What makes groups different?

James B. Wilson
Department of Mathematics

http://www.math.colostate.edu/∼jwilson

Why the interest in symmetry

Beyond aesthetics and curiosity, symmetry receives attention because:

- Symmetry reduces complex systems to manageable information, e.g. give me a basis, a generating set, etc. not the whole system.
- Presence/absence of symmetry exposes qualities in data, e.g. a rectangle is not a square – it has fewer symmetries.

Cayley's Theorem

All symmetries are representable as a groups acting on cosets.

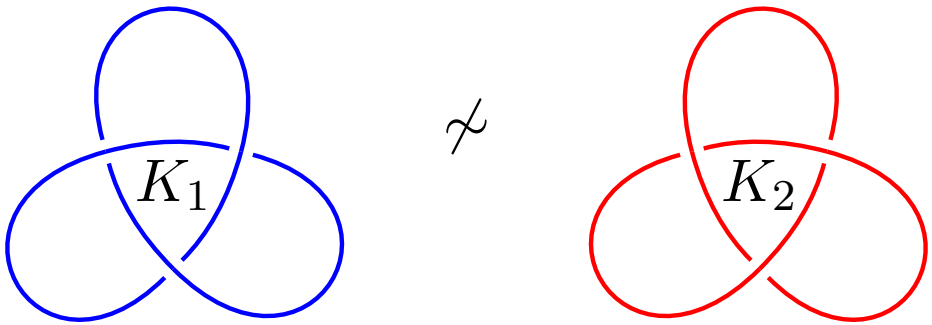
When do we know enough about a group?

"...one knows a group G when he can determine, given any other group H, whether or not G and H are isomorphic."

Joseph Rotman, The Theory of Groups, Allyn-Bacon, 1965, p.11.

This goes too far for some applications, but at times this is required.

A full use of group isomorphism (Dehn 1909)



- Mirror image implies an isomorphism $\phi : \pi_1(\mathbb{R}^3 - K_1) \to \pi_1(\mathbb{R}^3 - K_2)$, but negates crossing numbers.
- Compute generators T for automorphisms of $\pi_1(\mathbb{R}^3 - K_1)$.
- Confirm all $\tau \in T$ preserve crossing-numbers.
- Thus *all* isomorphisms $\pi_1(\mathbb{R}^3 - K_1) \to \pi_1(\mathbb{R}^3 - K_2)$ negate crossing-numbers. K_1 cannot be deformed to K_2.

How have we compared groups?

Classic homework assignment

Are the symmetries, D_8, of a square the same as the following?

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \qquad i^2 = j^2 = k^2 = -1, ij = k = -ji.$$

No.

D_8 has four flips, each of order 2,
In Q_8 only -1 has order 2.

Classic homework assignment

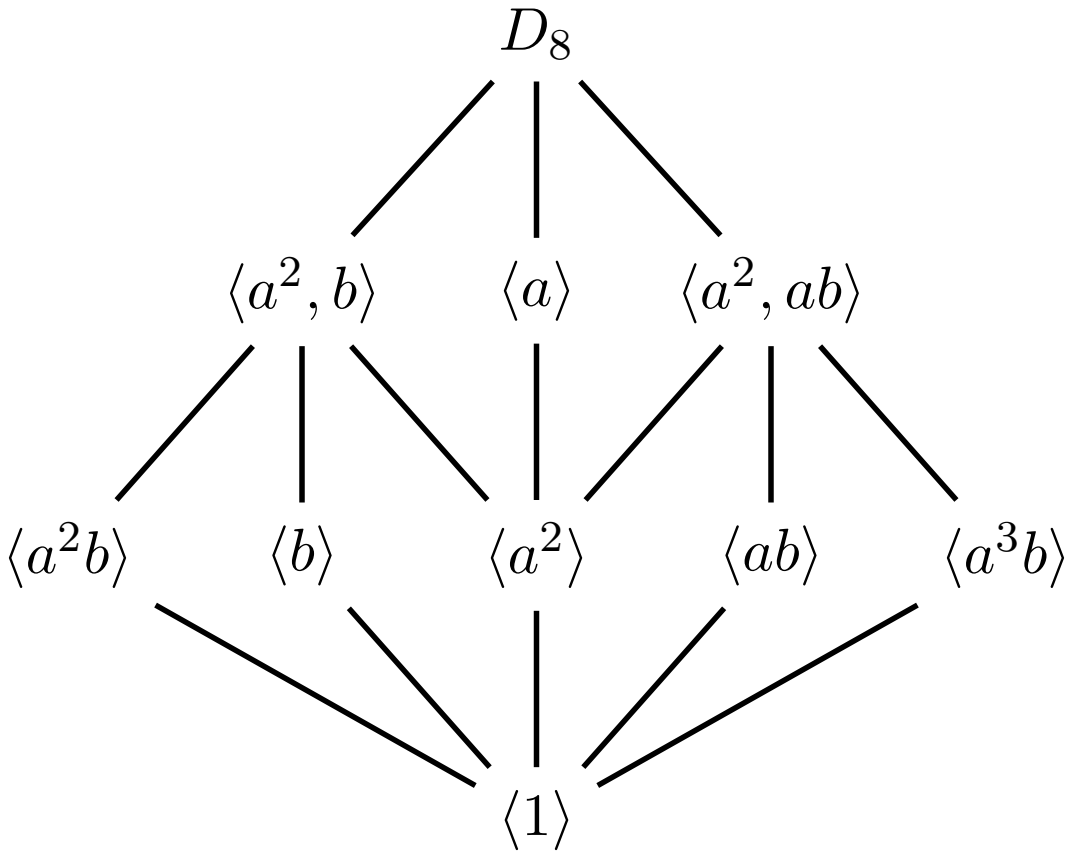
Are the symmetries, D_8, of a square the same as the following?

