From matrix groups to pro-finite groups and other matters

A Lecture for Galway

What classes of groups are we thinking about?

We are presented with a finite subset X of $\mathrm{GL}(d, K)$, for some field K in which precise computation is possible, and are asked to make some reasonable observations about $G := \langle X \rangle$. What should we do?

If K is a finite field, so that G too is finite, we know what questions to ask. What are the composition factors of G? The Sylow subgroups? Is G irreducible? What is more striking is that, after a vast effort by very many people, a project that has tended to dominate conferences on computational group theory is at last coming to fruition. Not only do we know what the questions are, but to a very great extent, and with much work still to do, we can answer them. That we should have got to where we are seemed unthinkable when the project started, and experts queued up (exaggeration here) to tell me why the project could not succeed.

So now we turn to infinite fields, and start again.

The primary difference between the finite and infinite case is ambition. In the finite case the objective has become to deal with all cases. In the case of $\mathrm{GL}(d, q)$ we aspire to understand any given subgroup in considerable detail for d up to say 240, and q up to 19^{17}. This is a slight exaggeration. There are not very interesting cases when we are defeated by integer factorisation or (more frequently) discrete log problems, and a few other issues remain unclear; but our basic objective, largely achieved, is to be able to do 'everything'. But in the infinite case, people are excited when they find a group that can be analysed; not when they find one that cannot.

The first objective, in the case of an infinite field, has been achieved. We can deal with the case when G itself is finite. If G is infinite then G (being linear) contains an element of infinite order, and we can construct such an element, as a word on X, and prove that it has infinite order. If, on the other hand, G is finite we can effectively reduce the problem to the case where the field is finite, and then the job is done.

So now G is infinite, and it is not so clear what questions we should ask. The Tits' alternative is the most obvious issue, and when this can be resolved, obviously important progress has been made. And if soluble-by-finite groups are too hard, we can consider polycyclic-by-finite groups.

However, I wish to suggest that we may be barking up the wrong tree.

Let R be the ring generated by the entries of $X \cup X^{-1}$; equivalently by the set of all entries of all elements of G. Then R is a residually finite Noetherian domain. If $\mathbf{a}$ is an ideal in R, let $G(\mathbf{a})$ be the kernel of the natural homomorphism of G into $\mathrm{GL}(d, R/\mathbf{a})$. By a theorem of Malcev, the intersection of the ideals of R of finite index is 0, and hence the intersection of the normal subgroups $G(\mathbf{a})$ as $\mathbf{a}$ varies over all ideals of finite index is trivial, and G is residually finite.

Let $\overline{G}$ denote the corresponding completion of G; that is, the inverse limit of all the groups $G/G(\mathbf{a})$ such that $R/\mathbf{a}$ is finite.

Suppose that Y is another finite subset of $\mathrm{GL}(d, R)$, and set $H := \langle Y \rangle$. If $\overline{G} = \overline{H}$, can we distinguish G from H, given X and Y? There is a problem about the assertion that $\overline{G} = \overline{H}$, in that an inverse limit is only defined up to isomorphism. So take $K = \langle X \cup Y \rangle$. Then $\overline{G}$ and $\overline{H}$ may be regarded as uniquely defined closed subgroups of $\overline{K}$, and then '$\overline{G} = \overline{H}$' becomes meaningful.

So here are some simple observations.

1. $\overline{G}$ is a theoretically more tractable object than G.

2. The most obvious tool for studying G is to look at the finite homomorphic images $G/G(\mathbf{a})$. If this is the only tool used in a computation then we are explicitly looking at $\overline{G}$, and not at G itself.

3. If we cannot distinguish G from H when $\overline{G} = \overline{H}$ then we *are* studying $\overline{G}$, and not G, whether we know it or not.

4. Only the more subtle group-theoretic properties of G are lost in passing to $\overline{G}$, so most questions will be more easily answered by working explicitly with $\overline{G}$.

5. If may often be important to be more drastic, and for some prime p work in $\overline{G}_p$, defined as the inverse limit of the images of G in $\mathrm{GL}(d, R/\mathbf{a})$ where $\mathbf{a}$ varies over all ideals of index a power of p for various primes p, so that $\overline{G}_p$ is virtually pro-p. We are particularly interested in the cases when $O_p(\overline{G}_p)$ is nontrivial; or better, infinite (that is to say, $\overline{G}_p$ is infinite).

