$, $n \geqslant 4$

where q is a power p^α of a prime p.

Exceptional groups:

- $G_2(q)$, $q \geqslant 3$; $F_4(q)$; $E_6(q)$; $E_7(q)$; $E_8(q)$
  where q is a power p^α of a prime p;
- Suzuki groups: ${}^2B_2(2^{2n+1})$, $n \geqslant 1$;
- Ree groups: ${}^2G_2(3^{2n+1})$, $n \geqslant 1$; ${}^2F_4(2^{2n+1})$, $n \geqslant 1$;
- the Tits group ${}^2F_4(2)$.

2.5 Finite Fields

Finite fields

Even the overview of Lie approach requires time that we have no it, so we concentrate on groups with natural matrix representation. Since our groups are defined over the finite fields, we recall some basic facts on these fields.

- Finite field F has the positive characteristic p, where p is a prime, and contains the prime subfield $\mathbb{F}_p$ of order p.
- F is a vector space over $\mathbb{F}_p$, so $|F| = q$, where $q = p^\alpha$.
- For every prime p and positive integer α there is the unique field $\mathbb{F}_q$ of order $q = p^\alpha$. If f is any irreducible polynomial over $\mathbb{F}_p$ of degree α, then $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(f)$, in particular, $\mathbb{F}_q$ does not depend on the choice of f.
- Multiplicative group $\mathbb{F}_q^*$ of the field $\mathbb{F}_q$ is cyclic.
- Automorphism group $\mathrm{Aut}(\mathbb{F}_q)$ has order α and is generated by the *Frobenius automorphism* σ given by $x\sigma = x^p$ for all $x \in \mathbb{F}_q$.

2.6 Linear Groups and Simplicity

The linear groups and their orders Let V be a vector space over the field $\mathbb{F}_q$.

The *general linear group* $GL_n(q)$ consists of all non-singular linear transformations of V. Since there is a one-to-one correspondence between such transformations and basises of V, the order of this group is given by $|GL_n(q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$. The center $Z(GL_n(q))$ of $GL_n(q)$ consists of all scalar transformations, so is of order $q - 1$. The factor group $GL_n(q)/Z(GL_n(q))$ is called the *projective general linear group* and denoted by $PGL_n(q)$.

The transformations of determinant 1 form a normal subgroup $SL_n(q)$ of index $q-1$, *the special linear group.* The center $Z(SL_n(q))$ equals $Z(GL_n(q)) \cap SL_n(q)$ and has order equal to $(n, q-1)$. The factor group $SL_n(q)/Z(SL_n(q))$ is called the *projective special linear group* and denoted by $PSL_n(q)$.

$$|PSL_n(q)| = \frac{1}{(n, q-1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1).$$

Simplicity

Theorem. *The group $PSL_n(q)$, $n \geqslant 2$, $q = p^\alpha$, p is a prime, iff $(n, q) \neq (2, 2), (2, 3)$.*

The key lemma is the following

Lemma (Iwasawa, 1941)**.** *If G is a finite perfect group (that is $G = G'$), acting faithfully and primitively on a set Ω, such that the point stabilizer H has a normal abelian subgroup A whose conjugates generate G, then G is simple.*

Now to prove the theorem is enough to check that the group $PSL_n(q)$ satisfies the conditions of the lemma.

2.7 Other Classical Groups

The unitary groups A finite field admits an automorphism of order 2 if its order is equal to q^2 for some prime-power q, and the involutory automorphism is given by $\overline{\lambda} \mapsto \lambda^q$ and called *conjugation.* Let V be a vector space over the field F_{q^2} which is endowed with a non-singular Hermitian scalar product. Thus (x, y) is linear in x, conjugate linear in y, and

$$(y, x) = \overline{(x, y)}.$$

The group of non-singular linear transformations of V preserving this product is called the *general unitary group* $GU_n(q)$. Groups $PGU_n(q)$, $SU_n(q)$, $PSU_n(q)$ are defined and called simultaneously to corresponding linear groups.

Groups $PSL_2(q)$ and $PSU_2(q)$ are isomorphic for all q.

Groups $PSU_n(q)$, $n \geqslant 3$, are simple except $PSU_3(2)$.

The symplectic groups Let V be a vector space of dimension $2n$ over the field $\mathbb{F}_q$ which is endowed with a non-singular bilinear scalar product. We assume that this scalar product is skew-symmetric, so that

$$(y, x) = -(x, y)$$

for all $x, y \in V$.

The group of non-singular linear transformations of V preserving this product is called the *symplectic group* $Sp_{2n}(q)$. This group is, to within isomorphism, independent of the choice of the scalar product.

Every symplectic transformation has determinant 1. The center of the group $Sp_{2n}(q)$ consists of transformations φ such that $x\varphi = \lambda x$ for all $x \in V$ where $\lambda = \pm 1$. The factor group $Sp_{2n}(q)/Z(Sp_{2n}(q))$ is called the *projective symplectic group* $PSp_{2n}(q)$.

$$Sp_2(q) = SL_2(q).$$

$$PSp_2(q) = PSL_2(q).$$

Groups $PSp_{2n}(q)$, $n \geqslant 2$ is simple except for $PSp_4(2)$.

The orthogonal groups over odd characteristic Let V be a vector space of dimension n over the field $\mathbb{F}_q$ of odd characteristic which is endowed with a non-singular bilinear scalar product. We assume that this scalar product is symmetric, so that

$$(y, x) = (x, y)$$

for all $x, y \in V$.

The group of non-singular linear transformations of V preserving this product is called the *general orthogonal group.* If n is odd this group is, to within isomorphism, independent of the choice of the scalar product and is denoted $GO_n(q)$. If n is even there are two inequivalent non-singular symmetric scalar products on V which give rise to distinct orthogonal groups. This groups are denoted $GO_n^+(q)$ and $GO_n^-(q)$.

Let ε be the empty symbol if n is odd and $\varepsilon \in \{+, -\}$ if n is even.

Every orthogonal transformation has determinant 1 or -1. The *special orthogonal group* $SO_n^\varepsilon(q)$ is the group of orthogonal transformations with determinant 1. The commutator subgroup of $SO_n^\varepsilon(q)$ is denoted by $\Omega_n^\varepsilon(q)$. If n is odd this group have trivial center and is simple except for $\Omega_3(3)$. If n is even $\Omega_n^\varepsilon(q)$ has the center of order $(4, q^{n/2} - \varepsilon 1)/2$, corresponding projective group $\Omega_n^\varepsilon(q)/Z(\Omega_n^\varepsilon(q))$ is denoted by $P\Omega_n^\varepsilon(q)$. These groups are not simple or isomorphic to some linear or unitary groups if $n < 4$, and are always simple for $n \geqslant 4$.

The orthogonal groups over characteristic 2 Let V be a vector space of dimension n over the field $\mathbb{F}_q$ of characteristic 2. In this case the notions of symmetric and skew-symmetric form coincide. Thus if we proceed in the way described above we will come to the symplectic groups again. Here quadratic forms come to the first place. The quadratic form on V is a function $f : V \to \mathbb{F}_q$ such that

$$f(\lambda x + \mu y) = \lambda^2 f(x) + \mu^2 f(y) + \lambda\mu(x, y)$$

for all $\lambda, \mu \in \mathbb{F}_q$ and $x, y \in V$ and some symmetric bilinear form (x, y).

Now the orthogonal group is the group of non-singular linear transformations of V preserving the quadratic form: $f(Tx) = f(x)$. Again there is only one group $GO_n(q) \simeq Sp_{n-1}(q)$ in odd dimension and there are two groups $GO_n^+(q)$ and $GO_n^-(q)$ in even dimension. The commutator subgroup Ω_n^ε is generally simple.

3 Spectra of finite simple classical groups

The spectrum $\omega(G)$ of a group G is the set of element orders.

$G = S_6$. The order of an element is determined by its decomposition into product of independent cycles. Thus $\omega(G) = \{1, 2, 3, 4, 5, 6\}$.

$\omega(G)$ is closed under taking divisors, i.e., for every $n \in \omega(G)$ and every d dividing n, d lies in $\omega(G)$.

$$\text{If } |g| = n, \text{then } |g^{n/d}| = d.$$

$\mu(G)$ is the set of maximal under divisibility elements of $\omega(G)$.

$\omega(S_6) = \{1, 2, 3, 4, 5, 6\} \Rightarrow \mu(S_6) = \{4, 5, 6\}$

$\omega(G)$ is uniquely determined by any set $\nu(G)$ such that

$$\mu(G) \subseteq \nu(G) \subseteq \omega(G)$$

and consists of all divisor of elements of $\nu(G)$.

3.1 Nonabelian simple groups

— 26 sporadic groups
— alternating groups
— groups of Lie type
  — classical
  — exceptional

The simple classical groups.

$GL_n(q) \to SL_n(q) \to PSL_n(q)$, $GU_n(q) \to SU_n(q) \to PSU_n(q)$
$Sp_{2n}(q) \to PSp_{2n}(q)$, $GO_{2n+1}(q) \to SO_{2n+1}(q) \to \Omega_{2n+1}(q)$,
$GO^{\pm}_{2n}(q) \to SO^{\pm}_{2n}(q) \to \Omega^{\pm}_{2n}(q) \to P\Omega^{\pm}_{2n}(q)$

Linear groups

$GL_n(q)$ is the group of all non-degenerate matrices of size $n \times n$ over a field F_q of order q.
$SL_n(q) = \{g \in GL_n(q) | \det g = 1\}$.
$Z(GL_n(q)) = \{\lambda E | \lambda \in F_q\} \Rightarrow Z(SL_n(q)) = \{\lambda E | \lambda \in F_q, \lambda^n = 1\}$. Thus $|Z(SL_n(q))| = (n, q-1)$.
$PSL_n(q) = SL_n(q)/Z(SL_n(q))$.

3.2 Unipotent elements

Let F be a field of characteristic $p > 0$.

$$GL_n(F) \ni g = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix} = E + J,$$

$$E \text{ is the identity matrix and } J = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix}.$$

$(E + J)^k = E + C^1_k J + C^2_k J^2 + \cdots + C^{n-1}_k J^{n-1}$
Thus $(E + J)^k = E$ iff p divides C^i_k for $1 \leqslant i \leqslant n-1$.
The least number k for which $(E + J)^k = E$ equals the least power of p which is greater then $n - 1$.
Thus $|g| = p^{l+1}$ where $p^l \leqslant n - 1 < p^{l+1}$.

3.3 Semisimple elements

$$GL_n(F) \ni g = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix},$$

$$|\lambda_1| = m_1, |\lambda_2| = m_2, \ldots, |\lambda_n| = m_n.$$
$$\Downarrow$$
$$|g| = [m_1, m_2, \ldots, m_n].$$

3.4 Elements of composite orders

$$GL_n(F) \ni g = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda & & & & \\ & \lambda & & & \\ & & \ddots & & \\ & & & \lambda & \\ & & & & \lambda \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{\lambda} & & & \\ & 1 & \frac{1}{\lambda} & & \\ & & \ddots & \ddots & \\ & & & 1 & \frac{1}{\lambda} \\ & & & & 1 \end{pmatrix} = su.$$

s semisimple, u unipotent, and since $su = us$, we have $|g| = |s||u|$.

3.5 Spectrum of a group of Lie type

Let G be a finite group of Lie type over a field of order q and characteristic p.

$$\omega(G) = \omega_p(G) \cup \omega_{p'}(G) \cup \omega_m(G)$$

$\omega_p(G)$ is the set of orders of p-elements
$\omega_{p'}(G)$ is the set of orders of p'-elements
$\omega_m(G)$ is the set of the rest "composite" orders
Define sets $\mu_p(G)$, $\mu_{p'}(G)$ and $\mu_m(G)$ to be the intersections of $\mu(G)$ and the corresponding subsets of $\omega(G)$.

3.6 Algebraic closure of F_p

For a prime p denote by $\overline{F}_p$ the algebraic closure of the field F_p. Recall that for every irreducible polynomial $f(x) \in F_p[x]$ there exists a finite field F_q such that F_q contains a root of $f(x)$. Let I be the ideal of $F_p[x]$ generated by $f(x)$. Since $f(x)$ is irreducible, the factor ring $F_p[x]/I$ is a field of order p^k where k is the degree of $f(x)$. In this field $f(x) = 0$. Thus x is a root of $f(x)$. Therefore, we can define $\overline{F}_p$ to be the union of field F_{p^k} over all possible values of k. But how one can combine two different fields?

Let F_r be a subfield of F_q where $q = p^k$. Then $r = p^l$ and l divides k. Indeed, F_q is a vector space over F_r. Thus F_q is isomorphic to F_r^m for some m. Moreover, a field of order p^k contains a subfield of order p^l for every natural number l dividing k.

Now it is clear how to construct the union. Let us take, for example, fields F_{p^2} and F_{p^3}. Both of them can be embedded into the field F_{p^6}. Thus we can add and multiply elements of these fields.

$$\overline{F}_p = \bigcup_{k \geqslant 1} F_{p^k}.$$

3.7 Frobenius map

$GL_n(q)$ can be embedded into $GL_n(\overline{F}_p)$. Hence we can speak about Jordan form of element of $GL_n(q)$ in $GL_n(\overline{F}_p)$.