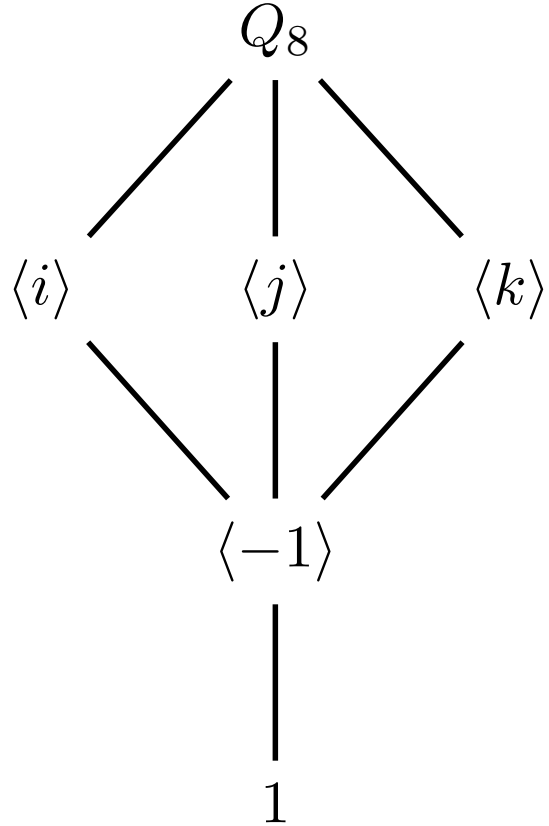
$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \qquad i^2 = j^2 = k^2 = -1, ij = k = -ji.$$

No.

D_8 has four flips, each of order 2,
In Q_8 only -1 has order 2.

