Counting Number Fields

Thm (Hermite) Given $X>0$, there are finitely many number fields K (up to isom, or in $\overline{\mathbb{Q}}$) with $|\mathrm{Disc}\, K| < X$.

Ques What are asymptotics in X of $N(X) := \#\{K \mid |\mathrm{Disc}(K)| < X\}$?

Galois group

K number field of degree n

Galois group of K, $\mathrm{Gal}(K)$

to be the image of

$$\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \longrightarrow S_n$$

Galois closure of K

given by the action on the n

homomorphisms from $K \to \overline{\mathbb{Q}}$.

Write

$K = \mathbb{Q}(\theta)$

$\theta_1, \ldots, \theta_n$ are n conjugates of θ in $\bar{\mathbb{Q}}$

then this is the action of $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ on $\theta_1, \ldots, \theta_n$.

$\overline{\mathrm{Gal}}(K)$ is a permutation groups

<u>ex</u> K cubic field

$\mathrm{Gal}(K) \subset S_3$

K cyclic cubic field $\quad \mathrm{Gal}(K) = A_3$
(K is Galois)

K non-Galois $\quad \mathrm{Gal}(K) = S_3$

What are the asymptotics of

$$N_\Gamma(X) := \#\{K \mid |\mathrm{Disc}\, K| < X,\ \mathrm{Gal}(K) \simeq \Gamma\}\ ?$$

Local Behavior

Given a place p of $\mathbb{Q}$, we can
(prime or ∞)

form $K_p := K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ $\quad (\mathbb{Q}_\infty = \mathbb{R})$

$K \quad p = \wp_1^{e_1} \cdots \wp_r^{e_r}$

$\mathbb{Q} \quad p$

So K_p is a direct sum of field extensions of $\mathbb{Q}_p$,

$$K_p = \bigoplus_i K_{\mathfrak{p}_i}$$

completions of K at places $\mathfrak{p}_i$ over p

étale $\mathbb{Q}_p$-algebra

What are the asymptotics of

$$N_{\Gamma, M}(X) := \#\{K \mid \operatorname{Disc} K < X, \operatorname{Gal}(K) \cong \Gamma, K_p \cong M\}?$$

Independence:

Are the probabilities at different primes independent?

<u>ex</u> How many quadratic number fields are there split completely at 7?

$N_{\Gamma,M}(X)$? $\Gamma = S_2$ $M = \mathbb{Q}_7^{\oplus 2}$

$\mathbb{P}_{\mathrm{Disc}}$(quadratic K split comp at 7)

$$= \lim_{X \to \infty} \frac{\#\{K \mid |\mathrm{Disc}\, K| < X,\ \mathrm{Gal}(K) = S_2,\ K \text{ s.c. @ } 7\}}{\#\{K \mid |\mathrm{Disc}\, K| < X,\ \mathrm{Gal}(K) = S_2\}}$$

$\mathbb{P}_{\text{Disc}}(K \text{ quad splits @ } 7) = 7/16$

$\mathbb{P}_{\text{Disc}}(K \text{ quad inert @ } 7) = 7/16$

$\mathbb{P}_{\text{Disc}}(K \text{ quad ramifies @ } 7) = 1/8$

Independence?

Chebotarev independence, i.e ind of fields, or rows in our chart

$$\text{Independence} \iff \begin{array}{cccc} S & S & I & I \\ S & I & S & I \end{array} \quad \boxed{\text{True}}$$

each 1/4 of time

quad fields / primes	2	3	5	7	…
⋮	⋮	⋮	⋮	⋮	
$\mathbb{Q}(\sqrt{-7})$	S	I	I	R	
$\mathbb{Q}(\sqrt{5})$	I	I	R	I	
$\mathbb{Q}(i)$	R	I	S	I	
$\mathbb{Q}(\sqrt{-3})$	I	R	I	S	…

S split
I inert
R ramify

Cheb. Look in a row, get $\frac{1}{2}$ S's 0 R's
(asymp.) $\frac{1}{2}$ I's

if I listed all (Galois) number fields for my rows,

Cheb. dependence iff K_1 + K_2 have a subfield in common larger than $\mathbb{Q}$

<u>Ques</u> What do we expect for primes?

Counting class groups

(of imag. quad fields)

<u>Ques</u> Given an odd prime p and a finite abelian p-group G, what proportion of imag. quad. K (ordered by disc) have Sylow p-subgroup of $Cl(K)$ isom to G?

K has $Cl(K) \leftarrow$ finite abelian group

genus theory tells us something about $p=2$

We can also ask for averages of other f over class groups.

(Above $f = 1_G$)

<u>Ex</u> $$\lim_{X\to\infty} \frac{\sum_{K} \#\left(Cl(K)/pCl(K)\right)^k}{\#\{K \mid K \text{ imag quad } |\mathrm{Disc}\, K| < X\}} \, ?$$

A fixed abelian group $$\lim_{X\to\infty} \frac{\sum_{K} \#\mathrm{Sur}(Cl(K), A)}{\text{same}} \, ?$$

For a function f on finite abelian groups, write $M_{\text{field}}(f)$ for this average.

Cohen-Lenstra Heuristics

Observation: things occur in nature with frequency inversely proportional to their number of automorphisms.

ex cubic fields in $\overline{\mathbb{Q}}$

Galois appear 1
have 3 Auts
non-Galois appear 3
have 1 Aut.

Conj (Cohen-Lenstra, Gerth for $p=2$)

For any "reasonable" f we have

$$M_{\text{field}}(f) = \lim_{n\to\infty} \frac{\displaystyle\sum_{\text{f.a.g size}\leq n} \frac{f(G)}{\#\mathrm{Aut}(G)}}{\displaystyle\sum_{\substack{\text{fin ab. gps up to}\\ \text{size } n}} \frac{1}{\#\mathrm{Aut}(G)}}.$$

(taken over $2Cl(K)$)

$$\| \quad M_{\text{group}}(f)$$

Cohen and Lenstra compute $M_{group}(f)$ for many examples of f.

example: $f: \mathbb{1}_{\text{odd part cyclic}}$

$M_{group}(f) \approx .977575$

example: A a fin ab group

$f(G) = \# \mathrm{Sur}(G, A)$ then

$M_{group}(f) = 1$.