Math 280Y: Arithmetic Statistics

Spring 2023

Problem set #6

due Sunday, April 23 at 10pm

Problem 1. Let K be any field. Let $\mathcal{V}^{a=0}(K)$ be the set of binary cubic forms $f = aX^3 + bX^2Y + cXY^2 + dY^3 \in \mathcal{V}(K)$ with $\operatorname{disc}(f) \neq 0$ and $a = 0$. Let $T_2(K)$ be the group of lower-triangular matrices in $\mathrm{GL}_2(K)$. Note that the action of $\mathrm{GL}_2(K)$ on $\mathcal{V}(K)$ restricts to an action of $T_2(K)$ on $\mathcal{V}^{a=0}(K)$.

a) Show that an étale cubic extension L of K is of the form $L = K \times L'$ for some étale quadratic extension L' of K if and only if the corresponding $\mathrm{GL}_2(K)$-orbit in $\mathcal{V}(K)$ intersects $\mathcal{V}^{a=0}(K)$.

b) How many $T_2(K)$-orbits in $\mathcal{V}^{a=0}(K)$ does such an étale cubic extension $L = K \times L'$ correspond to? (Does the number depend on L'?)

Problem 2. Let R be a principal ideal domain and let the cubic form $f(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3 \in \mathcal{V}(R)$ correspond to the cubic extension S of R with basis $(1, \omega_1, \omega_2)$.

a) Show that $S = R[\omega_1]$ if and only if $a \in R^\times$.

b) Show that S is *monogenic* (meaning $S = R[\alpha]$ for some $\alpha \in S$) if and only if $f(x, y) \in R^\times$ for some $x, y \in R$.

Problem 3. Let $M = \{2, 3, 5, \ldots, \infty\}$ be the set of places of $\mathbb{Q}$. Let $\mathbb{Q}_\infty = \mathbb{R}$. For each place $v \in M$, let Σ_v be a set of isomorphism classes of étale cubic $\mathbb{Q}_v$-algebras. Assume that for all but finitely many $v \in M$, Σ_v contains all such isomorphism classes. We have

$$\sum_{\substack{L \text{ cubic number field} \\ L \otimes \mathbb{Q}_v \in \Sigma_v \, \forall v \in M \\ |\operatorname{disc}(L)| \leqslant T}} \frac{1}{\#\operatorname{Aut}(L)} \sim_\Sigma C_\Sigma \cdot T$$

for $T \to \infty$. What is the constant C_Σ? (You will technically only be able to prove this after the lecture on Tuesday, but you can already make an educated guess right now!)

Problem 4 (Kummer theory for C_3-extensions of $\mathbb{Q}$)**.** Let C_3 be the cyclic group of order 3. Consider the algebraic group $\mathcal{G}$ defined over $\mathbb{Q}$ given by $\mathcal{G}(K) = (\mathbb{Q}(\zeta_3) \otimes_{\mathbb{Q}} K)^\times = (K[Z]/(Z^2+Z+1))^\times$ for any number field K. (As a variety, $\mathcal{G}$ is the subvariety of $\mathbb{A}^2$ of pairs (a, b), corresponding to $a + bZ$, such that $[N(a + bZ) = (a + bZ)(a + bZ^2) =]a^2 - ab + b^2 \neq 0$. This is also called the *Weil restriction* of the multiplicative group $\mathbb{G}_m$ from $\mathbb{Q}(\zeta_3)$ to $\mathbb{Q}$.) Denote the automorphism of $\mathbb{Q}(\zeta_3)$ sending ζ_3 to ζ_3^2 by σ_2. We also denote by σ_2 the resulting automorphism of $\mathcal{G}(K)$.

a) Show that the kernel of the map $\mathcal{G}(\overline{\mathbb{Q}}) \to \mathcal{G}(\overline{\mathbb{Q}})$ sending x to x^3 is isomorphic to $C_3 \times C_3$.

b) Show that the map $\varphi : \mathcal{G}(\overline{\mathbb{Q}}) \to \mathcal{G}(\overline{\mathbb{Q}})$ sending x to $x^2/\sigma_2(x)$ is surjective and has kernel contained in $\mathcal{G}(\mathbb{Q})$ and isomorphic to C_3.

c) One can show using *Shapiro's lemma* that $H^1(\overline{\mathbb{Q}}|\mathbb{Q}, \mathcal{G}(\overline{\mathbb{Q}})) = \{*\}$. Use this to construct a bijection between $\mathrm{Hom}_{\mathrm{cont}}(\Gamma_{\mathbb{Q}}, C_3)$ and $\mathcal{G}(\mathbb{Q})/\varphi(\mathcal{G}(\mathbb{Q}))$.

Problem 5 (More of Serre's mass formula)**.** Let K be a local field with normalized valuation v_K and let $n \geqslant 1$.

a) Show that the discriminant of an Eisenstein polynomial $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ with $a_n = 1$ satisfies

$$v_K(\mathrm{disc}(f)) = \min_{1 \leqslant i \leqslant n} (i - 1 + n v_K(i a_i)).$$

b) Show that K has infinitely many separable totally ramified field extensions of degree n if and only if $\mathrm{char}(K) \mid n$.

c) Show that K has infinitely many field extensions of degree n if and only if $\mathrm{char}(K) \mid n$.

d) (bonus) Let $d \geqslant 0$. Show that K has a totally ramified field extension L of degree n with $v_K(D_{L|K}) = d$ if and only if

$$n \cdot v_K(l) \leqslant d - n + 1 \leqslant n \cdot v_K(n),$$

where $1 \leqslant l \leqslant n$ with $l \equiv d + 1 \mod n$.

e) (bonus) Compute the number of totally ramified field extensions $L \subset K^{\mathrm{sep}}$ of K of degree n with $v_K(D_{L|K}) = d$.