In characteristic 0, when can we determine the set of primes p for which $\overline{G}_p$ is infinite?

6. The Tits' alternative. If G contains a free subgroup it would be good to exhibit one. But how can one prove that a subgroup of G is free; or even free on a given set? Observe that if Y is a subset of G then to say that Y freely generates a free group is far weaker than to say that the image of Y in $\overline{G}$ freely generates a free pro-finite group. So testing for freeness is perhaps not eased by passing to $\overline{G}$. When can we settle the Tits alternative?

7. What is sauce for the goose is sauce for the gander. It may be even more fruitful to work in $\mathrm{GL}(d, \overline{R})$, where $\overline{R}$ is the pro-finite completion of R, or in $\overline{R}_p$, where $\overline{R}_p$ is the inverse limit of $R/\mathbf{a}$, as $\mathbf{a}$ varies over all ideals of prime power index. Now the underlying space has changed, and the underlying geometry. If the characteristic polynomial of g in $R[t]$ was irreducible, it may factorise over $\overline{R}_p$. So even such a basic question as the irreducibility of the representation has changed.

Moral; ask not 'is the representation irreducible?', but rather 'over what primes is the representation irreducible?' Of course if we are in characteristic p no other prime arises here. But even then, localising helps. Local rings are far easier to deal with than global rings. So we want a meat axe that works locally rather than globally.

8. Division rings. We cannot avoid working over division rings, central simple algebras, orders in division rings, and so forth. If D is a division ring of finite index k over its centre F, and if V is a $D-F(G)$-bimodule of dimension d over D then V is also an $F(G)$-module of dimension dk^2 over F; but we do not want to throw this extra structure away; so we have to regard G as a subgroup of $\mathrm{GL}(d, D)$, not of $\mathrm{GL}(dk^2, F)$. There is an analogy here with finite fields. If we can write a matrix group over a finite field as a group of smaller dimension over a larger field (the original representation was probably irreducible, but certainly not absolutely irreducible) we do so. The larger field is in principle a nuisance; it may kill us because of problems with discrete logs; but we have to move up to the larger field. The same will happen here. We cannot assume that we are working over a commutative ring. Fortunately there is a great deal of useful theory concerning matrix groups over division rings that are of finite dimension over their centres. Unfortunately we will have to learn this theory.

Of course this is not the only road forwards. As in the finite case, we can hope to make progress geometrically. Instead of looking to ideals in R, or in $\overline{R}$, we can look for G-invariant subspaces of the given space, presumably as an $\overline{R}$-module. The extreme case, when there is a maximal invariant flag; that is to say, when G is triangularisable; is obviously particularly tractable. If G is irreducible, a proof that G is irreducible may shed light on the endomorphism ring of G, and at this point, division rings may appear.

We now have three ways of finding normal subgroups:

Congruence subgroups:

Geometric subgroups:

Kernels of localisation.

If we have a normal subgroup of finite index we can find all larger normal subgroups by going to the finite quotient. (Of course there may be too many such larger normal subgroups).

If we study $\overline{G}_p$ for some prime p it may still be difficult to get to grips with the kernel of the localisation map.

If we have a homomorphism of G onto a group K, there are two ways of trying to get into the kernel. We may be able to find a presentation of K on a suitable generating set. Alternatively, if we can construct random elements of G, and solve the explicit membership problem in K, we can find random elements of the kernel. If K is infinite the kernel may not be finitely generated. If it is finitely generated, and if K is finitely presented, and if we construct a finite generating set for the kernel, and if we can test for membership in this kernel, then we can prove that we have generated the whole kernel. Too many implausible conditions. The random method might possibly be of some help if we take $K = \overline{G}_p$ for some p. Even if K is infinite, if we can construct a large enough finite quotient of $\overline{G}_p$, then we can find good approximations to elements of the kernel. Whether such elements will be useful I don't know; but in the pro-finite case we are dealing in approximations.