Let σ be an automorphism of the field F_{p^k} given by $\lambda \mapsto \lambda^{p^l}$. If k divides l this automorphism is trivial and nontrivial otherwise. The elements of the field $\overline{F}_p$ which are invariant under the action of the map σ form the field F_{p^l}.

A standard Frobenius map σ_q of $GL_n(\overline{F}_p)$: $(a_{ij}) \mapsto (a_{ij}^q)$ where q is a power of p. σ_q is an endomorphism of $GL_n(\overline{F}_p)$ into itself. The elements of $GL_n(\overline{F}_p)$ which are invariant under the action of σ_q forms the group $GL_n(q)$.

A homomorphism $\sigma : GL_n(\overline{F}_p) \to GL_n(\overline{F}_p)$ is called a Frobenius map if some power of σ is a standard Frobenius map.

3.8 Unipotent elements

Let $G = GL_n(q)$ where q is a power of a prime p. Recall that the maximal power of p lying in $\omega(G)$ is the least power of p that is greater than $n-1$. $n-1$ can be interpreted as the maximal height among the roots of the root system of $GL_n(q)$. It turns out to be true in the general case.

Testerman D. M. A_1-Type overgroups of order p in semisimple algebraic groups and the associated finite groups, J. Algebra, 1995, V. 177, N 1, P. 34–76.

Theorem. *Let G be a finite group of Lie type over a field of positive characteristic p. Then the maximal power of p lying in the spectrum of G is equal to the minimal power of p that is greater than the maximal height of the roots in the root system of G.*

The maximal heights

linear and unitary groups of dimension n	$n-1$
symplectic groups of dimension $2n$	$2n-1$
orthogonal groups of dimension $2n+1$	$2n-1$
orthogonal groups of dimension $2n$	$2n-3$

Let $G = PSL_7(25)$. The characteristic is 5. The height of the highest root is equal to $7-1=6$. We have $5 < 6 < 25$. Hence $25 \in \omega(G)$ and $125 \notin \omega(G)$.

Let $G = Sp_{10}(9)$. The characteristic is 3. The height of the highest root is equal to $10-1=9$. We have $9 \leqslant 9 < 27$. Hence $27 \in \omega(G)$ and $81 \notin \omega(G)$.

3.9 Semisimple elements

R. W. Carter, Finite Groups of Lie Type: Conjugacy Classes and Complex Characters, Wiley, New York (1985).

Let $\overline{G} = GL_n(\overline{F}_p)$ and $G = GL_n(q)$. Put $\sigma = \sigma_q$. For a group H and a homomorphism $\alpha : H \to H$ denote by H_α the group of α-fixed points.

$$\overline{G}_\sigma = \{g \in \overline{G} | g^\sigma = g\} = G.$$

Denote by $\overline{T}$ the subgroup of $\overline{G}$ consisting of all diagonal matrices. Since semisimple elements are diagonalizable, each of them is conjugate to some element of $\overline{T}$. $\overline{T}$ and all its conjugate are called maximal tori of $\overline{G}$. Thus every semisimple element is contained in some maximal torus.

Let $\overline{S}$ be a σ-stable maximal torus of $\overline{G}$. The group $S = \overline{S}_\sigma$ is called a maximal torus of G. Every semisimple element of G is contained is some maximal torus of G. $\mu(S)$ consists of one number - the exponent of S. Thus we are to determine exponents of all maximal tori.

Let $\overline{T}^g$ be σ-stable maximal torus of $\overline{G}$. We have

$$(\overline{T}^g)^\sigma = \overline{T}^g,$$

$$(\overline{T}^\sigma)^{g^\sigma} = \overline{T}^g.$$

Thus $g^\sigma g^{-1}$ normalizes $\overline{T}$.

Proposition. *Let $\overline{T}^g$ be a σ-stable maximal torus of $\overline{G}$. The groups $(\overline{T}^g)_\sigma$ and $\overline{T}_{\sigma \circ g^\sigma g^{-1}}$ are conjugate in $\overline{G}$.*

Proof. Let t be an element of $\overline{T}$ such that t^g lies in $(\overline{T}^g)_\sigma$. We have

$$(t^g)^\sigma = t^g,$$

$$(t^\sigma)^{g^\sigma} = t^g,$$

$$(t^\sigma)^{g^\sigma g^{-1}} = t.$$

Thus t^g lies in $(\overline{T}^g)_\sigma$ iff t lies in $(\overline{T})_{\sigma \circ g^\sigma g^{-1}}$.

Moreover, $(\overline{T})_{\sigma \circ n}$ for $n \in N_{\overline{G}}(\overline{T})$ is conjugate to some maximal torus of G.

A matrix is called monomial if each column and each row in it contain exactly one non-zero element. A monomial matrix is called a permutation matrix if all non-zero entries are unities. $N_{\overline{G}}(\overline{T})$ consists of all monomial matrices. Every monomial matrix can be presented as a product of a diagonal matrix and a permutation matrix.

Since $\overline{T}$ acts on itself trivially, the factor group $W = N_{\overline{G}}(\overline{T})/\overline{T}$ acts on $\overline{T}$. This group is independent of the choice of the maximal torus and called the Weyl group of $\overline{G}$. Clearly, W is isomorphic to Sym_n.

Let $\pi : N_{\overline{G}}(\overline{T}) \to W$ be the natural homomorphism. The proposition we proved implies that $(\overline{T}^g)_\sigma$ is conjugate to $\overline{T}_{\sigma \circ w}$ where $w = \pi(g^\sigma g^{-1})$.

Since $\overline{T}$ is σ-stable, $N_{\overline{G}}(\overline{T})$ is also σ-stable. Thus σ acts on W. Elements w_1 and w_2 are called σ-conjugate if there exists $w \in W$ such that $w_1 = w^\sigma w_2 w^{-1}$.

If w_1 and w_2 are σ-conjugate then groups $\overline{T}_{\sigma \circ w_1}$ and $\overline{T}_{\sigma \circ w_2}$ are conjugate in $\overline{G}$. This implies that to describe the structure of all maximal tori we should describe the structure of groups $\overline{T}_{\sigma \circ w}$ where w runs over a full system of representatives of σ-conjugacy classes.

σ act on W trivially. Thus σ-conjugacy=conjugacy. Two elements of Sym_n are conjugate if there cyclic types coincide. W acts on matrices by permuting rows and columns.

Let $w = (12\dots k)w_1$.

$$\overline{T}_{\sigma\circ w} \ni \begin{pmatrix} \lambda_1 & & & & & \\ & \lambda_2 & & & & \\ & & \ddots & & & \\ & & & \lambda_k & & \\ & & & & \ddots & \\ & & & & & \lambda_n \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda_1 & & & & & \\ & \lambda_2 & & & & \\ & & \ddots & & & \\ & & & \lambda_k & & \\ & & & & \ddots & \\ & & & & & \lambda_n \end{pmatrix}^{\sigma\circ w} = \begin{pmatrix} \lambda_k^q & & & & & \\ & \lambda_1^q & & & & \\ & & \lambda_2^q & & & \\ & & & \ddots & & \\ & & & & \lambda_{k-1}^q & \\ & & & & & \ddots \end{pmatrix}.$$

We have $\lambda_1 = \lambda_k^q$, $\lambda_2 = \lambda_1^q, \dots, \lambda_k = \lambda_{k-1}^q$. This system is equivalent to the following one: $\lambda_1^{q^k-1} = 1$, $\lambda_2 = \lambda_1^q$, $\lambda_3 = \lambda_1^{q^2}, \dots, \lambda_k = \lambda_1^{q^{k-1}}$. Hence if the decomposition of w into disjoint cycles contains a k-cycle then each matrix of $\overline{T}_{\sigma\circ w}$ contains a block of the form

$$\begin{pmatrix} \lambda & & & & \\ & \lambda^q & & & \\ & & \lambda^{q^2} & & \\ & & & \ddots & \\ & & & & \lambda^{q^{k-1}} \end{pmatrix},$$

where $\lambda^{q^k-1} = 1$. Now let $n = n_1 + n_2 + \dots + n_s$. This partition determines a conjugacy class of Sym_n. Let w be an element of the conjugacy class given by the partition. Then the decomposition of w into disjoint cycles contains cycles of lengths $n_1, n_2, \dots, n_s$.

$$\overline{T}_{\sigma\circ w} \simeq (q^{n_1} - 1) \times (q^{n_2} - 1) \times \dots \times (q^{n_s} - 1).$$

Theorem. *Let $G = GL_n(q)$. Let T be a maximal torus corresponding to the partition $n = n_1 + n_2 + \dots + n_s$. Then*

$$T \simeq (q^{n_1} - 1) \times (q^{n_2} - 1) \times \dots \times (q^{n_s} - 1).$$

3.10 Elements of composite orders

R. W. Carter, Centralizers of semisimple elements in the finite groups of Lie type, Proc. London Math. Soc. (3), 1978, V. 37, N 3, P. 491–507.

R. W. Carter, Centralizers of semisimple elements in the finite classical groups, Proc. Lond. Math. Soc. (3), 1981, V. 42, N 1, P. 1–41.

Recall that every element in G can be presented as a product of a semisimple element and unipotent element.

$$g = su = us.$$

Hence g lies in $C_G(s)$. We have $C_G(s) = (C_{\overline{G}}(s))_\sigma$. $C_{\overline{G}}(s)^0$ is a connected centralizer. It contains s and all unipotent elements of $C_{\overline{G}}(s)$, thus it contains g. The connected centralizer is a reductive subgroup of maximal rank.

Every reductive subgroup of maximal rank in $\overline{G}$ is isomorphic to a group of the form

$$GL_{n_1}(\overline{F}_p) \times GL_{n_2}(\overline{F}_p) \times \dots \times GL_{n_s}(\overline{F}_p),$$

where $n_1 + n_2 + \dots + n_s = n$.

Every reductive subgroup of maximal rank in G is isomorphic to a group of the form

$$GL_{n_1}(q^{k_1}) \times GL_{n_2}(q^{k_2}) \times \dots \times GL_{n_s}(q^{k_s}),$$

where $n_1k_1 + n_2k_2 + \dots + n_sk_s = n$.

To describe the composite part of the spectrum it suffices to consider all reductive subgroups of the form

$$GL_{n_1}(q) \times T,$$

where T is a maximal torus of $GL_{n-n_1}(q)$.

Theorem. *Let q be a power of a prime p. Let $\nu_m(GL_n(q))$ consist of all numbers* $p^k[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ *with* $s \geqslant 1$ *and* $p^{k-1}+1+n_1+n_2+\cdots+n_s = n$.

Then $\mu_m(GL_n(q)) \subseteq \nu_m(GL_n(q)) \subseteq \omega(GL_n(q))$.

3.11 Spectrum of $PSL_n(q)$

Theorem. *Let $G = PSL_n(q)$, where $n \geqslant 2$ and q is a power of a prime p. Put $d = (n, q-1)$. Then $\omega(G)$ consists of all divisors of the following numbers:*

1) $\frac{q^n-1}{d(q-1)}$;

2) $\frac{[q^{n_1}-1, q^{n_2}-1]}{(n/(n_1,n_2), q-1)}$ *for* $n_1, n_2 > 0$ *such that* $n_1+n_2 = n$;

3) $[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ *for* $s \geqslant 3$ *and* $n_1, n_2, \ldots, n_s > 0$ *such that* $n_1+n_2+\ldots+n_s = n$;

4) $p^k\frac{q^{n_1}-1}{d}$ *for* $k, n_1 > 0$ *such that* $p^{k-1}+1+n_1 = n$;

5) $p^k[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ *for* $s \geqslant 2$ *and* $k, n_1, n_2 \ldots, n_s > 0$ *such that* $p^{k-1}+1+n_1+n_2+\ldots+n_s = n$;

6) p^k, *if* $p^{k-1}+1 = n$ *for* $k > 0$.

Let $G = PSL_5(3)$. $d = (n, q-1) = (5, 3-1) = 1$.

1) $\frac{q^n-1}{d(q-1)}$.

   $\frac{3^5-1}{1(3-1)} = 121 = 11^2$.

2) $\frac{[q^{n_1}-1, q^{n_2}-1]}{(n/(n_1,n_2), q-1)}$ for $n_1, n_2 > 0$ such that $n_1+n_2 = n$.

   $\frac{[3^4-1, 3-1]}{(5/(4,1), 3-1)} = 80 = 2^4 \cdot 5$.

   $\frac{[3^3-1, 3^2-1]}{(5/(3,2), 3-1)} = [26, 8] = 104 = 2^3 \cdot 13$.

3) $[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ for $s \geqslant 3$ and $n_1, n_2, \ldots, n_s > 0$ such that $n_1+n_2+\ldots+n_s = n$.

   No new elements.

4) $p^k\frac{q^{n_1}-1}{d}$ for $k, n_1 > 0$ such that $p^{k-1}+1+n_1 = n$.

   $3(3^3-1) = 78 = 2 \cdot 3 \cdot 13$.

   $3^2(3-1) = 18 = 2 \cdot 3^2$.

