Finite groups with small automorphism groups

Robert A. Wilson

QMUL 7/10/04; Manchester 30/11/04

In this talk all groups are finite. This is joint work with John Bray [1].

I want to make this talk as gentle as possible, so I'll assume you know what a group is, but not necessarily what an automorphism group is.

Automorphisms. An *automorphism* of a group G is an isomorphism $\alpha : G \to G$. The automorphisms of G form a group under composition, called the *automorphism group*, $\mathrm{Aut}\, G$.

For any $g \in G$, the map $\phi_g : x \mapsto g^{-1}xg$ is an automorphism, and $\phi_g\phi_h = \phi_{gh}$ (reading from left to right), so the set of these ϕ_g is a subgroup of $\mathrm{Aut}\, G$, called $\mathrm{Inn}\, G$, the subgroup of *inner automorphisms*.

Also $\alpha^{-1}\phi_g\alpha = \phi_{g^\alpha}$ so $\mathrm{Inn}\, G$ is normal in $\mathrm{Aut}\, G$ and the map $\phi : G \to \mathrm{Inn}\, G : g \mapsto \phi_g$ is onto with kernel $\ker \phi = Z(G)$.

Example. If $G = C_n = \langle g \mid g^n = 1\rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ then $\alpha \in \mathrm{Aut}\, G$ is defined by $\alpha(g) = g^k$ say. But g^k must generate G so k is prime to n. Therefore $|\mathrm{Aut}\, G| = \phi(n)$, the number of positive integers less than n and prime to n (thus ϕ is Euler's totient function). E.g. if $n = 6$ then $\alpha : g \mapsto g^{\pm 1}$ only.

Properties of ϕ. First, $\phi(p) = p - 1$ and more generally $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$. If $n = p_1^{a_1}.p_2^{a_2}.\cdots.p_r^{a_r}$ where p_i are distinct primes, then $C_n = C_{p_1^{a_1}} \times \cdots \times C_{p_r^{a_r}}$ and $\phi(n) = \prod_{i=1}^{r} p_i^{a_i-1}(p_i - 1)$. Or to put it another way, $\phi(n)/n = \prod_{p|n}(1 - 1/p)$.

Abelian groups. The structure theorem for finite abelian groups implies in particular that any such group A is a direct product of uniquely determined abelian p-groups for different primes p. Thus $\mathrm{Aut}\, A$ is the direct product of $\mathrm{Aut}\, P$ as P ranges over these (Sylow) p-subgroups.

(In general $\mathrm{Aut}\, G \times \mathrm{Aut}\, H$ is a subgroup of $\mathrm{Aut}\,(G \times H)$, but may be a proper subgroup.)

Automorphisms of abelian p-groups. The structure theorem tells us that if A is a finite abelian p-group, then $\mathrm{Aut}\,A$ acts transitively on the elements in A of largest order. It is easy to see that there are at least $\phi(|A|)$ elements of this order, because the elements of smaller order form a proper subgroup, which has order at most $|A|/p$. Moreover, if g is any element of largest order then $A = \langle g\rangle \times B$, and provided A is not cyclic we have $|\mathrm{Aut}\,A| \geq \phi(|A|).|\mathrm{Aut}\,B| > \phi(|A|)$. We have proved:

Theorem 1 *If G is a finite abelian group, then $|\mathrm{Aut}\,G| \geq \phi(|G|)$, with equality if and only if G is (non-trivial) cyclic.*

Non-abelian groups. Question 15.43 of the Kourovka Notebook asks: is this true if the abelian condition is dropped?

In fact, the answer is no. A couple of counterexamples emerged quickly by thinking about quasisimple groups in the Atlas. (E.g. $G = 12M_{22}$ has order divisible by 2, 3, 5, 7, and 11, so $\phi(|G|)/|G| = \frac{1}{2}.\frac{2}{3}.\frac{4}{5}.\frac{6}{7}.\frac{10}{11} = \frac{16}{77}$ while $\mathrm{Aut}\,G = M_{22}.2$ so $|\mathrm{Aut}\,G|/|G| = \frac{1}{6}$ which is smaller.) But we have some easier examples now.