Clearly different structure





Subgroup structure is not enough

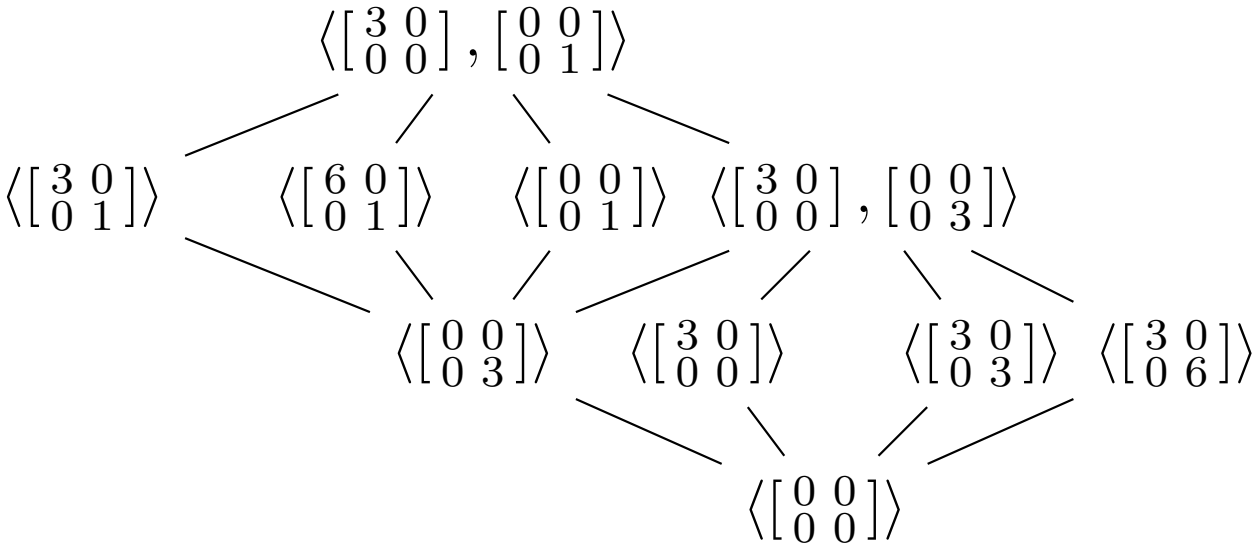
Consider

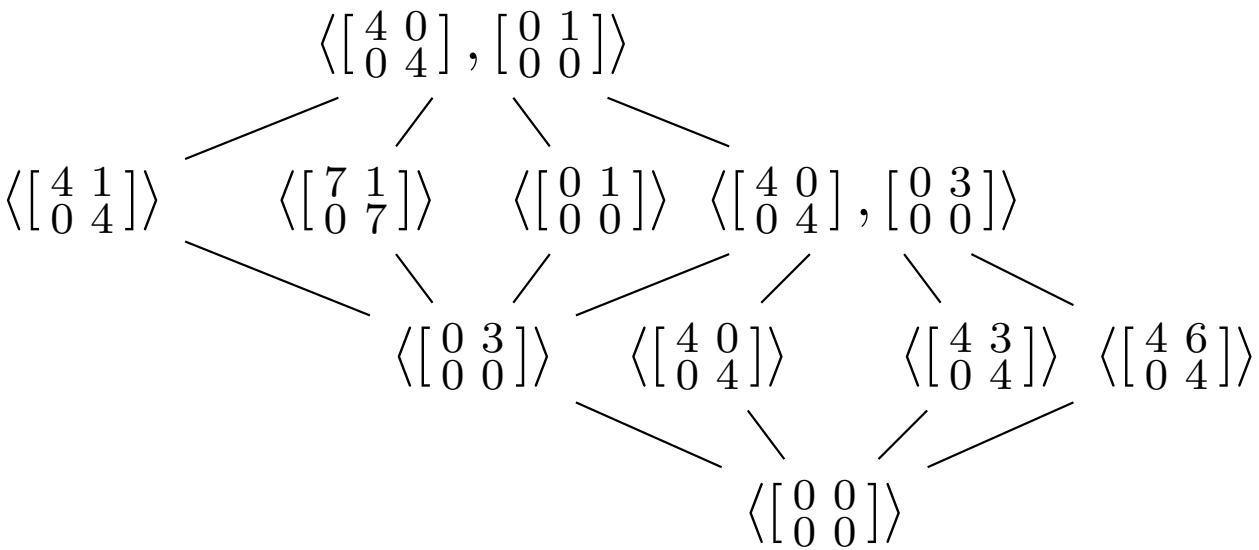
$$A = \left\{ \begin{bmatrix} 3a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{Z}/9\mathbb{Z} \right\}$$

$$B = \left\{ \begin{bmatrix} 4a & b \\ 0 & 4a \end{bmatrix} : a, b \in \mathbb{Z}/9\mathbb{Z} \right\}$$

A is abelian, B is not. We can tell that easy, but does the subgroup lattice say that easily?