5) $p^k[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ for $s \geqslant 2$ and $k, n_1, n_2 \ldots, n_s > 0$ such that $p^{k-1}+1+n_1+n_2+\ldots+n_s = n$;

   $3[3^2-1, 3-1] = 24 = 2^3 \cdot 3$.

6) p^k, if $p^{k-1}+1 = n$ for $k > 0$.

$\mu(G) = \{121, 104, 80, 78, 24, 18\}$.

3.12 Spectrum of $P\Omega^{\pm}_{2n}(q)$

Theorem. *Let $G = P\Omega^{\varepsilon}_{2n}(q)$, where $n \geqslant 4$, $\varepsilon \in \{+,-\}$, q is a power of an odd prime p, and $(4, q^n - \varepsilon 1) = 4$. For $k \geqslant 1$ put $n(k) = (p^{k-1}+3)/2$. Then $\omega(G)$ consists of all divisor of the following numbers:*

1) $\frac{q^n-\varepsilon 1}{4}$;

2) $\frac{[q^{n_1}-\varepsilon_1 1, q^{n_2}-\varepsilon\varepsilon_1 1]}{d}$, *where* $n_1+n_2 = n$, $\varepsilon_1 \in \{+,-\}$, $d = 2$, *if* $(q^{n_1}-\varepsilon_1 1)_{\{2\}} = (q^{n_2}-\varepsilon\varepsilon_1 1)_{\{2\}}$, *and* $d = 1$ *otherwise;*

3) $[q^{n_1}+1, q^{n_2}+1, \ldots, q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1, \ldots, q^{n_s}-1]$ *for every* $s > 2$, *even* l, *if* $\varepsilon = +$, *and odd, if* $\varepsilon = -$, *and* $n_1, n_2, \ldots, n_s > 0$ *such that* $n_1+n_2+\cdots+n_s = n$;

4) $p^k\frac{q^{n-n(k)}\pm 1}{2}$ *for every* k *such that* $n(k) < n$;

5) $p^k[q^{n_1}+1, q^{n_2}+1, \ldots, q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1, \ldots, q^{n_s}-1]$ *for every* $s > 1$ *and* $n_1, n_2, \ldots, n_s > 0$ *such that* $n(k)+n_1+n_2+\cdots+n_s = n$;

6) $p[q \pm 1, q^{n_1}+1, q^{n_2}+1, \ldots, q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1, \ldots, q^{n_s}-1]$ *for every* $s > 1$, *even* l, *if* $\varepsilon = +$, *and odd, if* $\varepsilon = -$, *and* $n_1, n_2, \ldots, n_s > 0$ *such that* $2 + n_1 + n_2 + \cdots + n_s = n$;

7) $p[q \pm 1, \frac{q^{n-2}-\varepsilon 1}{2}]$;

8) p^k, *if* $n = n(k)$ *for some* k.

$\mu(P\Omega_{10}^{+}(9)) =?$.

A. A. Buturlakin, M. A. Grechkoseeva, The cyclic structure of maximal tori of the finite classical groups, Algebra and Logic, Springer US, vol. 46, no. 2, pp. 73–89.

A. A. Buturlakin, Spectra of finite linear and unitary groups, Algebra and Logic, Springer US, vol. 47, no. 2, pp. 91–99.

A. A. Buturlakin, The spectra of finite symplectic and orthogonal groups, to appear in Siberian Advances in Mathematics.

4 Petroglyphs

4.1 Frobenius Group

Definition (1). *Let* G *be a transitive permutation group of a set* Ω. *If* $G_\alpha \neq 1$ *while* $G_{\alpha\beta} = G_\alpha \cap G_\beta = 1$ *for every* $\alpha, \beta \in \Omega$, *then* G *is called a Frobenius group.*

Theorem (Frobenius). *Let* G *be a Frobenius group and* H *be a point stabilizer. If* $K = \{x \in G \mid \forall \alpha \in \Omega \quad \alpha x \neq \alpha\} \cup \{1\}$, *then* K *forms a normal subgroup in* G *of order* $|G : H|$.

Definition (2). *Let* G *be a semidirect product of a normal subgroup* K *by a subgroup* H. *If the centralizer* $C_K(h)$ *is trivial for every nontrivial* $h \in H$, *then* G *is called a Frobenius group with kernel* K *and complement* H.

Prove [2] ⇒ [1], considering the action of G on $\Omega = G/H$ by right multiplication.
Simple examples: $\mathrm{Sym}_3 \simeq 3 : 2$, $\mathrm{Alt}_4 = 2^2 : 3$.

Proposition. *Let* G *be a Frobenius group with kernel* K *and complement* H. *Then*

- K *is nilpotent, and is abelian if* $|H|$ *is even.*
- $\pi(K) \cap \pi(H) = \varnothing$, *and* $|H|$ *divides* $|K| - 1$.
- *Sylow* p*-subgroup of* H *is cyclic for odd* p, *and is cyclic or generalized quaternion for* $p = 2$.

$G = \langle a, b \mid a^{2^{\alpha-1}} = b^2 = c, c^2 = 1, a^b = a^{-1}\rangle$, $\alpha \geqslant 2$, is a generalized quaternion group

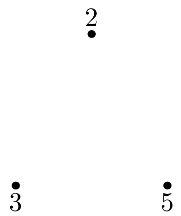
Definition. *A group* $G = ABC$ *is called* 2*-Frobenius, if* $A \trianglelefteq B$, $B \trianglelefteq C$, *and groups* $A : B$ *and* $B : C$ *are Frobenius.*

4.2 Definition and Examples

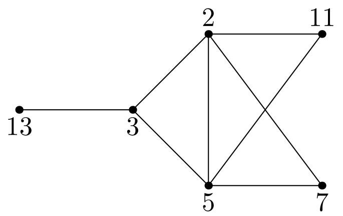
Let G be a finite group

The Gruenberg — Kegel graph $GK(G)$ (the prime graph of G)
Vertex set $V(GK(G)) = \pi(G)$ Edge set $E(GK(G)) = \{(r, s) | r, s \in \pi(G), r \neq s, rs \in \omega(G)\}$

Alt_5



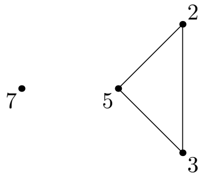
Alt_{16}

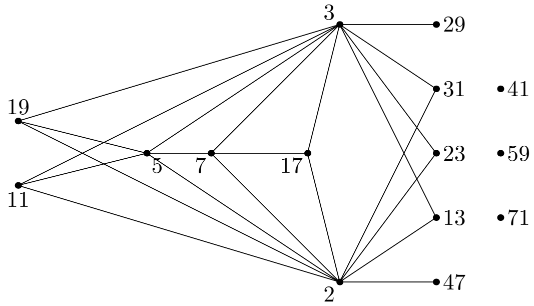


$M = F_1$

J_2

Sporadic Groups

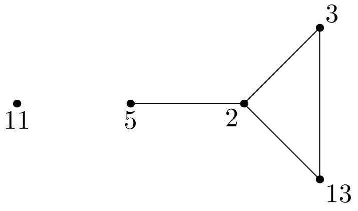


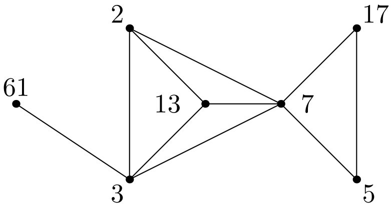


$PSL_5(3)$

$PSL_4(13)$

Linear Groups





4.3 Gruenberg — Kegel Theorem

- $s = s(G)$ is the number of connected component of $GK(G)$
- $\pi_i(G)$, $i = 1, \dots, s(G)$, is ith connected component
- if $2 \in \pi(G)$ put $2 \in \pi_1(G)$
- $\omega_i(G) = \{n \in \omega(G) \mid \pi(n) \subseteq \pi_i(G)\}$, $i = 1, \dots, s(G)$

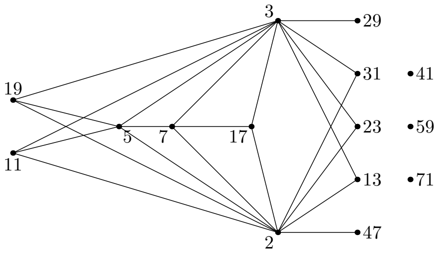
Theorem (Gruenberg — Kegel)**.** *If G is a finite group with $s(G) \geqslant 2$, then then one of the following holds:*

- *$s(G) = 2$ and G is a Frobenius or 2-Frobenius group;*
- *there exists a nonabelian simple group S such that*

$$S \leq \overline{G} = G/K \leq \mathrm{Aut}(S),$$

where K is the soluble radical of G; furthermore, K and $\overline{G}/S$ are $\pi_1(G)$-groups, $s(S) \geq s(G)$, and for every i, $2 \leq i \leq s(G)$, there is j, $2 \leq j \leq s(S)$, such that $\omega_i(G) = \omega_j(S)$.

Let $L = M$ be the Monster (the largest sporadic group), and G be a finite group with $\omega(G) = \omega(L)$.



$\omega(G) = \omega(L) \Rightarrow GK(G) = GK(L) \Rightarrow S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$

$s(S) \geqslant s(G) \geqslant 4$ and, up-to renumbering of indices, $\omega_2(S) = \{41\}$, $\omega_3(S) = \{59\}$, $\omega_4(S) = \{71\}$.

There are no such simple groups S except the Monster itself. It easy to verify due to the classification of simple groups with disconnected prime graph obtained by Williams and Kondrat′ev.
A nonabelian simple group L is called *quasirecognizable* (by spectrum) if every finite group G *isospectral* (= with the same spectrum) to L has a unique nonabelian composition factor S and $S \simeq L$.

Example on the previous slide demonstrates that the Gruenberg — Kegel Theorem not only allows to establish the existence of nonabelian factor S but helps to prove that $L \simeq S$.

The problem is what can be done if the prime graph of G is connected?

First result on the recognition by spectrum of simple groups with the connected prime graph was obtained in 2000 (cf. with the fact that the recognition problem for all sporadic groups has been solved in 1998).

Zavarnitsine, 2000: Alt_{16} is recognizable.

4.4 Cocliques and 2-cocliques

A *coclique* (or an *independent set of vertices*) of a graph Γ is any subset of vertex set consisting of pairwise non-adjacent vertices.
Let $\rho(\Gamma)$ be a coclique of maximal size in Γ. Its size $t(\Gamma) = |\rho(\Gamma)|$ is called the *independence number* of Γ.

Let $\Gamma = GK(G)$ be the prime graph of a finite group G.

- $\rho(G) = \rho(\Gamma)$ is a coclique of maximal size in $GK(G)$
- $t(G) = t(\Gamma)$ is the *independence number* of $GK(G)$

By analogy

- $\rho(r, G)$ is a coclique of maximal size in $GK(G)$ containing the prime r
- $t(r, G)$ is the *r-independence number* of $GK(G)$, i.e., the size of $\rho(r, G)$

Theorem (V,2005)**.** *Let G be a finite group with $t(G) \geq 3$ and $t(2, G) \geq 2$. Then*
(1) There exists a finite simple nonabelian group S such that $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ for maximal soluble normal subgroup K of G.
(2) For every coclique ρ of $\pi(G)$ with $|\rho| \geq 3$ at most one prime in ρ divides the product $|K| \cdot |\overline{G}/S|$. In particular, $t(S) \geq t(G) - 1$.
(3) One of the following holds:
(a) every prime $r \in \pi(G)$ non-adjacent in $GK(G)$ to 2 does not divide the product $|K| \cdot |\overline{G}/S|$; in particular, $t(2, S) \geq t(2, G)$;
(b) there exists a prime $r \in \pi(K)$ non-adjacent in $GK(G)$ to 2; in which case $t(G) = 3$, $t(2, G) = 2$, and $S \simeq Alt_7$ or $A_1(q)$ for some odd q.

Thus, if L is a finite simple group with $t(L) \geq 3$ and $t(2, L) \geq 2$, and G is a finite group with $GK(G) = GK(L)$, then for G the conclusion of the theorem holds.
Tools:

- lemma on insolubility of a group G with $t(G) \geqslant 3$ (Lecture 1)
- properties of Frobenius groups
- Brauer — Suzuki's theorem on a group with generalized quaternion Sylow 2-subgroups
- Gorenstein — Walter's classification of groups with dihedral Sylow 2-subgroups
- Steinberg's description of automorphisms of groups of Lie type

Which finite simple groups can the theorem be applied for?

Vasil'ev - Vdovin, 2005
For every finite nonabelian simple group G an arithmetical criterion of adjacency of vertices in the prime graph $GK(G)$ was given.

Using this criterion we determined for every finite simple group G

- at least one coclique $\rho(G)$ of maximal size in $GK(G)$, and so $t(G)$
- all cocliques $\rho(2, G)$, and so $t(2, G)$

- all cocliques $\rho(p,G)$ for groups of Lie type over a field of characteristic p, and so $t(p,G)$

Simple groups L with $t(L) < 3$:

- sporadic J_2
- alternating Alt_{10}
- exceptional ${}^3D_4(q)$
- classical $PSL_3(q)$, $(q-1)_3 \neq 3$, $q+1 = 2^k$; $PSU_3(3)$; $PSU_3(q)$, $(q+1)_3 \neq 3$, $q-1 = 2^k$; $PSp_4(q)$, $q \geqslant 3$; $PSp_6(2)$; $\Omega_8^+(2)$.

