RANDOM PRO–p GROUPS, BRAID GROUPS, AND RANDOM TAME GALOIS GROUPS

NIGEL BOSTON AND JORDAN S. ELLENBERG, REVIEWED BY THOMAS KOBERDA

In the article under review, the authors give a heuristic prediction for the distribution of isomorphism classes for the Galois groups of the maximal pro–p extension of $\mathbb{Q}$ which are unramified outside of a finite "random" set of primes.

Let S be a finite set of primes and let $G_S(p)$ be the Galois group of the maximal pro–p extension of $\mathbb{Q}$ which is unramified outside of S. The present article wishes to give a heuristic answer to the question, "when S is a random set of primes, what is the probability that $G_S(p)$ is isomorphic to some specified finite p–group Γ?"

If $S = (\ell_1, \ldots, \ell_g)$ is a tuple of primes congruent to 1 modulo p, the authors write Z_i for the closure of $\ell_i^{\mathbb{Z}}$ in $\mathbb{Z}_p^*$ and W_i for the group $\mathbb{Z}_p/(\ell_i - 1)\mathbb{Z}_p$. They write

$$W = \bigoplus_{i=1}^{g} W_i.$$

The set S is always an ordered g–tuple of primes. The type of S is the sequence of groups $(Z_1, \ldots, Z_g)$. The group $W(Z)$ is the group W associated to the type Z.

Let $A_Z(\Gamma)$ be the number of pairs $((c_1, \ldots, c_g), \iota)$, where $(c_, \ldots, c_g)$ is a g–tuple of conjugacy classes in Γ and ι is an involution in Γ such that $c_i^z = c_i$ for all $z \in Z_i$, the images of $c_1, \ldots, c_g$ under the abelianization map π generate the abelianization of Γ, the map $W(Z) \to \Gamma^{ab}$ sending $(w_1, \ldots, w_g)$ to $\sum_i w_i \pi(c_i)$ is an isomorphism, and when $p = 2$ and ι_i is the unique nontrivial involution in the cyclic subgroup of Γ^{ab} generated by $\pi(c_i)$, then $\sum_{i=1}^{g} \iota_i = \pi(\iota)$. The probability $P(Z, \Gamma, X)$ is the proportion of g–tuples of primes S with type Z in $[X, \ldots, 2X]^g$ such that $G_S(p) \cong \Gamma$.

With the notation of the previous paragraph, the main heuristic of the article says that $\lim_{X \to \infty} P(Z, \Gamma, X)$ exists and is equal to $A_Z(\Gamma)/|\mathrm{Aut}(\Gamma)|$.

The article is also concerned with the pro–p braid group and random pro–p groups. We write P_N for the pure pro–p braid group for the N–generated pro–p group F with the single relation $x_1 \cdots x_N = 1$. The heuristic concerns the action of P_N on the set of epimorphisms from a random (with respect to Haar measure) quotient of F (together with some extra data) to a pro–p group Γ together with a g–tuple of conjugacy classes. If Γ has an equal number of generators and relators then the heuristic asserts that the action of P_N on this set of epimorphisms is transitive.

The authors provide copious computational evidence to justify their heuristics.

Department of Mathematics, Harvard University, 1 Oxford St., Cambridge, MA 02138
E-mail address: koberda@math.harvard.edu