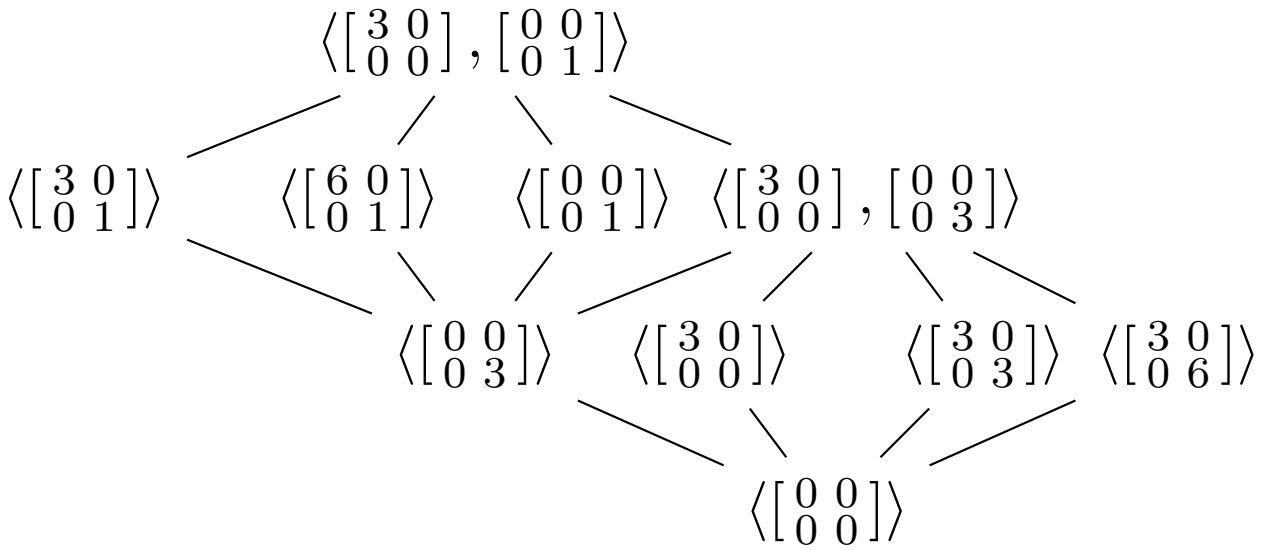
Subgroup structure is not enough

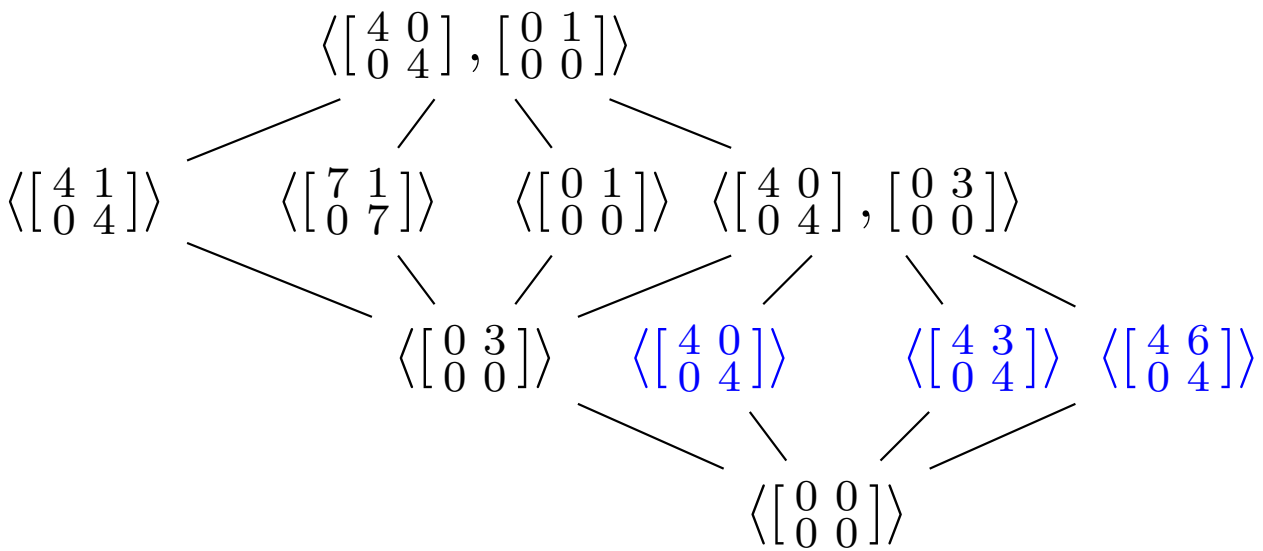




Subgroup structure is not enough

Color lattice with information like conjugacy and order.





Even colored lattices are not enough

Fix primes p and q with $q \equiv 1 \pmod{p}$. Let $\omega, \tau \in \mathbb{Z}_q^\times$ of order p.

$$R_{p,q}(\omega,\tau) = \left\{ \begin{bmatrix} 1 & x & y \\ 0 & \omega^i & 0 \\ 0 & 0 & \tau^i \end{bmatrix} : x, y \in \mathbb{Z}_q, i \in \mathbb{Z}_p \right\}$$

Theorem Rottländer 1928

The groups $R_{p,q}(\omega,\tau)$ have a common lattices of subgroups even when considering conjugacy classes and isomorphism types. Yet they are not in general isomorphic.

Differences in actions

Character tables are a devise that encodes how a group can act on a complex vector space. I.e. all the ways you will "see the group".
D_8 and Q_8 have equal character tables, but not when considering also p-th powers.

Dade, 1964

There are non-isomorphic groups with isomorphic character tables together with p-th powers.

Ideas that have worked.

- Triple character tables (keep track of 3 representations at once in the table, results in storing $g * h = k$ in the table).
- Colored table of marks (similar triplication of information stores $g * h = k$ in the data).
- Ellienberg-Maclane spaces (make a CW-complex where gluing stores relations of the group).

These isomorphism invaraints are substantially harder to compare than the groups they characterize, so they are not of use to the question of group isomorphism.

Gowers' Profiles

Objective

Tell two objects (groups) apart by calculating a list of isomorphism invariants and compare the lists for differences.

Invariants sofar either failed or were harder than isomorphism.

Constraint

Isomorphism invariants used only if easier to compute than it takes to compute isomorphisms.

Question: can we easily grow the list of invariants by a parameter and shut it off when we get enough information?

Gowers' threshold

Set $G_k = \{\langle g_1, \ldots, g_k \rangle : g_i \in G\}$.
$G_k/\cong$ can be calculated in time $|G|^k$; isomorphism takes $|G|^{O(\log |G|)}$.

Profile Threshold

$\kappa(G)$ is the minimum k where G is defined upto isomorphism by $G_k/\cong$.
$\kappa(n) = \max\{\kappa(G) : |G| = n\}$.

Gowers' Threshold Problem

Is $\kappa(n) \in O(1)$?

Known examples are not counter-examples

All groups G described above have $\kappa(G) \leq 3$.

Information theoretic lower bound

$\kappa(n) \in O(1)$ is reasonable, profiles have **exponentially** more possible information than necessary.