Alt_{10} is the only group from this list with connected prime graph

Simple groups L with $t(2,L) = 1$ are the alternating groups Alt_n satisfying the condition: there is no prime among the numbers $n, n-1, n-2, n-3$.

4.5 Adjacency criterion

Adjacency criterion
Let $L = Alt_n$ be an alternating group of degree n, $n \geqslant 5$.

- odd primes $r, s \in \pi(L)$ are adjacent iff $r + s \leqslant n$
- odd prime $r \in \pi(L)$ and 2 are adjacent iff $4 + r \leqslant n$

Remark. $t(L)$ increases with a growth of the degree n of L.

The criterion for groups of Lie type is substantially complicated and we need two number-theoretical facts to formulate it.

Given a prime r and a non-zero integer m, denote by m_r the highest r-power dividing m.

Lemma. *Let q be an integer, $|q| > 1$, m be a natural number.*
(1) *If odd r divides $q-1$ then $|q^m - 1|_r = m_r|q-1|_r$.*
(2) *If $q-1$ is divisible by 4 or m is odd then $|q^m-1|_2 = m_2|q-1|_2$. If $q+1$ is divisible by 4 and m is even then $|q^m-1|_2 = m_2|q+1|_2$.*

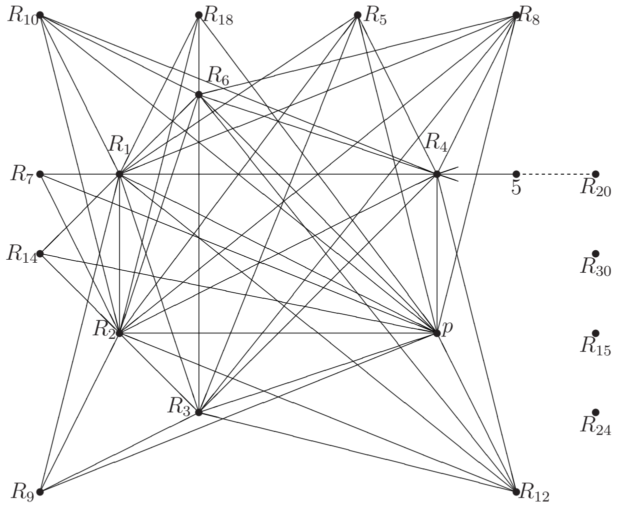
Zsigmondy primes
If q is a natural number greater than 1, r is an odd prime and $(q,r) = 1$, then $e(r,q)$ denotes a multiplicative order of q modulo r, that is a minimal natural number m with $q^m \equiv 1 \pmod r$. For an odd q, we put $e(2,q) = 1$ if $q \equiv 1 \pmod 4$, and $e(2,q) = 2$ otherwise.

Zsigmondy's theorem
Let q be a natural number greater than 1. For every natural number m there exists a prime r with $e(r,q) = m$ but for the cases $q = 2$ and $m = 1$, $q = 3$ and $m = 1$, and $q = 2$ and $m = 6$.

A prime r with $e(r,q) = m$ is called a *primitive prime divisor* of $q^m - 1$. By Zsigmondy's theorem such a number exists except for the cases mentioned above. Given q we denote by $R_m(q)$ the set of all primitive prime divisors of $q^m - 1$ and by $r_m(q)$ any element of $R_m(q)$.
On adjacency criterion for groups of Lie type
Let G be a finite simple group of Lie type with the base field of order q and characteristic p. It is well-known that every prime divisor of order of G is a primitive prime divisor of $q^i - 1$, where i is bounded by some function depending on the Lie rank of G. For simplicity suppose that G is not Suzuki or Ree group. Given a finite simple group G of Lie type, define a set $I(G) = \{i \mid \pi(G) \cap R_i(q) \neq \varnothing\}$. Notice that if $\pi(G) \cap R_i(q) \neq \varnothing$, then $R_i(q) \subseteq \pi(G)$. Thus, the following partition of $\pi(G)$ arises:

$$\pi(G) = \{p\} \cup \bigcup_{i \in I(G)} R_i(q).$$

As followed from an adjacency criterion, two distinct primes from the same class of the partition are always adjacent. Moreover, in most cases an answer to the question: whether two primes from distinct classes $R_i(q)$ and $R_j(q)$ of the partition are adjacent, depends only on the choice of the indices i and j.
Example. $G = E_8(q)$



5 is adjacent to any prime from R_{20} iff $5 \in R_4$ that is $q \equiv 2$ or $q \equiv 3$ modulo 5.

4.6 Linear Groups

Adjacency Criterion for Linear groups
Let $G = PSL_n(q)$ be a simple group over a field of characteristic p.
$|L| = q^{n(n-1)/2}(q^2-1)(q^3-1)\cdots(q^n-1)/(n, q-1)$.

Proposition (1). *Let r, s be odd primes and $r, s \in \pi(G) \setminus \{p\}$. Denote $k = e(r, q)$, $l = e(s, q)$ and suppose that $2 \leq k \leq l$. Then r and s are non-adjacent if and only if $k + l > n$ and k does not divide l.*

Proposition (2). *Let $r \in \pi(G)$ and $r \neq p$. Then r and p are non-adjacent if and only if one of the following holds:*

1. *r is odd, and $e(r, q) > n - 2$.*

6. *$n = 2$, $r = 2$.*

7. *$n = 3$, $r = 3$ and $(q-1)_3 = 3$.*

Proof. See the previous lecture.

Proposition (3). *Let r be a prime divisor of $q - 1$ and s be an odd prime distinct from the characteristic. Denote $k = e(s, q)$. Then s and r are non-adjacent if and only if one of the following holds:*

1. *$k = n$, $n_r \leq (q-1)_r$, and if $n_r = (q-1)_r$, then $2 < (q-1)_r$.*

2. *$k = n - 1$ and $(q-1)_r \leq n_r$.*

Proof. See the previous lecture and the lemma on $|q^n - 1|_r$.

5 Detective Story

5.1 Adjacency in Linear Groups

Recall that we discuss the criterion of adjacency in the prime graph of a finite group.

If q is a natural number greater than 1, r is an odd prime and $(q, r) = 1$, then $e(r, q)$ denotes the least natural number m with $q^m \equiv 1 \pmod r$. A prime r with $e(r, q) = m$ is called a *primitive prime divisor* of $q^m - 1$. Given q we denote by $R_m(q)$ the set of all primitive prime divisors of $q^m - 1$ and by $r_m(q)$ any element of $R_m(q)$.

Given a finite simple group G of Lie type with the base field of order q and characteristic p, we have the following partition:

$$\pi(G) = \{p\} \cup \bigcup_{i \in I(G)} R_i(q).$$

As follows from an adjacency criterion, two distinct primes from the same class of the partition are always adjacent. Moreover, in most cases an answer to the question: whether two primes from distinct classes $R_i(q)$ and $R_j(q)$ of the partition are adjacent, depends only on the choice of the indices i and j.

Adjacency Criterion for Linear groups

Let $L = PSL_n(q)$ be a simple group over a field of characteristic p.

$|L| = q^{n(n-1)/2}(q^2 - 1)(q^3 - 1) \cdots (q^n - 1)/(n, q - 1)$.

Proposition (1)**.** *Let r, s be odd primes and $r, s \in \pi(L) \setminus \{p\}$. Denote $k = e(r, q)$, $l = e(s, q)$ and suppose that $2 \leq k \leq l$. Then r and s are non-adjacent if and only if $k + l > n$ and k does not divide l.*

Proposition (2)**.** *Let $r \in \pi(L)$ and $r \neq p$. Then r and p are non-adjacent if and only if one of the following holds:*

1. *r is odd, and $e(r, q) > n - 2$.*
2. *$n = 2$, $r = 2$.*
3. *$n = 3$, $r = 3$ and $(q - 1)_3 = 3$.*

Proof. See the following theorem from Lecture 3.

Theorem. *Let $L = PSL_n(q)$, where $n \geqslant 2$ and q is a power of a prime p. Put $d = (n, q - 1)$. Then $\omega(L)$ consists of all divisors of the following numbers:*

1) $\frac{q^n - 1}{d(q-1)}$;

2) $\frac{[q^{n_1}-1, q^{n_2}-1]}{(n/(n_1,n_2), q-1)}$ *for $n_1, n_2 > 0$ such that $n_1 + n_2 = n$;*

3) $[q^{n_1} - 1, q^{n_2} - 1, \dots, q^{n_s} - 1]$ *for $s \geqslant 3$ and $n_1, n_2, \dots, n_s > 0$ such that $n_1 + n_2 + \ldots + n_s = n$;*

4) $p^k \frac{q^{n_1}-1}{d}$ *for $k, n_1 > 0$ such that $p^{k-1} + 1 + n_1 = n$;*

5) $p^k[q^{n_1} - 1, q^{n_2} - 1, \dots, q^{n_s} - 1]$ *for $s \geqslant 2$ and $k, n_1, n_2 \dots, n_s > 0$ such that $p^{k-1} + 1 + n_1 + n_2 + \ldots + n_s = n$;*

6) p^k*, if $p^{k-1} + 1 = n$ for $k > 0$.*

Proposition (3)**.** *Let r be a prime divisor of $q - 1$ and s be an odd prime distinct from the characteristic. Denote $k = e(s, q)$. Then s and r are non-adjacent if and only if one of the following holds:*

1. *$k = n$, $n_r \leq (q - 1)_r$, and if $n_r = (q - 1)_r$, then $2 < (q - 1)_r$.*
2. *$k = n - 1$ and $(q - 1)_r \leq n_r$.*

Proof. See the theorem and the lemma on $|q^n - 1|_r$.

Recall that for an odd q, we put $e(2, q) = 1$ if $q \equiv 1 \pmod 4$, and $e(2, q) = 2$ otherwise; and m_r is the highest r-power dividing m.

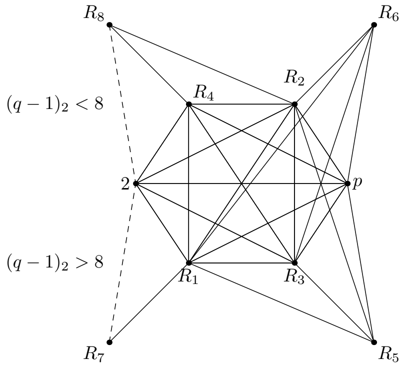
Lemma. *Let q be an integer, $|q| > 1$, m be a natural number.*

(1) *If odd r divides $q - 1$ then $|q^m - 1|_r = m_r|q - 1|_r$.*

(2) *If $q - 1$ is divisible by 4 or m is odd then $|q^m - 1|_2 = m_2|q - 1|_2$. If $q + 1$ is divisible by 4 and m is even then $|q^m - 1|_2 = m_2|q + 1|_2$.*

5.2 Cliques and Cocliques

Let us describe cocliques of maximal size in GK(L). We start with an example: $L = PSL_8(q)$, q odd



$\rho(L) = \{r_5, r_6, r_7, r_8\} \Rightarrow t(L) = 4$, and $\rho(p, L) = \{p, r_7, r_8\} \Rightarrow t(p, L) = 3$.

$\rho(2, L) = \{2, r_7, r_8\}$ and $t(2, L) = 3$ if $(q-1)_2 = 8$; and $t(2, L) = 2$ otherwise.

To describe the situation in general we assume that $n \geqslant 7$ (and $n \geqslant 12$ if $q = 2$) to avoid exceptions arising when n or q is small enough. Put $m = [n/2]$.

$\rho(L) = \{r_{m+1}, r_{m+2}, \ldots, r_n\}$ is a coclique of maximal size in $GK(L) \Rightarrow t(L) = [\frac{n+1}{2}]$.

Note also that the set $\{p\} \cup R_1 \cup \ldots \cup R_m$ is always a clique.

$\rho(p, L) = \{p, r_{n-1}(q), r_n(q)\} \Rightarrow t(p, L) = 3$.

If p is odd, then $\rho(2, L) \subseteq \{2, r_{n-1}(q), r_n(q)\}$ and $2 \leqslant t(2, L) \leqslant 3$.

5.3 Quasirecognition of Linear Groups

Now we try to quasirecognize $L = PSL_n(q)$.

Recall that L is quasirecognizable if every G with $\omega(G) = \omega(L)$ has exactly one nonabelian composition factor S, and $S \simeq L$.

How can we do that? In fact, there exists one very old approach...

Approach (Sherlock Holmes, 1890)
"...when you have eliminated the impossible, whatever remains, however improbable, must be the truth..."

If $L = PSL_n(q)$ is simple, then

- $t(2, L) \geqslant 2$ (= there is an odd prime r non-adjacent to 2)
- $t(L) = [\frac{n+1}{2}]$ and so it is an increasing function.