In this context, we should consider $G/O^p(G)$, and again we need to decide which primes to take. So we need to look at G/G'. This may not be so easy. My simple trick for trying to prove that a group is perfect in the finite case makes serious use of element orders, and is in any case only a one-sided Monte Carlo algorithm. So I am pessimistic in the infinite case. But still, the question is important. So I ask, in ascending order of difficulty:

When can we decide if G is perfect?

When can we determine which primes divide the order of G/G'? (The answer is either a finite list, or 'all primes').

When can we determine the structure of G/G'?

Explicit membership in pro-finite groups

The explicit membership problem is as follows. Given a (finite) group G, and a subgroup $H = \langle Y \rangle$, and $g \in G$, then decide whether or not $g \in H$, and in the affirmative case, write g in terms of Y. If G and H are no longer finite, and H is topologically generated by Y, this question must be diluted, as the words required to write g in terms of Y may be infinite. In pro-finite groups we are only interested in closed subgroups, and as these are the intersections of sets of open subgroups then we can hope that restricting to open subgroups is not too serious a restriction; and it guarantees that the subgroup is topologically finitely generated.

So now suppose that we are looking for a version of explicit membership that will be valid in pro-finite groups, where H is an open subgroup of G. In the finite case we solve the problem by analysing H, dealing first with the case when H is simple, and having an algorithm for every type of simple group. So this is a major undertaking. In the present context it is unreasonable to assume any understanding of H, so we concentrate instead on the relation between H and G. Suppose then that we can find a normal open subgroup N of G that is contained in H (and hence in the core of H). Now we can decide whether $g \in G$ lies in H by seeing if the image of g in G/N lies in H/N, which we can do as we are dealing with finite images.

So I ask the following questions, in increasing order of difficulty, given a finite subset Y of G, and $H := \langle Y \rangle$.

When can we decide whether $\overline{H} = \overline{G}$?

When can we decide if $\overline{H}$ is open in $\overline{G}$?

Given a positive answer to the previous question, when can we find an ideal $\mathbf{a}$ in R of finite index such that $G(\mathbf{a})$ is contained in the core of $\overline{H}$?

We may need to be able to answer this last question to have an adequately constructive answer to the membership problem in $\overline{H}$. In cases where we do not expect to be able to answer these questions we may have to restrict to open subgroups that are given in the form $\overline{G}(\mathbf{a})$ for some explicit $\mathbf{a}$ or overgroups of such subgroups.

Classical groups

Dealing with classical groups in the finite case has proved to be (and is still proving to be) a major effort, that has triggered important theoretical work and a wide range of rather subtle algorithms. Implicit recognition, explicit recognition, odd characteristic, even characteristic, natural representation, other equi-characteristic representations, black box, presentations for the groups, constructive membership. So dealing with classical groups over infinite rings requires courage. None the less, there are fundamentally important generalisations of the concept of classical groups, and fundamentally important theorems, that need to be made constructive.

Suppose now that every element of X has determinant 1. One of the first questions to ask is whether $G = \mathrm{SL}(d, R)$; or perhaps, more reasonably, whether $\overline{G} = \mathrm{SL}(d, \overline{R})$. But there is already a problem. Let $\mathrm{E}(d, R)$ denote the subgroup of $\mathrm{SL}(d, R)$ generated by the elementary matrices. If $d > 2$ then $\mathrm{E}(d, R)$ is a normal subgroup of $\mathrm{SL}(d, R)$, and the quotient is an abelian group. However, if A is any abelian or countably infinite abelian group, then there is a division ring R of finite dimension over its centre such that $\mathrm{SL}(d, R)/\mathrm{E}(d, R)$ is isomorphic to A. We are interested in the case where R is not a division ring, but is residually finite. This will not force $\mathrm{SL}(d, R)/\mathrm{E}(d, R)$ to behave. So I ask:

If $g \in \mathrm{SL}(d, \overline{R})$, when can we decide whether $g \in \mathrm{E}(d, \overline{R})$?

If S is a Euclidean ring then $\mathrm{E}(d, S) = \mathrm{SL}(d, S)$ and the question disappears.

Another critical question is:

Given $X \subset \mathrm{SL}(d, R)$, determine whether $G = \langle X \rangle$ is dense in $\mathrm{SL}(d, \overline{R})$.