Sketch of proof. For a group G of order n, the minimum number $\epsilon_k(n)$ of k-generated subgroups needed to have enough information to characterize G upto isomorphism satisfies

$$\epsilon_k(n) - \frac{2\log n}{27k} \in \Omega(1/k).$$

The number of k-generated subgroups is $n^{O(k)} = \exp(O(k \log n))$. □

Strong support for Gower's intuition

- Groups are powerful because *logarithmic data* capture the whole.
- Profiles simply partition these data into small subgroups.
- Even if $\kappa(n) \in O(\log \log n)$ or less than $(1 - \varepsilon) \log n$, still an improvement.
- Heuristically unassailable: how could we ever study **all** $n^{\Theta(\log n)}$ subgroups of a large group to prove otherwise?!

Theorem Glauberman-Grobowski

For $p > 2$, $\kappa(p^\ell) \in \Omega(\sqrt{\ell})$.

Proof sketch. Make p-groups with a single interesting relation. Set

$$F = \left\{ \begin{bmatrix} 1 & & & u_1 & * & \cdots & * \\ & \ddots & & u_1 & \vdots & \ddots & \vdots \\ & & 1 & u_m & * & \cdots & * \\ & & & 1 & u_1 & \cdots & u_m \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} \right\}$$

Carefully chosen subgroups M and N of size p (one relation).
$F/M \ncong F/N$ yet it takes very large subgroups to encounter the one relation and expose the non-isomorphism. □

Generalizing?

The 1-relator replaced by 2, 3, $O(1)$ relators starts to imply short relations (formally theory of hyperbolic groups). So cannot play the game this way for much else.

Babai's Conjecture

$\kappa(n) \in O(\sqrt{\log n})$.

Note: $\kappa(n) \leq \log n$ by Lagrange's theorem, with a little more thought $\kappa(n) \leq \log n - 2$.

Theorem W.

For $p > 2$, $\kappa(p^\ell) = \ell - 2$ (recall $\kappa(n) \leq \log n - 2$ always).

... in fact

The family of groups used has all the following the same:

- Isomorphic character tables.
- Multiset of isomorphism types of proper subgroups.
- Multiset of isomorphism types of proper quotient groups.
- And a long and growing list of more technical invariants agree.

...oh, and size of the family grows at the rate $p^{\Theta(\ell)}$;
...one last thing, we can decide isomorphism in time $O(\ell^6 \log^2 p)$.

How to grapple with profiles

Profile Counting Theorem.

Let G be a finite p-group and M a maximal subgroup. Assume

1. $\forall M'$, M' maximal in G, $\exists \alpha$, an automorphism of G, $M^\alpha = M'$;
2. $d(G) = 1 + d(M)$.

Then $\forall J < G$, the profile map

$$J \mapsto |\{K < G : K \cong J\}|$$

Depends only on the isomorphism type of M, not G.

How to prove a claim about all subgroups?

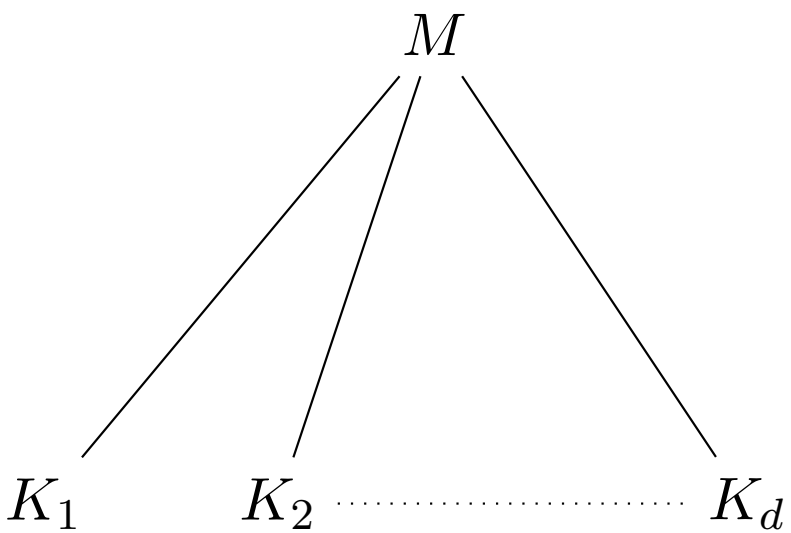
$\mathcal{M}$ the set of maximal subgroups; $\mathcal{J}(J) = \{K < G : K \cong J\}$.
$\Phi(X)$ is the intersection of maximal subgroups of X.

$$\mathcal{J}(J) = \bigsqcup_f \{K < G : K \cong J, |G : K\Phi(G)| = p^f\}.$$

Make a bipartite graph from $\mathcal{M}$ to
$\mathcal{J}(J, f) = \{K < G : K \cong J, |G : K\Phi(G)| = p^f\}$ by subgroup containment.