If G is a finite group with $\omega(G) = \omega(L)$, then

- $S \leqslant \overline{G} = G/K \leqslant \mathrm{Aut}(S)$, where S is nonabelian simple and K is the soluble radical of G
- if ρ is a coclique of $GK(L)$ of size at least 3, then primes from ρ (excepting at most one) do not divide $|K| \cdot |\overline{G}/S|$ and forms a coclique in $GK(S)$, in particular, $t(S) \geqslant t(L) - 1 = [\frac{n-1}{2}]$, so $t(S)$ increases together with $t(L)$.
- if a prime r is non-adjacent to 2, then r does not divide $|K| \cdot |\overline{G}/S|$ and so $r \in \pi(S)$.

In fact, the most of the above statements are wrong. However, all of them become true if n is sufficiently large (not as much as in Professor Olshanskiy's lectures though). Since we try to explain a general idea why S must be isomorphic to L, further we exploit the principle of taking n as large as we need (but we don't overreach 40).

5.4 Neither Sporadic, no Exceptional

An example of this principle:

Assume that S is a sporadic simple group. Then $t(S) \leqslant t(M) = 11$. For $n \geqslant 25$ we have $t(L) - 1 \geqslant [\frac{25+1}{2}] - 1 = 12 > t(S)$; a contradiction. In fact an elimination of sporadic group is easy anyway.

Since the Lie rank of exceptional groups is bounded (by 8), the size of maximal coclique is bounded as well (by $12 = t(E_8(q))$). Therefore, if $n \geqslant 27$, then S cannot be an exceptional group. To tell the truth, it's not so easy to prove that S is not an exceptional for $n < 27$.

Two possibilities remain: S is an alternating group or a classical group, and we need some additional information to move forward.

A divisor $k_i(q)$ of $q^i - 1$ is said to be the *greatest primitive divisor* if $\pi(k_i(q)) = R_i(q)$ and $k_i(q)$ is the greatest divisor with this property.

If $i \geqslant 3$, then $k_i(q) = \Phi_i(q)/(r, \Phi_{i_{r'}}(q))$, where $\Phi_i(x)$ is the ith cyclotomic polynomial and r is the largest prime dividing i, and if $i_{r'}$ does not divide $r-1$, then $(r, \Phi_{i_{r'}}(q)) = 1$.

In particularly, if i is prime, $k_i(q) = \frac{q^i-1}{(q-1)(i,q-1)} > q^{i-2}$.

5.5 Alternative of Alternating

$L = PSL_n(q)$ and $S \simeq \mathrm{Alt}_m$.

Suppose that for L there exists a set M of 3 positive integers with

$(*)$ for every $i \in M$ the number $k_i(q)$ is not equal to 1;

$(**)$ primitive prime divisors $r_i(q)$, $r_j(q)$, where $i, j \in M$, are non-adjacent in $GK(L)$ if $i \neq j$.

Consider the numbers $k_i(q)$ where i runs over M. We know that at least two of these primes are coprime to $|K| \cdot |\overline{G}/S|$ and lie in $\omega(S)$. Denote them by a and b. Assume that there exists a prime divisor r of a such that $r \leqslant m/2$. Since all the prime divisors of b are nonadjacent to r in $GK(G)$, all of them exceed $m/2$. It follows that either all primes from $\pi(a)$ or all primes from $\pi(b)$ are greater than $m/2$. Denote by k that of the numbers a and b which has this property.

Let $r', r'' \in \pi(k), r' \neq r''$. Then $r' + r'' > m \Rightarrow r'r'' \notin \omega(S) \Rightarrow r'r'' \in \omega(L) \setminus \omega(G)$, a contradiction. Let k be an r-power exceeding r. Then $r^2 > (m/2)^2 > m \Rightarrow r^2 \in \omega(L) \setminus \omega(G)$; a contradiction. Therefore, k is a prime, and the condition $k \in \omega(S)$ implies $m \geqslant k$. Thus, $m \geqslant k_i(q)$ for some $i \in M$.

Denote by p^l the p-period of L. As we know (Lecture 3)

$$p^{l-1} + 1 \leqslant n \leqslant p^l. \tag{1}$$

Assume for simplicity that $n \geqslant 17$ (it is our old trick again). Then there are at least three primes in $(n/2, n]$, and each of them is not less than $\max\{(n+1)/2, 11\}$. By adjacency criterion the set M consisting of three such primes satisfies the conditions $(*)$ and $(**)$. So for at least one prime $i \in M$ the number $k_i(q)$ is a prime and does not exceed m.

$i \geqslant \max\{(n+1)/2, 11\} \Rightarrow m \geqslant k_i(q) > \max\left\{q^{\frac{n-3}{2}}, q^9\right\}$.

$m > q^9 > p^7 + 1 \Rightarrow p^7 \in \omega(S)$. It follows $p^7 \in \omega(L)$ and $l \geqslant 7$. For $l \geqslant 7$ the inequality $l + 2 < (2^{l-1} - 2)/2$ holds, so $l + 2 < (p^{l-1} - 2)/2$.

(1) $\Rightarrow (p^{l-1} - 2)/2 \leqslant (n-3)/2$. Thus, $l + 2 < (n-3)/2$, so $m > q^{(n-3)/2} > p^{l+1}$, hence, $p^{l+1} \in \omega(G) \setminus \omega(L)$; which is impossible.

5.6 Classical Groups in the Same Characteristic

We obtained that S must be a classical group. Suppose $n \geqslant 4$, $L = PSL_n(p^\alpha)$ and $S = PSL_m(p^\beta)$, that is S is a group over the field of the same characteristic p as L. We start with two auxiliary facts which are true under our assumptions:

(1) $R_{i\gamma}(p) \subseteq R_i(p^\gamma)$

(2) $r \in \pi(L)$ and r is non-adjacent to p in $GK(L)$, then r is greater than 3 and does not divide $|K| \cdot |\overline{G}/S|$

Put $r_{n-1} = r_{(n-1)\alpha}(p)$ and $r_n = r_{n\alpha}(p)$. (1) $\Rightarrow r_{n-1} \in R_{n-1}(p^\alpha)$, $r_n \in R_n(p^\alpha)$. By adjacency criterion $\{p, r_{n-1}, r_n\}$ is a coclique in $GK(L)$, so (2) $\Rightarrow r_{n-1}, r_n \in \pi(S)$. Put $e_{n-1} = e(r_{n-1}, p^\beta)$, $e_n = e(r_n, p^\beta)$. By definition of primitive prime divisor, $e_{n-1}\beta = a(n-1)\alpha$ for a positive integer a.

$r_{n-1} \in \pi(S) \Rightarrow k_{e_{n-1}}(p^\beta)$ divides $|S|$. A prime $r_{e_{(n-1)\beta}}(p)$ divides $k_{e_{n-1}}(p^\beta)$, so it lies in $\pi(S) \subseteq \pi(L)$. Hence $e(r_{e_{n-1}\beta}(p), p^\alpha) \leqslant n$. But $e(r_{e_{n-1}\beta}(p), p^\alpha) = e(r_{a(n-1)\alpha}(p), p^\alpha) = a(n-1)$. It follows $a(n-1) \leqslant n$, hence $a = 1$ and $e_{n-1}\beta = (n-1)\alpha$.

By the same argument $e_n\beta = n\alpha$. In particular, $\frac{e_n}{e_{n-1}} = \frac{n}{n-1}$.

$\{p, r_{n-1}, r_n\}$ is a coclique in $GK(S) \Rightarrow \{e_{n-1}, e_n\} = \{m-1, m\}$. Now $e_n/e_{n-1} = n/(n-1) \Rightarrow m = n$. Moreover, $e_n\beta = n\alpha \Rightarrow \beta = \alpha$. Thus, $L \simeq S$.

The proof in case of other classical (or even exceptional) groups of the same characteristic is very similar but a little bit troublesome. Furthermore, the result for symplectic and orthogonal groups contains some exceptional cases which should be treated by a more subtle way (we'll see this later).

But how one can prove that S must have the same characteristic as L?

We'll discuss this problem tomorrow.

6 From Gap till Map

6.1 Gap

During the last lecture we were proving that the nonabelian composition factor S of group G isospectral to simple group $L = PSL_n(q)$ must be isomorphic L. We deduced that S must be a classical group, and if S has the same characteristic as L, we proved that $S \simeq L$. So to complete the proof we have to answer the question:

Why S must have the same characteristic as L?

In fact, I don't know the complete answer to this question. This is still an open problem, the most intriguing gap. However, I strongly believe that the answer can be obtained and, moreover, there is a general way to prove $S \simeq L$ for all L of sufficiently large dimension (say, for $n > 40$).

At first we show that this trouble can be overreached under additional assumption that $|L| = |G|$.

6.2 Shi Conjecture

Question 12.39, Kourovka Notebook, 1992
Is it true that a finite group and a finite simple group are isomorphic if they have the same orders and sets of element orders?

This question is inspired by

Conjecture (Shi Wujie, 1987)
Every finite simple group is uniquely determined by its order and spectrum in the class of all finite groups.

W. Shi, J. Bi, H. Cao, M. Xu, 1987,...,2003
Shi's conjecture is valid for all simple groups except symplectic and orthogonal groups (more precisely, except simple groups of Lie type D_n with n even, B_n and C_n).

Grechkoseeva, Mazurov and Vasil′ev, 2009
Shi's conjecture is true for remaining groups. It follows

Theorem
If L is a finite simple group, and G is a finite group with $|G| = |L|$ and $\omega(G) = \omega(L)$, then $G \simeq L$.

First of all, let us realize that if a simple group L is quasirecognizable, then it is recognizable by spectrum and order. In the previous lecture we deduced the problem of quasirecognizability of $L = PSL_n(q)$ to the case, when S is a classical group over a field of characteristic distinct from characteristic of L (for brevity we call it a cross-characteristic case). To prove the Shi Conjecture for $L = PSL_n(q)$ we consider this case under additional condition $|L| = |G|$.

It may seem strange that we handle the case of linear group established by Shi in 1990. But it is very logical from my point of view. Arguing as in our paper, you don't feel the difference treating any type of classical groups. On the other hand, Shi's arguments obviously fails for symplectic and orthogonal groups.

6.3 Proof

Proof. $L = PSL_n(q)$, $q = p^\alpha$, n is sufficiently large, G satisfies $\omega(G) = \omega(L)$, and $|G| = |L|$.
Since n is large, G has the unique nonabelian factor S, and by arguments from the previous lecture, we can suppose that S is a classical group over the field of characteristic $v \neq p$ and order $u = v^\beta$.
$|S|$ divides $|G| = |L| \Rightarrow |S|_v \leqslant |L|_v$.

$$|S|_v = \begin{cases} u^{m(m-1)/2}, \text{ if } S = PSL_m(u) \text{ or } PSU_m(u); \\ u^{m^2/2}, \text{ if } S = PSp_{2m}(u) \text{ or } \Omega_{2m+1}(u); \\ u^{m(m-1)}, \text{ if } S = P\Omega^{\varepsilon}_{2m}(u), \varepsilon = \pm \end{cases}$$

Thus, $u^{m(m-1)/2} \leqslant |S|_v$. Now we find an upper bound for $|L|_v$ in a way to prove that

$$u^{m(m-1)/2} \leqslant q^{3n/2} \qquad (2)$$

Since $v \neq p$, put $e(v,q) = i$ and $(q^i - 1)_v = v^k$. Then for $1 \leqslant j \leqslant n$

$$(q^j - 1)_v = \begin{cases} 1, \text{ if } i \nmid j; \\ (q^i - 1)_v (j/i)_v, \text{ if } i \mid j. \end{cases}$$

In fact, when $v = 2$, $(q-1)_2 = 2$, j is even, the last equation ought to be replaced by $(q^j-1)_v = (q^i+1)_v(j/i)_v$, but we forget about the case $v = 2$ for brevity.

Among the natural numbers not exceeding n, there are exactly $[n/i]$ numbers divisible by i; among them there are exactly $[n/iv^l]$ numbers divisible by iv^l. Therefore, $|S|_v$ is at most $v^{k[n/i]+t}$, where $t = \sum_{l=1}^{\infty}\left[n/iv^l\right]$. We have $t = \sum_{l=1}^{\infty}\left[\frac{n}{iv^l}\right] \leqslant \frac{1}{i}\sum_{l=1}^{\infty}\left[\frac{n}{v^l}\right] \leqslant \frac{1}{i}\left[\sum_{l=1}^{\infty}\frac{n}{v^l}\right] = \frac{1}{i}\left[\frac{n}{v-1}\right]$.

Since $v^k < q^i$, we have $|S|_v \leqslant$

$$\leqslant v^{k[n/i]+[n/(v-1)]/i} \leqslant v^{kn/i}\cdot v^{[n/(v-1)]/i} \leqslant q^{in/i}\cdot q^{[n/(v-1)]/k} \leqslant q^{3n/2}$$

.

$t(S) \geqslant t(L) - 1 = [(n-1)/2]$. However, $t(S)$ is a linear function of type $am + b$, where $1 \leqslant a \leqslant 2$ and $-5 \leqslant b \leqslant 5$ for every classical group S. Hence $n/(m-1) \leqslant$ const depends on type of S. On the other hand, the inequality (1) implies $u^m \leqslant q^{3n/(m-1)}$. Using information on $t(S)$ it easy to calculate that

$$u^m \leqslant q^{7/2} \tag{3}$$

Let k be the greatest element of $\omega(S)$, then by results on spectra of classical groups (see Lecture 3), we have $k \leqslant 2u^m$.