Is it the case that if $G \leq \mathrm{SL}(d, \mathrm{Z})$ then $G = \mathrm{SL}(d, \mathrm{Z})$ if and only if the natural map of G into $\mathrm{SL}(d, \mathrm{Z}/p)$ is onto for any sufficiently large prime p? Since $\mathrm{SL}(d, \mathrm{Z})$ contains a non-abelian free group if $d > 1$ the requirement that the map be natural is essential.

I think that an even more important question; perhaps the most central question of all; is 'Is G a full subgroup of $\mathrm{GL}(d, K)$?'

There are various equivalent definitions of a full subgroup of $\mathrm{GL}(d, D)$, where D is a division ring. For our purposes the following definition, though only valid for $d > 2$, is the most suitable.

Let $d \geq 3$, and let $G \leq \mathrm{GL}(d, D)$. Then G is *full* if and only if there is a subring R of D, with ring of quotients D, and a non-zero ideal $\mathbf{a}$ of R, such that G contains $\mathrm{E}(d, \mathbf{a})$.

So the full subgroups are the big subgroups.

Note that $\mathrm{E}(d, R)$ is finitely generated if R is a finitely generated as a ring. ($\mathrm{E}(2, R)$ is finitely generated if R is finitely generated as an abelian group).

Is it the case that most pairs of elements of $\mathrm{E}(d, \overline{R})$ generate $\mathrm{E}(d, \overline{R})$?

One of the critical properties of full groups is that they are only related by the obvious isomorphisms; that is to say, isomorphisms arising from module isomorphisms, field isomorphisms, and inverse-transpose.

I think that the question of deciding whether or not G is a full subgroup of $\mathrm{GL}(d, K)$ should not only be tractable, but is also fundamental. If this question can be answered (or when it can be answered) for the discrete group (and the discrete ring), we can ask for a constructive version that finds an appropriate ideal $\mathbf{a}$, and finds the Steinberg generators in terms of the given generators. (One needs a variant of the Steinberg generators as there are infinitely many Steinberg generators in general). And so forth. In many cases $\mathrm{E}(d, \mathbf{a})$ is finitely presented. So there are ambitious goals to be attempted. What is the relation between G being a full subgroup of $\mathrm{GL}(d, R)$ and $\overline{G}$ being a full subgroup of $\mathrm{GL}(d, \overline{R})$?

Random elements

Using product replacement is fine if we are working in $\overline{G}$. The elements produced can be defined by straight line programs, and then evaluated over finite rings. Moreover we have the Haar measure, and product replacement constructs evenly distributed elements with respect to this measure (asymptotically speaking). But if we are going to work in the discrete group G, and work with matrices over the discrete ring R, then entry explosion, being exponential, will limit the length of word we can use. Since product replacement increases word length exponentially it is no longer an appropriate tool. One has to decide on the word length that one can tolerate, and hope that random words of that length will give reasonably random elements of G, there being no measure on G that will define 'random' usefully.

Summary:

Philosophy:

In general, we need to form the appropriate completion; both of the the group and of the ring. For example: produce a meat axe for complete local rings.

We need to deal with full subgroups in the spirit that we deal with the special linear group in the finite case. We can then attack groups that preserve forms.

Calculate $K_1(R)$, and other invariants of R and $\overline{R}$, such as Krull dimension, and the *stable rank* of R. A vector v in R^k is *unimodular* if there is a vector w in R^k such that the inner product $v.w = 1$. Then R satisfies the stable range condition S_k if, for every unimodular vector $(r_0, r_1, \ldots, r_k)$ in R^{k+1} there exist $s_1, \ldots, s_k$ such that if $r'_i = r_i + s_i r_0$ then $(r'_1, \ldots, r'_k)$ is unimodular. The least $k > 0$ such that R satisfies S_k (and hence satisfies S_{k+1}) is the *stable rank* of R. In the context of full subgroups this is a critical invariant of R; it is finite, and at most the Krull dimension of R, if R is Noetherian. Many important theorems about $\mathrm{E}(n, R)$, and $\mathrm{SL}(n, R)$, require $n > s + 1$, where s is the stable rank of R. In fact the stable rank is determined by the maximum length of a chain of prime ideals of R, where each prime ideal is required to be the intersection of maximal ideals of R; exactly the prime ideals we expect to be interested in.