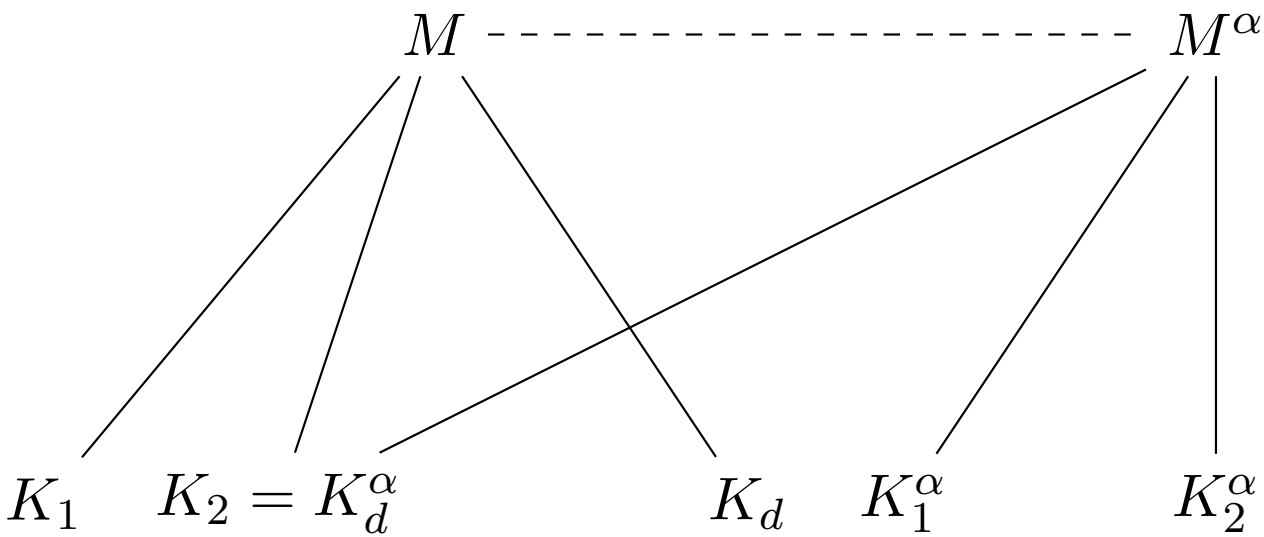
$\deg(M^\alpha) = |\{K \leq M : K \cong J, |M : K\Phi(M)| = p^{f-1}\}|.$

M maximal, $M \geq K_i \cong J$ and $|M : K_i\Phi(G)| = |M : K_i\Phi(M)| = p^{f-1}$



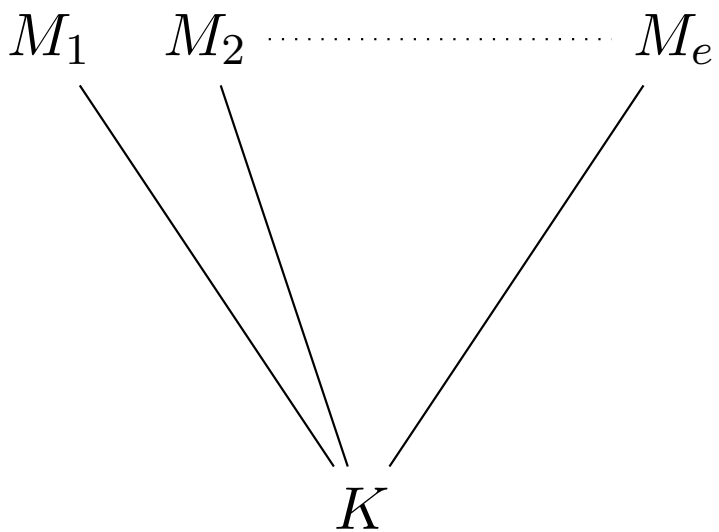
$$\deg(M^\alpha) = |\{K \leq M : K \cong J, |M : K\Phi(M)| = p^{f-1}\}|.$$