On the other hand, if $n \geqslant 17$, there are three primes in $(n/2, n]$, and (see arguments from the previous lecture) for at least two of them, say i and j, their greatest prime divisors $k_i(q)$ and $k_j(q)$ lie in $\omega(S)$. Thus,

$$q^{n/2} \leqslant k \leqslant 2u^m \tag{4}$$

Combining (2) and (3) we obtain $q^n \leqslant 4q^7$, which is obviously impossible for sufficiently large n. Theorem is proved.

Remark. It's worth saying that the treating of small n was most troublesome part of our proof of the Shi Conjecture.

We'll devote the rest of the lecture to overview of modern results on recognition just by spectrum.

For brevity we take an agreement to denote simple classical groups by one letter which points to its type. For example, $L_n(q) = PSL_n(q)$, $O_n^+(q) = P\Omega_n^+(q)$, and so on.

6.4 Just by Spectrum Again

- G is a finite group
- $h(G)$ is the number of pairwise non-isomorphic finite groups H with $\omega(H) = \omega(G)$
- G is *recognizable* (by spectrum) if $h(G) = 1$
- G is almost recognizable if $h(G) < \infty$
- G is non-recognizable if $h(G) = \infty$

Recognition problem
Given a finite group G, find $h(G)$. If $h(G)$ is finite, describe finite groups H with $\omega(H) = \omega(G)$.

There exist non-recognizable simple groups. For example, $h(\mathrm{L}_2(9)) = \infty$, since

$$\omega(L_2(9)) = \omega(V \leftthreetimes L_2(4)),$$

where V is the elementary abelian group of order 2^4.

Brandl-Shi, 1994
If $L = L_2(q)$ is a simple linear group and $q \neq 9$, then $h(L) = 1$.

Thus, almost all groups $L_2(q)$ are recognizable.
Shi, 1987; Mazurov-Xu-Cao, 2000; Zavarnitsine-Mazurov, 2007; Mazurov-Chen, 2008; Grechkoseeva, Grechkoseeva-Vasil′ev, 2008

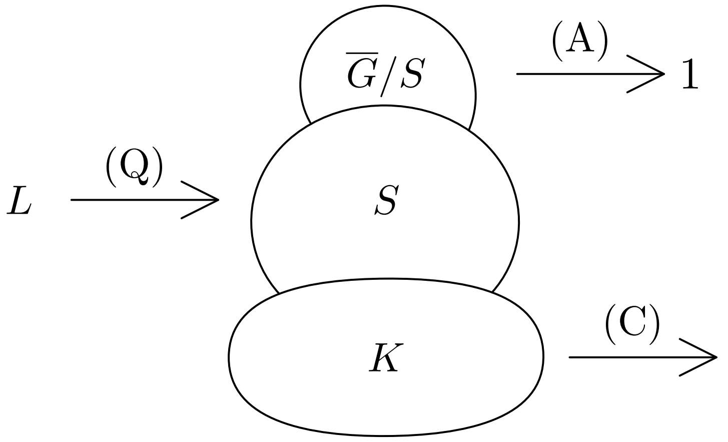
Theorem. *Let $L = L_n(q)$, where $n \geqslant 2$, $q = 2^k$, and let $d = (n, q-1)$.*
(1) If $n = 2^m + 1$ for some natural number m then $h(L) = 1$.
(2) If $n \neq 2^m + 1$ for any natural number m then $h(L)$ is equal the number of positive integers dividing the d-share of $(\frac{q-1}{d}, k)$. Moreover, a finite group G satisfies the equality $\omega(G) = \omega(L)$ if and only if G is isomorphic to a natural extension of L by a field automorphism of order dividing the d-share of $(\frac{q-1}{d}, k)$.
In particular, L is recognizable if and only if n is of the form $2^m + 1$ or $(d, \frac{q-1}{d}, k) = 1$.

Corollary
All simple linear groups over fields of characteristic 2 are almost recognizable.

Main Conjecture
“Almost all” nonabelian simple groups are almost recognizable.

For groups of Lie type “almost all” means “of almost all ranks”.
L is a nonabelian simple group, G is a group with $\omega(G)=\omega(L)$

$$S \leqslant \overline{G} = G/K \leqslant \mathrm{Aut}(S)$$



L is a nonabelian simple group

(Q) L is quasirecognizable if every G with $\omega(G)=\omega(L)$ has exactly one nonabelian composition factor S, and $S\simeq L$.

(C) L is recognizable among its coverings if for every G such that L is an homomorphic image of G the equality $\omega(G)=\omega(L)$ implies $G\simeq L$.

Note. If for L we prove (Q) and (C) then $L\leqslant G\leqslant \mathrm{Aut}(L)$.
In particular, L is almost recognizable.

(A) Describe groups G with $\omega(G)=\omega(L)$ and $L\leqslant G\leqslant \mathrm{Aut}(L)$

Solution of Recognition Problem
Achieve (Q), (C), and (A) for all nonabelian simple groups L

6.5 Map

	Sporadic	Alternating	Exceptional	Classical
Q	🟧	⬛	🟩	🟦
C	🟧	🟧	🟩	🟩
A	🟧	🟧	🟩	🟦

The problem is solved

🟧 completely 🟩 mostly 🟪 partially ⬛ poorly

Simple Groups Isospectral to Soluble Groups

Lucido, Moghaddamfar, 2004

Let L be a nonabelian simple group and G be a soluble group.

$\omega(L) = \omega(G) \Rightarrow L \in \{L_3(3), U_3(3), S_4(3), \mathrm{Alt}_{10}\}$.

Theorem

Let L be a nonabelian simple group. Then a soluble group G with $\omega(G) = \omega(L)$ exists if and only if $L \in \{L_3(3), U_3(3), S_4(3)\}$.

$L_3(3)$, Mazurov (2002);
$U_3(3)$, Zinov′eva (2003);
Alt_{10}, Staroletov (2008);
$S_4(3)$, Zavarnitsine (2010).

Sporadic Groups

Let L be a sporadic simple group.

Shi, 1988, ..., Shi-Mazurov, 1998

- If $L \neq J_2$, then $h(L) = 1$.
- If $L = J_2$, then $\omega(L) = \omega(V \leftthreetimes L_4(2))$, where V is the elementary abelian group of order 2^6, and $h(L) = \infty$.

Alternating Groups

Let $L = \mathrm{Alt}_n$, $n \geqslant 5$, be a simple alternating group.

(C) Zavarnitsine, Mazurov, 1999
If G is a covering of L, then $\omega(G) \neq \omega(L)$.

(A) If $n \neq 6$, then $\mathrm{Aut}(L) = \mathrm{Sym}_n$.
If $L < G \leqslant \mathrm{Aut}(L)$, then $G = \mathrm{Sym}_n$, and $\omega(G) \neq \omega(L)$.
(Q) Let L be a simple alternating group Alt_n, $n \geqslant 5$.

If $n = 6$, then $L \simeq L_2(9)$ and $h(L) = \infty$.
If $n = 10$, then there is a group G satisfying $\omega(G) = \omega(L)$ with a non-trivial soluble radical and a composition factor $S \simeq \mathrm{Alt}_5$.
If $n \neq 6, 10$ and either $n < 26$ or there is a prime in the set $\{n, n-1, n-2\}$, then $h(L) = 1$.

However, if there are no primes among the numbers $n, n-1, n-2, n-3$, nobody can even prove that a group G with $\omega(G) = \omega(L)$ has the only nonabelian composition factor.

Several years ago I. A. Vakula announced the following statement that seems provable.

If $\omega(G) = \omega(L)$ and p is the greatest prime $\leqslant n$, then among composition factors of G there is a factor $S \simeq \mathrm{Alt}_m$, where $p \leqslant m \leqslant n$.

Exceptional Groups of Lie Type

Let L be an exceptional group of Lie type over a field of characteristic p.

(Q) L is quasirecognizable
(unpublished for $L = E_7(q), q > 3$, which is my fault).

(C) It is sufficient to prove the following assertion.
If $L \in \{E_6^\varepsilon(q), E_7(q), {}^3D_4(q)\}$ and $G = V \leftthreetimes L$, where V is an elementary abelian p-group, then $\omega(L) \neq \omega(G)$.

(A) It is apparently valid (and mostly proved) that $\omega(G) \neq \omega(L)$ if $L < G \leqslant \mathrm{Aut}(L)$.

Conjecture (Question 16.24 in *Kourovka Notebook*)
If L is exceptional then there are no exceptions, and $h(L) = 1$.

Coverings of Classical Groups

Let L be a classical group of Lie type over field of characteristic p, and G be a covering of L. Proving $\omega(G) \neq \omega(L)$ we can assume that $G = V \rtimes L$ is a semidirect product of elementary abelian r-subgroup V and the group L.

Grechkoseeva, 2010
If $r \neq p$ and the dimension of L as a matrix group is greater than 5, then $\omega(G) \neq \omega(L)$.

Zavarnitsine, 2008
If $r = p$, L is a linear or unitary group of dimension other than 4, then $\omega(G) \neq \omega(L)$.

Is it true that $\omega(G) \neq \omega(L)$, if $G = V \rtimes L$ is a semidirect product of elementary abelian p-subgroup V and simple symplectic or orthogonal group L of dimension greater than 5?

Table

Zavarnitsine, 2006
Let H be a connected linear algebraic group over an algebraically closed field of characteristic p and φ be a surjective endomorphism of H. Given natural number r, put $H_r = C_H(\varphi^r)$. If H_r is finite for some r then φ is an automorphism of H_r of order r and

$$\omega((H_r)\langle\varphi\rangle) = \bigcup_{k|r} \frac{r}{k}\omega(H_k).$$

Example of Application:
Let $L = L_3(q)$, $q = p^n$, p an odd prime. Let G satisfy $L \leqslant G \leqslant \mathrm{Aut}(L)$ and $\omega(G) = \omega(L)$.
If $q \equiv 1 \pmod 3$ then $G = L\langle\rho^{3^i}\rangle$, where $0 \leqslant i \leqslant f$, $3^f||n$, and ρ is a field automorphism of L of order 3^f.
If $q \equiv 5, 9 \pmod{12}$ then $G = L\langle\gamma^i\rangle$, where $i = 0, 1$ and γ is a graph automorphism of L.
If $q \equiv 3, 11 \pmod{12}$ then $G = L$.

Theorem
Let L be a simple classical group over a field of characteristic p, and $L \notin \{L_2(9), L_3(3), U_3(3), U_3(5), U_5(2), S_4(3)\}$. Suppose G is a finite group with $\omega(G) = \omega(L)$ and S is the unique nonabelian composition factor of G. Then one of the following holds

- $S \simeq L$
- $L = S_4(q)$, where $q > 3$, and $S \simeq L_2(q^2)$
- $L \in \{S_6(q), O_7(q), O_8^+(q)\}$ and $S \in \{L_2(q^3), G_2(q), S_6(q), O_7(q)\}$
- $n \geq 4$, $L \in \{S_{2n}(q), O_{2n+1}(q)\}$ and $S \in \{O_{2n+1}(q), O_{2n}^-(q)\}$
- $n \geq 6$ is even, $L = O_{2n}^+(q)$ and $S \in \{S_{2n-2}(q), O_{2n-2}(q)\}$
- S is a group of Lie type over a field of characteristic $v \neq p$.

Grechkoseeva, Vasil′ev, Mazurov, 2009 (symplectic and orthogonal)
G., V., and Staroletov, 2010 (linear and unitary groups)
Remark. The results concerning symplectic and orthogonal groups take a considerable part in proving Shi's conjecture.

Quasirecognizability of Classical Groups

$L\diagdown S$	Sporadic	Alternating	Same Char	Other Char
L & U	🟧	🟧	🟧	🟦
S & O	🟧	🟧	🟩	🟦

The problem is solved

🟧 completely 🟩 mostly 🟦 partially ⬛ poorly

Thus, the conjecture on quasirecognizability of “almost all” simple classical groups is “almost” equivalent to the following

Conjecture
Let L be a simple classical group over field of characteristic p, and S be a nonabelian composition factor of a group G with $\omega(G) = \omega(L)$. Then for “almost all” groups L the factor S is not isomorphic to a group of Lie type over field of characteristic $v \neq p$.

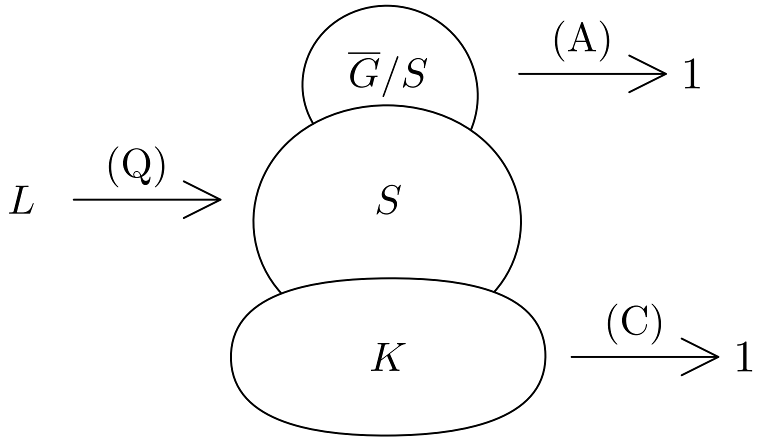
As I said in the beginning, I believe that the conjecture is true.

