COUNTING NUMBER FIELDS

MELANIE WOOD

1. Introduction and results

Let K be a number field, $[K:\mathbb{Q}] < \infty$, $\mathcal{O}_K$ maximal order in K. Let Disc K = Disc $\mathcal{O}_K \in \mathbb{Z}$. Everything we say today will be over $\mathbb{Q}$ for simplicity, but we could also do this for relative extensions and ask the same questions and get the same sort of results.

Let $\mathrm{Gal}(K) = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ be the Galois group of K ($\mathrm{Gal}(K) \subset S_{[K:\mathbb{Q}]}$) acting on $K \to \mathbb{C}$. Suppose we have a permutation group $G \subset S_n$, and define

$$N(G, X) := \#\{\text{isomorphism classes of } K \text{ with } \mathrm{Gal}(K) = G \text{ and } \mathrm{Disc}(K)| \leq X.$$

The question of counting number fields, then, amounts to studying this asymptotically in X.

We can formulate more refined counting questions. Let p be a prime of $\mathbb{Z}$, $p\mathcal{O}_K = \prod \mathfrak{p_i}^{e_i}$, $f_i = [\mathcal{O}_K/\mathfrak{p_i} : \mathbb{Z}/p]$.

Definition 1.1. A *splitting type* is the multiset of ramification and inertia degrees: $\{\{(e_i, f_i)\}\}$ (or more precisely, isomorphism class of $K \otimes \mathbb{Q}_p$ as a $\mathbb{Q}_p$-algebra).

Let S be a splitting type at p. We define

$$\mathrm{Prob}_G(S) := \lim_{X\to\infty} \frac{\#\{\text{isomorphism classes of } K \text{ with } \mathrm{Gal}(K) = G, |\,\mathrm{Disc}(K)| \leq X, \text{ splitting type } S\}}{N(G, X)}.$$

Understanding these probabilities is a "vertical question," which we compare to the "horizontal question": fix K, vary p, ask about the densities of splitting types. These are given by Chebotarev density theorem as a function of $\mathrm{Gal}(K)$.

Remark 1.2. For fixed K, finitely many p ramify. For fixed p, there can be infinitely many K in which p ramify.

Guesses:

(1) Chebotarev probability: restrict to unramified splitting, might guess that horizontal probabilities equal vertical probabilities
(2) Fix $S_1, \dots, S_k$ splitting types at distinct primes, "independence guess": $\mathrm{Prob}(S_1 + \ldots + S_k) = \prod_i \mathrm{Prob}(S_i)$

There are many ways and reasons in which these guesses are wrong.

Example 1.3. $G = \mathbb{Z}/8 \subset S_8$ (Wang) There is no K with $\mathrm{Gal}(K) = \mathbb{Z}/8$, unramified and unsplit at 2. S at 2, $e = 1, f = 8\,\mathrm{Prob}_{\mathbb{Z}/8}(S) = 0$. For fixed K, $\mathrm{Gal}(K) = \mathbb{Z}/8$, half of the primes have this splitting type.

Theorem 1.4 (Wright)**.** *Given G abelian, prime p, all splitting types that occur over p for some K with $Gal(K) = G$, occur with positive probability.*

Theorem 1.5 (Wood)**.** *These probabilities do not always agree with the Chebotarev probabilities, even over odd primes.*

Example 1.6. $\mathrm{Prob}_{\mathbb{Z}/9}$ (split completely at q $\mid$ unramified at q) $< \frac{1}{9}$, q prime, $q = 2, \dots, 13$.

Theorem 1.7 (Wood)**.** *Given G abelian, p prime, if we count by conductor instead of discriminant, over $p \neq 2$, splitting types occur with the Chebotarev probability, and for $p = 2$, the splitting types that occur have the same relative probabilities as in the Chebotarev question.*

Theorem 1.8 (Wood)**.** *Independence can fail when counting by discriminant.*

Theorem 1.9 (Wood)**.** *For G abelian, counting by conductor, independence holds.*

So this raises the question: if we're counting number fields, which invariant should we use? (See Wood's talk next week.)

How do we count number fields with abelian Galois groups and certain splitting types?

2. Proofs

The strategy does not differ, whether counting by discriminant or counting by conductor. For G abelian, $G \subset S_G$. By class field theory, we know

$$\{K \text{ with } \mathrm{Gal}(K) = G\} \longleftrightarrow \{J_{\mathbb{Q}} \to G\},$$

where the idèle class group $J_{\mathbb{Q}} = (\mathbb{R}^* \times \prod_p \mathbb{Q}_p^*)/\mathbb{Q}^* \twoheadrightarrow G$.

Make the Dirichlet series $\sum a_n n^{-s}$, where a_n is the number of homomorphisms with invariant n. So if we can study $\sum a_n n^{-s}$ as a complex function of s, then the rightmost pole determines the order of growth of $\sum_{n \le X} a_n$, and the residue determines the constant. This needs analytic continuation of the function of s to the line of the rightmost pole.

In the case of S_3, Datskovsky and Wright used this. Can use CFT to count abelian number fields.

If we use $J_Q^0 \twoheadrightarrow G$, with $J_Q^0 \simeq \prod_p \mathbb{Z}_p^*$ then we have

$$\begin{tikzcd} J_{\mathbb{Q}}^0 \arrow[r] \arrow[d] & G \\ \prod_p \mathbb{Z}_p^* \arrow[ur, "\phi"] & \end{tikzcd}$$

with $\phi(1, \dots, 1, p, 1, \dots, 1) = \phi(\frac{1}{p}, \dots, \frac{1}{p}, 1, \frac{1}{p}, \dots, \frac{1}{p})$.

Then writing

$$\prod_p \left(\sum_{\phi : \mathbb{Z}_p^* \to G} \frac{1}{\mathrm{invt}(\phi)^s} \right),$$

we compute local factors and relate this to L-functions to get analytic continuation (expressing in terms of roots of Hecke L-functions, zeta functions of number fields, and other parts that are easy to continue). If we do this, we obtain total asymptotics of counting $J_{\mathbb{Q}} \to G$, and inclusion-exclusion allows us count the surjective homomorphisms.

Harder: say we wanted to know the probability Prob(2 splits completely). This is a question about if $(1, 2, 1, ..., 1) \mapsto 0$. So we'll count continuous homomorphisms $\mathbb{Q}_2^* \times \prod_{p>2} \mathbb{Z}_p^* \to G$. Then we pick out the ones in which $(2, 2, ...2) \mapsto 0$. Here we're using

$$\mathbb{Q}_2^* \times \prod_{p>2} \mathbb{Z}_p^*/\langle 2 \rangle \simeq J_{\mathbb{Q}}^0.$$

We do this by summing over group characters. Then

$$\sum a_n n^{-s} = \sum_{\text{inc-excl}} \sum_{\text{group char}} \text{Euler products.}$$

Multiple summands have the same rightmost pole, but when counting by conductor, they have the same residue. Counting by discriminant, they have different residues.