Degrees of M and M^α preserved by automorphism α



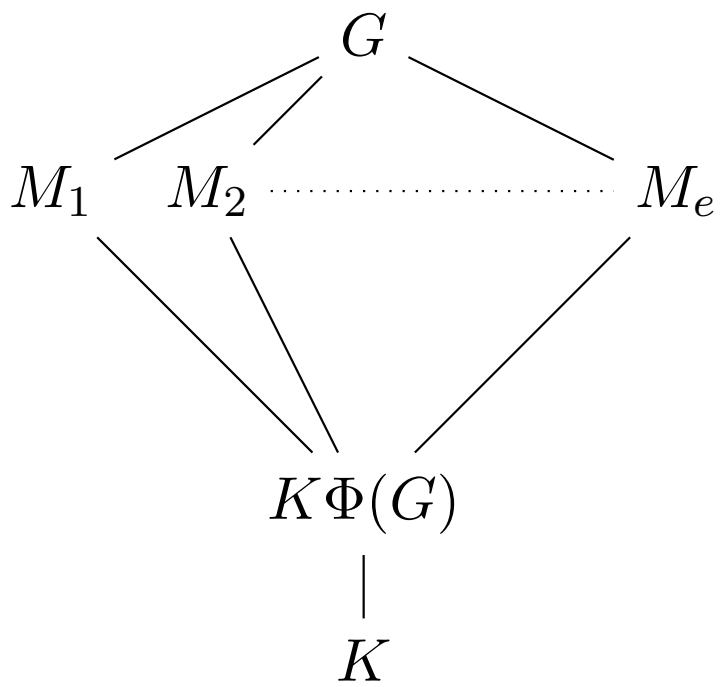
$\deg(K) = (p^{d(G)-f} - 1)/(p-1)$

$M \geq K \cong J$, $|M : K\Phi(M)| = p^{f-1}$, M_i maximal & $K \leq M_i$



$\deg(K) = (p^{d(G)-f} - 1)/(p-1)$

$\Phi(G) \leq M_i$ & $K \leq M_i$ implies $K\Phi(G) \leq M_i$



By Burnside basis theorem, $G/\Phi(G) \cong \mathbb{Z}_p^{d(G)}$.
$\{M_i/K\Phi(G)\}$ in bijection with hyperplanes in $G/K\Phi(G) \cong \mathbb{Z}_p^f$.

Proof of Profile Count

The bipartite graph $\mathcal{J}(J) \times \mathcal{M}$ is regular, so count edges 2 ways.

$$\sum_{M' \in \mathcal{M}} \deg(M') = \sum_{K \in \mathcal{J}(J,f)} \deg(K)$$

$$|\mathcal{M}| \cdot \deg(M) = |\mathcal{J}(J,f)| \cdot \deg(K)$$

$$\frac{p^{1+d(M)} - 1}{p-1} \cdot \deg(M) = |\mathcal{J}(J,f)| \cdot \frac{p^f - 1}{p-1}.$$

The size of $\mathcal{J}(J,f)$ is now a formula independent of G.

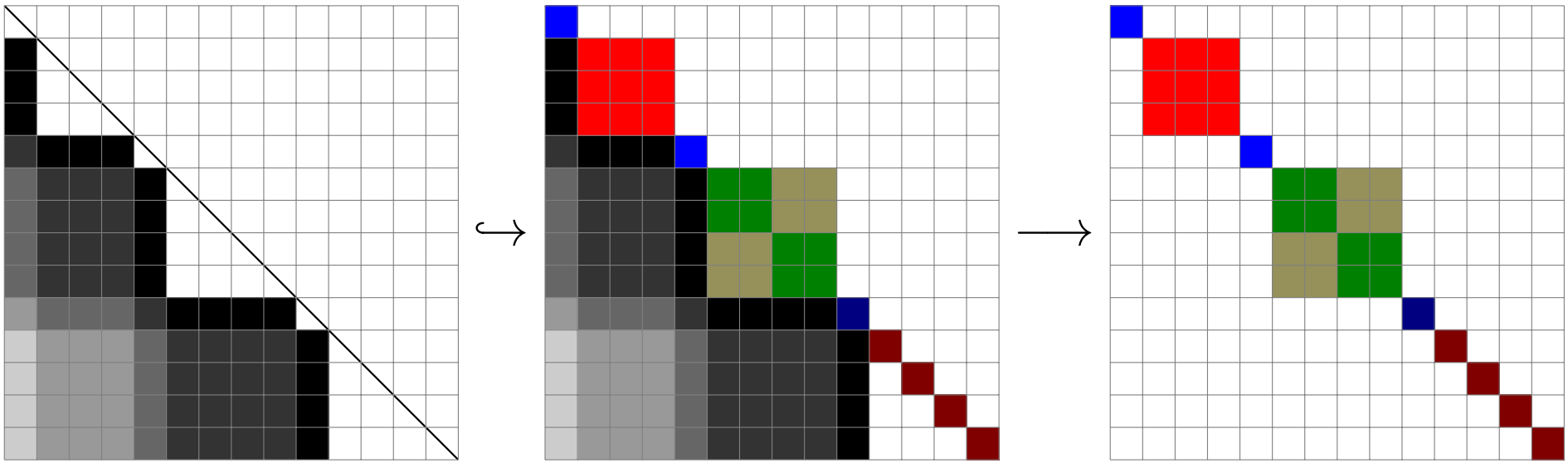
$$\sum_{f=1}^{1+d(M)} \frac{p^{1+d(M)} - 1}{p^f - 1} \cdot \left| \left\{ K \leq M : \begin{array}{c} K \cong J, \\ |M : K\Phi(M)| = p^{f-1} \end{array} \right\} \right|.$$

□

Exploring groups

Fitting Theory of finite groups

Finite groups split up into nilpotent + something like block diagonal + permutations of blocks.



When exploring what a group might do, thinking of actual matrices is often enough.

An ordinary group we can study

$L_1, \ldots, L_t$ are $(r \times s)$-matrices over numbers K.

$$B(L_1, \ldots, L_t) = \left\{ \left[\begin{array}{c|c|ccc} 1 & a & \multicolumn{3}{c}{c} \\ \hline & I_r & L_1 b^\dagger & \cdots & L_t b^\dagger \\ \hline & & \multicolumn{3}{c}{I_t} \end{array}\right] : \begin{array}{l} a \in K^r \\ b \in K^s \\ c \in K^t \end{array} \right\}.$$

Humble? Perhaps, yet on log-scale this approaches 50% of all possible finite groups.