7 Last Labours

7.1 Two Problems

L is a nonabelian simple group, G is a group with $\omega(G) = \omega(L)$

$$S \leqslant \overline{G} = G/K \leqslant \mathrm{Aut}(S)$$



7.2 Automorphic Extensions

Recognition among Automorphic Extensions

Question 17.36, *Kourovka Notebook*
Find all finite nonabelian simple groups L such that for every of them there exists a finite group G isospectral to L and possessing a proper normal subgroup isomorphic to L. For every simple group L determine all groups G satisfying this condition.

It is easy to show that a group G must satisfy the condition $L < G \leqslant \mathrm{Aut}\, L$.

As we have seen at the last lecture, there is no problem at all for sporadic and alternating groups. Although the problem has not been completely solved for exceptional groups, it is very close to that. So one can assume that L is a classical simple group. Here I'll show only one auxiliary result on linear algebraic groups, and one example of its application.

Automorphic Extensions of Classical Groups

Zavarnitsine, 2006

Let H be a connected linear algebraic group over an algebraically closed field of characteristic p and φ be a surjective endomorphism of H. Given natural number r, put $H_r = C_H(\varphi^r)$. If H_r is finite for some r then φ is an automorphism of H_r of order r and

$$\omega((H_r)\langle\varphi\rangle) = \bigcup_{k|r} \frac{r}{k}\omega(H_k).$$

Example of Application:

Assume that $L = L_3(q)$, $q = p^n$, p is an odd prime. Let G satisfy $L \leqslant G \leqslant \mathrm{Aut}(L)$ and $\omega(G) = \omega(L)$.

If $q \equiv 1 \pmod 3$ then $G = L\langle\rho^{3^i}\rangle$, where $0 \leqslant i \leqslant f$, $3^f||n$, and ρ is a field automorphism of L of order 3^f.

If $q \equiv 5, 9 \pmod{12}$ then $G = L\langle\gamma^i\rangle$, where $i = 0, 1$ and γ is a graph automorphism of L.

If $q \equiv 3, 11 \pmod{12}$ then $G = L$.

7.3 Coverings

A finite group G is called a *covering* (or a *cover*) of a group H if H is a homomorphic image of G.

A group L is *recognizable by spectrum from its covers* if $\omega(G) \neq \omega(L)$ for every proper cover G of L.

First of all we prove the following

Proposition. *Let L be a finite group. Then L is recognizable by spectrum from its covers if and only if $\omega(L) \neq \omega(G)$ for every semidirect product $G = K \leftthreetimes L$, where K is an elementary abelian group and L acts on K absolutely irreducibly. Furthermore, if L is a simple group of Lie type or sporadic group, then L acts on K faithfully.*

Proof. $\Rightarrow$) is obviously true.

$\Leftarrow$) We prove sufficiency in a contrapositive form.

Step 1. Let G be a nontrivial covering of $L \simeq G/K$ of minimal order such that $\omega(G) = \omega(L)$. Let $r \in \pi(K)$, S be a Sylow r-subgroup of K, and let $N = N_G(S)$ be its normalizer in G. Then by Frattini argument, $G = KN$ and thus $N/(N \cap K) \simeq L$. Since G is minimal, we have $N = G$. It follows that K is nilpotent. Put $T = O_{r'}(K)\Phi(K)$, where $O_{r'}(K)$ is the maximal normal r'-subgroup of K, and $\Phi(K)$ is the Frattini subgroup of K. Then K/T is an elementary abelian r-group for a prime r. Since $(G/T)/(K/T) \simeq L$, we have $T = 1$ by minimality of G. Thus, K is an elementary abelian r-group.

Step 2. A group $L = G/K$ acts by conjugation on K. Indeed, if $y \in \overline{x} = Kx \in L$, then $z^y = z^{kx} = z^x$ for every element $z \in K$, so the action of L on K by $z^{\overline{x}} = z^x$ is correctly defined. Denote by $H = K \leftthreetimes L$ a natural semidirect product under this action. We prove that $\omega(H) \subseteq \omega(G)$, and so G can be replaced by H. Let $h = (\overline{x}, k) \in H$, where $\overline{x}$ is a coset from G/K with representative x and $k \in K$. Put $|\overline{x}| = n$. If $|h| = n$ or $|x| \neq n$, then there is nothing to prove. Thus $|h| = rn$, and so $1 \neq h^n = (\overline{x}, k)^n = (1, k^{\overline{x}^{n-1}} \dots k^{\overline{x}}k) \Rightarrow k^{x^{n-1}} \dots k^x k \neq 1$. Then $(xk)^n = x^n \cdot k^{x^{n-1}} \dots k^x k = k^{x^{n-1}} \dots k^x k \Rightarrow |(xk)| = rn = |h|$. Thus, $\omega(H) \subseteq \omega(G)$, and we may assume that G is a semidirect product.

Step 3. Let M be a proper L-invariant subgroup of K. Since $(G/M)/(K/M) \simeq L$, we have $M = 1$. Thus, L acts irreducibly on K. Assume that this action is not absolutely irreducible. Let F be an extension of $\mathbb{F}_r$ such that FL-module $K \otimes_{\mathbb{F}_r} F$ is reducible. Denote by K_0 the proper submodule of this module. As in the previous step, it is sufficient to show that $\omega(K_0 \leftthreetimes L) = \omega(L)$. Suppose to the contrary that $(k_0 x) \in K_0 \leftthreetimes L$ is an element of order nr not belonging to $\omega(L)$, (here we assume that $|x| = n$). Then again as in the previous step, the element $x^{n-1} + \ldots + x + 1$ considered as a linear transformation of K_0 is nonzero. This means that it is also nonzero as a linear transformation of K and hence G contains an element (kh) of order nr, a contradiction.

If L is a simple group of Lie type or sporadic group, then the adjacency criterion implies that the prime graph $GK(L)$ has the following property: for every $r \in \pi(L)$ there is $s \in \pi(L)$ such that $rs \notin \omega(G)$. Thus, the kernel of action of L on K cannot coincide with L. Therefore, it is trivial, and the action is faithful.

7.4 Frobenius Action

Definition. *Let G be a semidirect product of a normal subgroup N by a subgroup H. If the centralizer $C_N(h)$ is trivial for every nontrivial $h \in H$, then G is called a Frobenius group with kernel N and complement H.*

The next lemma is one of the main tools for recognizing from the covers.

Lemma. *Let $G = NH$ be a Frobenius group with kernel N and complement H. If V is a G-module over the algebraically closed field of characteristic r coprime to $|N|$, and N does not lie in the kernel of an action of G on V, then there exists a vector $v \in V$ such that the collection of vectors $\{vh \mid h \in H\}$ is linearly independent. If $T = V \leftthreetimes G$ is a natural semidirect product, then for every element $h \in H$ we can find an element $v \in V$ such that $|vh| = r|h|$.*

Proof. $G = NH$ acts on V over a.c.f. F of char r.

- For every $h \in H$ the group N consists of $[n, h]$, where n runs over N.
- If K is the kernel of an action, then $K < N$, and G/K is Frobenius with the kernel N/K. Taking G/K instead of G, assume that G acts faithfully on V.
- N is nilpotent $\Rightarrow$ H normalizes the center Z of every Sylow subgroup of N $\Rightarrow$ ZH is Frobenius, so assume that $N = Z$ is abelian.
- $(r, |N|) = 1 \Rightarrow V = [V, N] \oplus C_V(N)$.
- $[V, N]$ is a G-submodule $\Rightarrow$ assume $V = [V, N]$ and $C_W(N) = 0$ for every nontrivial submodule W of V $\Rightarrow$ V is an irreducible G-module.
- N is abelian $\Rightarrow$ there is 1-dimensional N-submodule W such that N acts nontrivially on W. Put $W = \langle v \rangle$.
- Define scalar function $\lambda : N \to F$ by $vn = \lambda(n)v$ and notice that $\lambda(n_1 \cdot n_2) = \lambda(n_1) \cdot \lambda(n_2)$.
- For $1 \neq h \in H$, $n \in N$, we have $(vh)n = v(hnh^{-1})h = v(n^{h^{-1}})h = \lambda(n^{h^{-1}})(vh) \Rightarrow Wh = \langle vh \rangle$ is N-submodule.
- If $\lambda(n^{h^{-1}}) = \lambda(n)$ for every $n \in N$, then $\lambda(hnh^{-1}n^{-1}) = 1$ for every $n \in N \Rightarrow \lambda(n) = 1$ for every $n \in N$, which is impossible.
- There is $n \in N$ with $\lambda(n^{h^{-1}}) \neq \lambda(n) \Rightarrow \{vh \mid h \in H\}$ is linearly independent.
- Take an element v in V such that $\{vh \mid h \in H\}$ is linearly independent, then $(vh)^{|h|} = v(h^{|h|-1} + \ldots + h + 1) \neq 0$ $\Rightarrow$ the order of vh in $T = V \rtimes G$ is equal to $r|h|$.

7.5 Applications

Applications $L = \mathrm{Alt}_5 \simeq SL_2(4) \simeq PSL_2(5)$.

$G = KL$ is a natural semidirect product, L acts on elementary abelian r-group K faithfully and absolutely irreducibly. Assume that $\omega(G) = \omega(L)$.

Suppose that $r = 2$. Consider a subgroup F of L isomorphic to Sym_3. F is a Frobenius group with a kernel N of order 3 and complement H generated by involution h. Applying the lemma, we obtain that K must contain an element k such that the element kh of KL is of order 4, which is impossible.

If $r \in \{3, 5\}$, then consider a subgroup $F \simeq \mathrm{Alt}_4$, which is Frobenius with elementary abelian kernel of order 4 and complement of order 3. Applying the lemma again, we derive that $3r \in \omega(G) \setminus \omega(L)$; a contradiction.

Let $L = M$ be the Monster.

$$\begin{aligned}\mu(M) \;&=\; \{32, 36, 38, 40, 41, 45, 48, 50, 51, 54, 56, 57, 59, 60, 62, 66, 68,\\ &\qquad 69, 70, 71, 78, 84, 87, 88, 92, 93, 94, 95, 104, 105, 110, 119\}\end{aligned}$$

The recognizability of L from its covers follows from existence of two Frobenius subgroups. Namely, L contains subgroups $A = 59 : 29$ and $B = 41 : 40$. Using A we can eliminate all possibilities except for $r = 3$. At the same time existence of B allows to construct an element of order 120 in any extension of elementary abelian 3-subgroup K by L.

7.6 Frobenius Subgroups in Linear Groups

Let $G = GL_n(q)$, $q = p^\alpha$, be a general linear group.

Consider the natural linear representation of G as a group of transformations of a space V over the field F of order q.

Denote by $W = \langle w \rangle$ a 1-dimensional subspace of V, and by H the stabilizer of W in G. Then H consists of all matrices of the shape

$$\begin{pmatrix} \lambda & 0 \\ v & A \end{pmatrix},$$

where $\lambda \in F^*$, $v' \in F^{n-1}$, $A \in GL_{n-1}(q)$.

The subset Q of matrices of the shape

$$\begin{pmatrix} 1 & 0 \\ v & E \end{pmatrix},$$

where E is identity matrix of size $(n-1)\times(n-1)$, is an elementary abelian normal p-subgroup of H.

The subset M of matrices of the shape

$$\begin{pmatrix} \lambda & 0 \\ 0 & A \end{pmatrix},$$

where $\lambda \in F^*$, $A \in GL_{n-1}(q)$, is a subgroup of H isomorphic to $F^* \times GL_{n-1}(q)$.

Moreover, $Q \cap M = 1$, so $Q : M$ is a semidirect product of Q by M.

Since Q is a p-group, it lies in $SL_n(q)$ and intersects with its center trivially. So its image $\overline{Q}$ in $L = PSL_n(q)$ is isomorphic to Q, and we identify Q with $\overline{Q}$. On the other hand, $M' = M \cap SL_n(q) \simeq GL_{n-1}(q)$ and $Z(SL_n(q)) \subseteq M'$. In particular, M' contains a cyclic subgroup X generated by an element x of order $q^{n-1}-1$. Denote by Y the image of X in L, then $|Y| = \frac{q^{n-1}-1}{(n,q-1)}$. Denote by F the subgroup $Q : Y$ of L.

Lemma. *The subgroup F of L is a Frobenius group with kernel Q, which is an elementary abelian p-group, and cyclic complement Y of order $\frac{q^{n-1}-1}{(n,q-1)}$.*

Corollary. *Let $L = PSL_n(q)$, $q = p^\alpha$ be a simple linear group. Then L is recognizable by spectrum from its covers if and only if $\omega(L) \neq \omega(G)$ for every semidirect product $G = K \leftthreetimes L$, where K is an elementary abelian p-group and L acts on K faithfully and absolutely irreducibly.*

Proof of the Corollary. If $G = K : L$, and K is an elementary abelian r-subgroup, where $r \neq p$, then we can apply the lemma on Frobenius action to the Frobenius group $F = Q : Y$. We obtain that $r\frac{q^{n-1}-1}{(n,q-1)} \in \omega(G)$. However, $\frac{q^{n-1}-1}{(n,q-1)} \in \mu(L)$, by the theorem on spectrum of L; a contradiction.

