Some Open Problems

John D. Dixon

Carleton University, Ottawa

17 November 2014

Some remarks on Zariski topology

- Assume that F is an infinite field.
- Zariski topology on F^n: $S \subseteq F^n$ is a closed subset $\iff$ $\exists$ a set $\mathcal{P} \subseteq F[X_1, ..., X_n]$ such that

$$S = \{(\xi_1, ..., \xi_n) \mid f(\xi_1, ..., \xi_n) = 0 \text{ for all } f \in \mathcal{P}\}$$

- Every finite subset of F^n is closed, but the topology is *not* Hausdorff except in trivial cases. Rational functions are continuous in this topology (see Wehrfritz (1973)).
- Any nonzero polynomial in $F[X_1, ..., X_n]$ is nonzero at infinitely many points of F^n. A closed subset $S \neq F^n$ is "small" (the union of proper closed subsets is a proper subset of F^n). Every nonempty open set is dense in F^n (every two nonempty open sets have a nonempty intersection).

- [Weyl's principle of irrelevancy of algebraic inequalities] If a polynomial f takes the value zero everywhere the polynomials $g_1,...,g_s$ take nonzero values, then f is the zero polynomial (consider $fg_1...g_s$).
- Ex. Cayley-Hamilton theorem.
- [Schwartz-Alon] Suppose that f be a nonzero polynomial of total degree d and that one of its nonzero terms of degree d is $cX_1^{k_1}...X_n^{k_n}$. Let $V_i \subseteq F$ have size $k_i + m_i$ with $m_i > 0$. Then f has a nonzero value at at least $m_1...m_n$ points in $V_1 \times ... \times V_n$ (F may be finite). .

Going from finite to infinite

If two elements $x, y \in GL(n, \mathbb{C})$ have order a power of p (a prime) with $p > 2n - 1$ and they generate a finite group, then $\langle x, y \rangle$ is a finite abelian p-group (Feit & Thompson (1963)).

- What can be said about $\langle x, y \rangle$ if this subgroup is not finite? Can we say more if we know that the group they generate is solvable?
- Consider the special case where x and y have order p, and let P be the free product of two groups of order p. Then we asking about what quotients P/N are linear. Is it possible to characterize the normal subgroups N in a reasonable way?
- Since the free product P itself is a linear group (take $x \in GL(n, \mathbb{C})$ of order p and z any matrix whose entries are independent transcendentals over the entries of x, then $\langle x, z^{-1}xz \rangle$ is a free product), it is known that P/N is linear for any (Zariski) closed normal subgroup N.

Finding cyclic matrices

(16.95 Kourovka Notebook) Is it true that for every $A \in GL(n, F)$ there exists a permutation matrix P such that PA is cyclic? [J.G. Thompson]

- A square matrix A over an algebraically closed field is cyclic if and only if its minimal polynomial is equal to its characteristic polynomial. Alternatively, considering F^n as an $F[X]$-module in which X acts as multiplication by A, A is cyclic $\iff$ F^n is a cyclic $F[X]$-module $\iff$ each of the blocks in the Jordan form of A corresponds to a different eigenvalue $\iff$ for each eigenvalue λ of A the eigenspace V_λ has dimension 1.
- The cyclic matrices form a dense subset of $GL(n, F)$ and almost all $v \in F^n$ generate F^n as a $F[X]$-module.
- [Conjecture] For each invertible A which is not cyclic there exists a permutation matrix P_{ij} (corresponding to the 2-cycle (i, j)) such that PA has a "smaller number" of eigenspaces with dimension > 1 (note P_{ij} is a reflection).

Do almost all pairs from GL(n,Q) generate a free group of rank 2?

- Is the set of such pairs (x, y) dense in $GL(n, \mathbb{Q}) \times GL(n, \mathbb{Q})$? Note that for each nontrivial word w the condition $w(x, y) \neq 1$ defines an open (dense) subset, but to be free we require infinitely many such conditions.
- Corresponding problem for $GL(n, \mathbb{Q})$ with the p-adic measure.
- Using the ping-pong lemma it can be shown that the pair $\begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix}, \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix}$ is a set of free generators for any rational with $|r| \geq 2$. It is an open question whether any such pair with $|r| < 2$ is free (15.83 Kourovka Notebook [Yu. Merzalyakov]).

- A related result. The following are equivalent for $G \leq SL(n, \mathbb{Z})$:

  (i) G is Zariski dense in $SL(n, \mathbb{Z})$

  (ii) $G \bmod p = SL(n, \mathbb{Z}/(p))$ for all but a finite set of p
  (C.R. Matthews, L.N. Vaserstein and B. Weisfeiler, 1984)

  (iii) there exists at least one $p \geq 5$ such that
  $G \bmod p = SL(n, \mathbb{Z}/(p))$ (T. Weigel, 1996)

There are no constructive lower bounds on p in (ii) and (iii). Alternative characterisations use Lie algebras (see Rivin (2010)).

Generating random elements in groups

- Is it possible to generate representatives of random conjugacy classes without generating random elements?
- This may explain in part why the product replacement algorithm appears to work so well.

Constructing elements of rank 1

Let G be a finite group and $\rho : G \to GL(n, \mathbb{C})$ be an absolutely irreducible representation which we know approximately (in some sense to be explained) and for which we can determine the character $\chi(x)$ exactly from our knowledge of the value of $tr\ \rho(x)$. We want to find an exact representation σ of G with character χ defined over $\mathbb{Q}[\omega]$ where ω is a primitive $|G|$th root of 1.

- Theorem: We can compute an exact representation σ of G if and only if we can find a in the group algebra for G such that $\rho(a)$ is of rank 1. How do we find such that an element?
- Simon Norton's irreducibility test (used in Meat Axe) over small finite fields: Let $\mathcal{A}$ be a subalgebra of $M_n(F)$ and $B \in \mathcal{A}$ be singular but not 0. If $\mathcal{A}$ is reducible, then either (i) there exists nonzero $u \in F^n$ such that $uB = 0$ and $u\mathcal{A} \neq F^n$ or (ii) for all $v \in F^n$ such that $vB^T = 0$ we have $v\mathcal{A}^T \neq F^n$.

References

1. Alon, N. Combinatorial Nullstellensatz, Combinatorics, Probability and Computing 8 (1999) 7-29.
2. Feit, W. and J.G. Thompson. Groups which have a faithful representation of degree less than (p-1)/2. Pacific J. Math. 11 (1961) 1257–1262.
3. Kourovka Notebook No. 18 (2014) V.D. Mazurov & E.I. Khukhro (eds.).
4. Matthews, C.R., L.N. Vaserstein & B. Weisfeiler. Congruence properties of Zariski-dense subgroups I. Proc. London Math. Soc. (3) 48 (1984) 514–32.
5. Michalek, M. A short proof of Combinatorial Nullstellensatz, Amer. Math. Monthly 117 (2010) 821-823.
6. Rivin, I. Zariski Density and Genericity. Internat. Math. Res. Notices (2010) 3649–3657.
7. Schwartz, J.T. Fast probabilistic algorithms for verification of polynomial identities. J. ACM. 27 (1980) 701–717.
8. Wehrfritz, B.A.F. Infinite Linear Groups. Springer, 1973 (esp. Theorem 6.4).
9. Weigel, T. On the Profinite Completion of Arithmetic Groups of Split Type. In Lois d'algebres et Varietes Algebriques (Colmar, 1991) pp. 79–101. Hermann, 1996.