Exploring subgroups

Easy subgroups of $B(L_1, \ldots, L_t)$, just limit a or b to a subspace.

$$\left\{ \left[\begin{array}{c|ccc|ccc} 1 & a_1 & \cdots a_{r-1} & 0 & \multicolumn{3}{c}{c} \\ \hline & \multicolumn{3}{c|}{} & \multicolumn{3}{c}{} \\ & \multicolumn{3}{c|}{I_r} & \multicolumn{3}{c}{L_1 b^\dagger \quad \cdots \quad L_t b^\dagger} \\ & \multicolumn{3}{c|}{} & \multicolumn{3}{c}{} \\ \hline & \multicolumn{3}{c|}{} & \multicolumn{3}{c}{} \\ & \multicolumn{3}{c|}{} & \multicolumn{3}{c}{I_t} \\ & \multicolumn{3}{c|}{} & \multicolumn{3}{c}{} \end{array}\right] : \begin{array}{l} a \in K^r \\ b \in K^s \\ c \in K^t \end{array} \right\}.$$

Effect the same as throwing out last row of each L_i.
Setting $b_j = 0$ same as removing column j from $L's$.

Example

Using row, column, and matrix insertion, we embed 3×3 upper triangular matrices over $\mathbb{F}_3$ into ones over $\mathbb{F}_9$. In this example we let $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$. We partition the matrices to help identify the row or column insertions.

$$\begin{aligned} B([1]) &\hookrightarrow B([1],[0]) \\ &\hookrightarrow B([1|0],[0|1]) \\ &\hookrightarrow B\left(\left[\begin{array}{cc} 1 & 0 \\ \hline 0 & -1 \end{array}\right], \left[\begin{array}{cc} 0 & 1 \\ \hline 1 & 0 \end{array}\right]\right) \end{aligned}$$

A larger example

$$B\left(\overbrace{\begin{bmatrix}1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0\end{bmatrix}}^{e}, \overbrace{\begin{bmatrix}0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1\end{bmatrix}}^{e}\right) \hookrightarrow$$

$$B\left(\left[\begin{array}{cccc}1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0\end{array}\right], \left[\begin{array}{cccc}0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1\end{array}\right]\right) = G.$$

$$\begin{bmatrix}0 & \cdots & & 1\end{bmatrix} \qquad \begin{bmatrix}a_0 & \cdots & & a_{e-1}\end{bmatrix}$$

So $2e = d(G) = 1 + d(M)$ and is not dependent on the $a_i's$
The a_i's certainly change isomorphism type of G, but M is maximal and always the same.

Final details

$$a(x) = a_0 + a_1 x + \cdots a_{e-1} x^{e-1} + x^e$$

$$G(a(x)) = B\left(\left[\begin{array}{cccc} 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \\ \hline 0 & \cdots & & 1 \end{array}\right], \left[\begin{array}{cccc} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ \hline a_0 & \cdots & & a_{e-1} \end{array}\right]\right)$$

Claim.

If $a(x)$ is irreducible then $\mathrm{SL}(2, \mathbb{F}_{p^e})$ acts as automorphisms of $G(a(x))$ and permutes the maximal subgroups of $G(a(x))$ transitively.

Proof. Let C be the companion matrix of $a(x)$.

$$B(I_n, C, C^2, \ldots, C^{e-1}) \to B(I_n, C) = G(a(x)).$$

That first group $B(I_n, C, \ldots)$ is the (3×3)-matrices over $\mathbb{Z}_p[x]/(a(x))$. Hence, $\mathrm{SL}(2, \mathbb{F}_{p^e})$ acts on it and as the identity on the $\Phi(B(I_n, C, \ldots))$, so that action passes to $G(a(x))$ and acts transitively the maximal subgroups. $\square$

Corollary

The groups $G(a(x))$ have the same subgroup profile.

Claim

$G(a(x)) \cong G(b(x))$ if, and only if, there is a Galois automorphism σ and a scalar s such that $sa(x) = b(x)^\sigma$. There are non-isomorphic $G(a(x))$.

Reflections

What I hope you learned from this.

- When conjecturing about groups think of large irregular blocked matrices.
- Model sub-/quotient groups as simple row-column removal.
- Isomorphism modeled as row-column operations.

I promise, this will explore the majority of groups and avoid the bias of textbook intuition, and still it is manageable. [1]

[1] All promises issued in this talk are worth exactly as much as you paid me to attend the talk.

Reflection

- Every attempt over the past century to capture isomorphism by a list of properties has failed.
- Perhaps it is time to admit that isomorphism is not an ad hoc list of properties we venerate as "structure" and say simply that isomorphism is the conclusion of a calculation.

Implication

Insofar as science uses symmetry to simplify complex systems:

Do the differences between groups we cannot explain matter?

To be serious about the question we would need to study coarser equivalences in algebra, I invite you to join me in this.