The proof of the lemma from the previous slide requires some additional information, so we prove a light version of this lemma here. Namely, let r be a primitive prime divisor of $q^{n-1}-1$, $Z = \langle z \rangle$ be a subgroup of cyclic complement Y such that $|z| = r$. We prove that $Q : Z$ is a Frobenius group. Indeed, by adjacency criterion, p is not adjacent to r in $GK(L)$. Therefore, $C_Q(z) = 1$, and $Q : Z$ is Frobenius.

The case when K is a p-group was handled by Mazurov and Zavarnitsine. The final result obtained by Zavarnitsine in 2008 is the following

Theorem. *Let $L = PSL_n(q)$ or $PSU_n(q)$, $q = p^m$ be a simple group. Suppose that either $n \geqslant 5$, or $n = 4$ and q is prime, or $n = 4$ and q is even. If L acts on a vector space W of characteristic p, then $\omega(W \leftthreetimes L) \neq \omega(L)$.*

Zavarnitsine has also constructed the example of $G = W \leftthreetimes L$ such that $\omega(G) = \omega(L)$, where $L = PSL_4(13^{24})$ and $\dim W = 96$.

7.7 Coverings of Classical Groups

Coverings of Classical Groups

Let L be a classical group of Lie type over field of characteristic p, and G be a covering of L. Proving $\omega(G) \neq \omega(L)$ we can assume that $G = V \leftthreetimes L$ is a semidirect product of elementary abelian r-subgroup V and the group L.

Grechkoseeva, 2010
If $r \neq p$ and the dimension of L as a matrix group is greater than 5, then $\omega(G) \neq \omega(L)$.

Zavarnitsine, 2008
If $r = p$, L is a linear or unitary group of dimension other than 4, then $\omega(G) \neq \omega(L)$.

Is it true that $\omega(G) \neq \omega(L)$, if $G = V \leftthreetimes L$ is a semidirect product of elementary abelian p-subgroup V and simple symplectic or orthogonal group L of dimension greater than 5?

8 Is the group $PSL_4(13)$ recognizable by spectrum?

8.1 Group $PSL_4(13)$ and its Order

$L = PSL_4(13)$ is the factor group of $SL_4(13)$ by center $Z(SL_4(13))$ of order $(4, 13-1)$.

Order?

$$|PSL_n(q)| = \frac{1}{(n,q-1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1).$$

$|L| = 13^{4(4-1)/2}(13^2-1)(13^3-1)(13^4-1)/(4, 13-1) =$

$$= 13^6 \cdot 2^7 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 17 \cdot 61$$

.

8.2 Spectrum of Linear Group

Theorem.

Let $G = PSL_n(q)$, where $n \geqslant 2$ and q is a power of a prime p. Put $d = (n, q-1)$. Then $\omega(G)$ consists of all divisors of the following numbers:

1) $\frac{q^n-1}{d(q-1)}$;

2) $\frac{[q^{n_1}-1, q^{n_2}-1]}{(n/(n_1,n_2), q-1)}$ *for* $n_1, n_2 > 0$ *such that* $n_1 + n_2 = n$;

3) $[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ *for* $s \geqslant 3$ *and* $n_1, n_2, \ldots, n_s > 0$ *such that* $n_1 + n_2 + \ldots + n_s = n$;

4) $p^k \frac{q^{n_1}-1}{d}$ *for* $k, n_1 > 0$ *such that* $p^{k-1} + 1 + n_1 = n$;

5) $p^k[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ *for* $s \geqslant 2$ *and* $k, n_1, n_2 \ldots, n_s > 0$ *such that* $p^{k-1} + 1 + n_1 + n_2 + \ldots + n_s = n$;

6) p^k, *if* $p^{k-1} + 1 = n$ *for* $k > 0$.

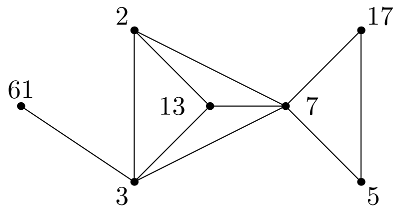
8.3 Spectrum of L

The apex of spectrum of L:

$$\mu(L) = \{156, 168, 546, 549, 595\} =$$
$$= \{2^2 \cdot 3 \cdot 13, 2^3 \cdot 3 \cdot 7, 2 \cdot 3 \cdot 7 \cdot 13, 3^2 \cdot 61, 5 \cdot 7 \cdot 17\}.$$

8.4 Prime Graph of L

$PSL_4(13)$



$\rho(L) = \{\{13 \text{ or } 2\}, 61, \{5 \text{ or } 17\}\}$	$t(L) = 3$
$\rho(13, L) = \{13, 61, \{5 \text{ or } 17\}\}$	$t(13, L) = 3$
$\rho(2, L) = \{2, 61, \{5 \text{ or } 17\}\}$	$t(2, L) = 3$

8.5 Structure Theorem

Theorem. *Let G be a finite group with $t(G) \geq 3$ and $t(2, G) \geq 2$. Then*

(1) There exists a finite simple nonabelian group S such that $S \leq \overline{G} = G/K \leq$ Aut(S) for maximal soluble normal subgroup K of G.

(2) For every coclique ρ of $\pi(G)$ with $|\rho| \geq 3$ at most one prime in ρ divides the product $|K| \cdot |\overline{G}/S|$. In particular, $t(S) \geq t(G) - 1$.

(3) One of the following holds:

(a) every prime $r \in \pi(G)$ non-adjacent in $GK(G)$ to 2 does not divide the product $|K| \cdot |\overline{G}/S|$; in particular, $t(2, S) \geq t(2, G)$;

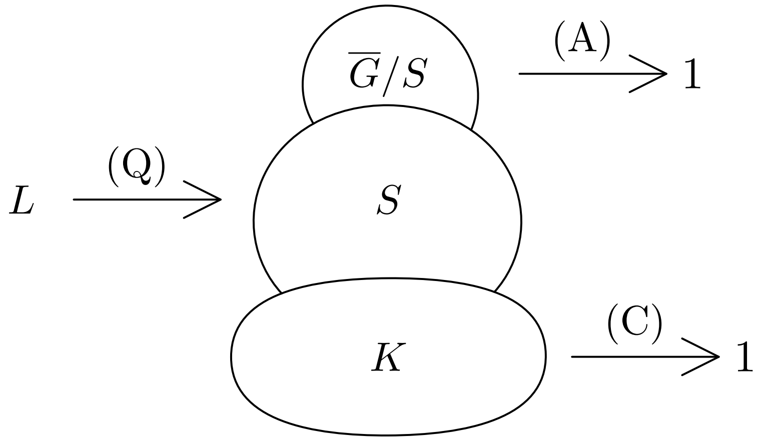
(b) there exists a prime $r \in \pi(K)$ non-adjacent in $GK(G)$ to 2; in which case $t(G) = 3$, $t(2, G) = 2$, and $S \simeq Alt_7$ or $PSL_2(q)$ for some odd q.

I.B. Gorshkov, V, 2009: If G satisfies the hypothesis and there is a nonabelian simple group L with $\omega(G) = \omega(L)$, then Item (3.a) of the conclusion must hold.

8.6 Scheme of Recognition

$L = PSL_4(13)$, G is a group with $\omega(G) = \omega(L)$

$$S \leqslant \overline{G} = G/K \leqslant \mathrm{Aut}(S)$$



8.7 Is L Quasirecognizable?

What do we know about S?

1. $\pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 13, 17, 61\}$
2. $\{61, 5, 17\} \subseteq \pi(S)$.

Let us check the list of simple groups satisfying these conditions.

There are no such groups except L itself. Thus, $S \simeq L$

Proposition. $L = PSL_4(13)$ *is quasirecognizable by spectrum.*

8.8 Is L Recognizable from Covers?

A finite group G is called a *covering* (or a *cover*) of a group H if H is a homomorphic image of G.
A group L is *recognizable by spectrum from its covers* if $\omega(G) \neq \omega(L)$ for every proper cover G of L.

Proposition. *Let L be a finite group. Then L is recognizable by spectrum from its covers if and only if $\omega(L) \neq \omega(G)$ for every semidirect product $G = K \leftthreetimes L$, where K is an elementary abelian group and L acts on K absolutely irreducibly. Furthermore, if L is a simple group of Lie type or sporadic group, then L acts on K faithfully.*

Lemma. *Let $G = NH$ be a Frobenius group with kernel N and complement H. If V is a G-module over the algebraically closed field of characteristic r coprime to $|N|$, and N does not lie in the kernel of an action of G on V, then there exists a vector $v \in V$ such that the collection of vectors $\{vh \mid h \in H\}$ is linearly independent. If $T = V \leftthreetimes G$ is a natural semidirect product, then for every element $h \in H$ we can find an element $v \in V$ such that $|vh| = r|h|$.*

Lemma. *The subgroup F of L is a Frobenius group with kernel Q, which is an elementary abelian p-group, and cyclic complement Y of order $\frac{q^{n-1}-1}{(n,q-1)}$.*

If $L = PSL_4(13)$, then $Q : Y = 13^3 : 549$. So for every $r \neq 13$ G contains element of order $549r$, which is impossible. Thus, $r = 13$.

Theorem (Zavarnitsine, 2008). *Let $L = PSL_n(q)$ or $PSU_n(q)$, $q = p^m$ be a simple group. Suppose that either $n \geqslant 5$, or $n = 4$ and q is prime, or $n = 4$ and q is even. If L acts on a vector space W of characteristic p, then $\omega(W \leftthreetimes L) \neq \omega(L)$.*

By the theorem, $K = 1$, so

Proposition. *If $L = PSL_4(13)$ and G with $\omega(G) = \omega(L)$, then $L \leqslant G \leqslant \mathrm{Aut}(L)$. In particular, L is almost recognizable.*

8.9 Automorphisms of L

By the Steinberg Theorem, every automorphism φ of a classical group L can be represented as

$$\varphi = \iota\delta\phi\gamma,$$

where

- ι is an inner automorphism
- δ is a diagonal automorphism
- ϕ is a field automorphism
- γ is a grpah automorphism

We are not interested in ι, and may assume that $\varphi = \delta\phi\gamma$.

Is there exists a field automorphism ϕ of $L = PSL_4(13)$?

No, since there is no a nonidentity automorphism of the base field.

Thus, assume that $G = L\langle\varphi\rangle$, where $\varphi = \delta\gamma$.

8.10 Is L Recognizable?

Suppose $\varphi = \gamma$ is a nontrivial graph automorphism, that is an automorphism induced by a symmetry of the Dynkin diagram of L.
In particular case of linear groups this automorphism can be represented as follows:
Consider the map $\gamma : GL_n(q) \to GL_n(q)$ defined by $A\gamma = (A^\top)^{-1}$.
Then $(AB)\gamma = A\gamma B\gamma$, so γ is an automorphism (obviously of order 2).
Since $\det(A\gamma) = \det(A^{-1})$, γ is an automorphism of $SL_n(q)$, and thus it induces an automorphism of $L = PSL_n(q)$.
For $n > 2$ this automorphism is not inner. Furthermore, it can be proved that $C_L(\varphi)$ contains section H isomorphic to $PSp_n(q)$

If $L = PSL_4(13)$ and $G = L\langle\gamma\rangle$, then $10 = 2 \cdot 5 \in \omega(G) \setminus \omega(L)$; a contradiction. Thus, $\varphi \neq \gamma$.
Suppose $\varphi = \delta$ is a nontrivial diagonal automorphism, that is a conjugation of L by a scalar matrix of $GL_n(q)$ (more precisely, by its image in $PGL_n(q)$) with the determinant not equal to 1. So $G = L\langle\delta\rangle$ is a subgroup of $PGL_n(q)$.

Let $L = PSL_4(13)$, and $G = L\langle\delta\rangle$. We may assume $|G : L| = 2$. Hence G is the subgroup of index 2 in $PGL_4(13)$. Therefore, $2 \cdot \frac{13^4-1}{(13-1)\cdot 4} = 1190 = 2 \cdot 5 \cdot 7 \cdot 17 \in \omega(G) \setminus \omega(L)$; a contradiction.

Finally, assume that $\varphi = \delta\gamma$, where δ, γ are both nontrivial, and $G = L\langle\varphi\rangle$, where $|G : L| = 2$. Since γ normalizes $PGL_n(q)$, δ can be chosen in $PGL_n(q)$ such that γ and δ commute. Then a Sylow 5-subgroup lies in the intersection of the centralizers of δ and γ in L. Therefore, it lies in the centralizer of φ in L. Thus, $10 \in \omega(G) \setminus \omega(L)$.

We proved the following theorem.

8.11 Final

Theorem (Participants of Erlagol Summer School, 2010)**.** *The group $L = PSL_4(13)$ is recognizable by spectrum*