An example. The key is to create a group G with a large centre $Z(G)$ and small outer automorphism group $\mathrm{Out}\,G = \mathrm{Aut}\,G/\mathrm{Inn}\,G$. For example if $G = A_5$ we have $\phi(|G|)/|G| = \frac{1}{2}.\frac{2}{3}.\frac{4}{5} = \frac{4}{15}$ and $\mathrm{Aut}\,G = S_5$ so $|\mathrm{Aut}\,G|/|G| = 2$, and therefore $|\mathrm{Aut}\,G|/\phi(|G|) = 15/2$. But if $G = C_2 \times A_5$ we have the same value of $\phi(|G|)/|G|$, while $\mathrm{Aut}\,G$ is still S_5, so $|\mathrm{Aut}\,G|/\phi(|G|) = 15/4$. Indeed, we can go further, and put $G = C_2 \times C_3 \times C_5 \times A_5$, so that $\mathrm{Aut}\,G = C_2 \times C_4 \times S_5$, giving $|\mathrm{Aut}\,G|/\phi(|G|) = 2$. If only A_5 did not have an outer automorphism, we could get this down to 1!

Well, there are simple groups with no outer automorphisms, for example M_{11}, of order $2^4.3^2.5.11$. So $G = C_2 \times C_3 \times C_5 \times C_{11} \times M_{11}$ satisfies $|\mathrm{Aut}\,G|/\phi(|G|) = 1$ (work it out if you don't believe me).

Infinitely many counterexamples. More generally, there are infinite series of simple groups with trivial outer automorphism groups, e.g. $G_2(p)$ for p prime, $p > 3$; or $F_4(p)$ for p an odd prime; or $E_8(p)$ for any prime p. If S is any such simple group, and π is the set of prime divisors of $|S|$, then $G = S \times \prod_{p\in\pi} C_p$ satisfies $|\mathrm{Aut}\,G|/\phi(|G|) = 1$.

Proof. We have $\phi(|G|)/|G| = \prod_{p\in\pi}(1 - 1/p)$ and

$$|\mathrm{Aut}\,G| = |S|.\prod_{p\in\pi}(p-1) = |G|.\prod_{p\in\pi}(1-1/p) = \phi(|G|).$$

Thus we obtain infinite series of counterexamples to the second part of the conjecture. What about the first part? Can we lose the centre even faster than we gain outer automorphisms?

Even smaller automorphism groups. The magic ingredient is a group G_p of shape $p^{1+2}{:}SL_2(5)$. Such groups exist for all primes $p \equiv \pm 1 \pmod 5$. For the experts, here is a sketch of how they are constructed. The extraspecial group p^{1+2} of exponent p has outer automorphism group $GL_2(p)$, of which a subgroup $SL_2(p)$ centralizes the centre of the extraspecial group. Thus we can construct a group $p^{1+2}{:}SL_2(p)$ which has centre of order p. Any automorphism must act on the extraspecial group in such a way as to normalize $SL_2(p)$. It can be shown that the outer automorphism group is cyclic of order $(p-1)/2$, realized by 'scalars modulo ± 1'. This construction can be modified by replacing $SL_2(p)$ by $SL_2(5)$, which is a subgroup of $SL_2(p)$ whenever $p \equiv \pm 1 \pmod 5$.

Anyway, all that you need to know about G_p is

- its order is $2^3.3.5.p^3$;
- its centre has order p;
- its outer automorphism group has order $(p-1)/2$.

Dirichlet's theorem implies that there are infinitely many primes $p \equiv \pm 1 \pmod 5$, so we can choose a set π of such primes, with $|\pi|$ as large as we like. Let $G = \prod_{p\in\pi} G_p$.

Then we calculate that $\phi(|G|)/|G| = \frac{4}{15}\prod_{p\in\pi}(1-1/p)$ and $|\mathrm{Aut}\, G|/|G| = \prod_{p\in\pi}(p-1)/2p$ and therefore

$$|\mathrm{Aut}\, G|/\phi(|G|) = \frac{15}{4}.2^{-|\pi|}$$

which tends to zero as $|\pi|$ tends to infinity.

Of course there are some technical details in the proof which I have left out. For example, we need to prove carefully that $\mathrm{Aut}\, G$ is equal to the direct product of the $\mathrm{Aut}\, G_p$.

Conclusion. So the conjecture is true for abelian groups, but false for arbitrary groups. Indeed it is false for perfect groups (G is perfect if $G = G'$).

By replacing G_p by $p^{1+2}{:}2S_4$ for $p \equiv \pm 1 \pmod 8$ we can show it is false for soluble groups. Now

$$\text{abelian} \subset \text{nilpotent} \subset \text{supersoluble} \subset \text{soluble}$$

so is the conjecture true for nilpotent or supersoluble groups?

There is a longstanding conjecture that $|\mathrm{Aut}\, N| \geq |N|$ for nonabelian nilpotent groups N. If true, this would imply an affirmative answer to our question in this case. It is known for groups of nilpotency class 2. We suggest that the answer may even be affirmative for supersoluble groups—but only because we were unable to find a counterexample!

References

[1] J. N. Bray and R. A. Wilson, On the orders of automorphism groups of finite groups, *Bull. London Math. Soc.*, to appear.