Math 286X: Arithmetic Statistics

Spring 2020

Problem set #6

Problem 1. Let $n \geqslant 1$.

a) Show that, up to isomorphism, there are exactly $\lfloor \frac{n}{2} \rfloor + 1$ degree n extensions K of $\mathbb{R}$.

Solution. In class, we counted degree n extensions of a finite field $\mathbb{F}_q$ using the fact that $\mathbb{F}_q$ has exactly one field extension of any given degree. In this problem, we use the same method over $\mathbb{R}$, which has only the two field extensions $\mathbb{R}$ and $\mathbb{C}$.

The degree n extensions are exactly the products of the form $\mathbb{C}^k \times \mathbb{R}^{n-2k}$ with $0 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$. $\square$

b) ([Bha07, Proposition 2.4]) Show that

$$\sum_{\substack{\text{degree } n \\ \text{extension } K|\mathbb{R}}} \frac{1}{\# \operatorname{Aut}_{\mathbb{R}}(K)} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{2^k \cdot k!(n-2k)!} = \mathbb{P}(\pi^2 = \mathrm{id} \mid \pi \in S_n).$$

Solution. The extension $\mathbb{C}^k \times \mathbb{R}^{n-2k}$ has exactly $2^k \cdot k!(n-2k)!$ automorphisms. (The automorphism group is generated by complex conjugation on the complex factors, permutation of the complex factors, and permutation of the real factors. It is isomorphic to $(C_2 \wr S_k) \times S_{n-2k}$.) We have seen that the probability that a random $\pi \in S_n$ consists of k two-cycles and $n-2k$ one-cycles is $\frac{1}{2^k \cdot k!(n-2k)!}$. It only remains to note that a permutation π satisfies $\pi^2 = \mathrm{id}$ if and only if it consists only of two-cycles and one-cycles. $\square$

Problem 2. Let K be a nonarchimedean local field with prime ideal $\mathfrak{p}$ and residue field $\mathbb{F}_q$.

a) Show that $\int_{\mathcal{O}_K} |x| \mathrm{d}x = 1 - \frac{1}{q+1}$.

Solution. Since $\mathcal{O}_K = \mathcal{O}_K^\times \sqcup \pi\mathcal{O}_K$, we have (using the change of variables formula for $y \mapsto x = \pi y$ and the fact that $|\pi| = q^{-1}$):

$$\begin{aligned}\int_{\mathcal{O}_K} |x| \mathrm{d}x &= \int_{\mathcal{O}_K^\times} |x| \mathrm{d}x + \int_{\pi\mathcal{O}_K} |x| \mathrm{d}x \\ &= \int_{\mathcal{O}_K^\times} 1 \mathrm{d}x + \int_{\mathcal{O}_K} |\pi y| \cdot |\pi| \mathrm{d}y \\ &= (1 - q^{-1}) + q^{-2} \cdot \int_{\mathcal{O}_K} |x| \mathrm{d}x.\end{aligned}$$

This implies that

$$\int_{\mathcal{O}_K} |x| \mathrm{d}x = \frac{1 - q^{-1}}{1 - q^{-2}} = \frac{1}{1 + q^{-1}} = 1 - \frac{1}{q+1}.$$

(Alternatively, just write $\mathcal{O}_K = \bigsqcup_{k \geqslant 0} \pi^k \mathcal{O}_K^\times$ and note that $|x|$ is the constant q^{-k} on the set $\pi^k\mathcal{O}_K^\times$ of measure $q^{-k}(1 - q^{-1})$.) $\square$

b) Let $f(X) \in \mathcal{O}_K[X]$ be a polynomial such that $f'(X) \bmod \mathfrak{p}$ has k simple roots in $\mathbb{F}_q$ and no roots of higher multiplicity in $\mathbb{F}_q$. For any $y \in \mathcal{O}_K$, let $m(y)$ be the number of $x \in \mathcal{O}_K$ such that $f(x) = y$. Show that

$$\int_{\mathcal{O}_K} m(y) \mathrm{d}y = 1 - \frac{k}{q+1}.$$

(This is the expected number of preimages of a random element $y \in \mathcal{O}_K$ under the map $f : \mathcal{O}_K \to \mathcal{O}_K$.)

Solution. By Hensel's lemma, we can write $f'(X) = (X - a_1) \cdots (X - a_k) \cdot g(X) \mod \mathfrak{p}$, where $a_1, \ldots, a_k \in \mathcal{O}_K$ are distinct and $g(X) \in \mathcal{O}_K[X]$ is a polynomial with no roots modulo $\mathfrak{p}$. Note that $v_p(g(x)) = 0$, so $v_p(f'(x)) = \sum_i v_p(x - a_i)$ for any $x \in \mathcal{O}_K$. Also note that, since $a_i \not\equiv a_j \mod \mathfrak{p}$ for all $i \neq j$, at most one of the numbers $v_p(x - a_i)$ can be nonzero for any $x \in \mathcal{O}_K$. In other words, we have $|f'(x)| = \prod_i |x - a_i|$, and at most one of the numbers $|x - a_i|$ is not 1. This implies that $|f'(x)| = \prod_i |x - a_i| = 1 - \sum_i (1 - |x - a_i|)$. Changing variables, we have

$$\begin{aligned}\int_{\mathcal{O}_K} m(y)\mathrm{d}y &= \int_{\mathcal{O}_K} |f'(x)|\mathrm{d}x \\ &= \int_{\mathcal{O}_K} (1 - \sum_i (1 - |x - a_i|))\mathrm{d}x \\ &= \int_{\mathcal{O}_K} \mathrm{d}x - \sum_i \int_{\mathcal{O}_K} (1 - |x - a_i|)\mathrm{d}x\end{aligned}$$

By part a) and $\int_{\mathcal{O}_K} \mathrm{d}x = 1$, this is

$$1 - \sum_i \frac{1}{q+1} = 1 - \frac{k}{q+1}. \qquad \square$$

Problem 3 ([Ser78, Section 4])**.** 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

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

Solution. Let π be a root of $f(X)$. We have

$$\mathrm{disc}(f) = \pm \mathrm{Nm}_{K(\pi)|K}(f'(\pi)),$$

so, denoting the extension of v_K to $K(\pi)$ also by v_K, we get

$$v_K(\mathrm{disc}(f)) = n \cdot v_K(f'(\pi)) = n \cdot v_K\left(\sum_{i=1}^{n} i a_i \pi^{i-1}\right).$$

Since $v_K(\pi) = \frac{1}{n}$, no two of the valuations $v_K(i a_i \pi^{i-1}) = v_K(i a_i) + \frac{i-1}{n} \in \mathbb{Z} + \frac{i-1}{n}$ are the same. Hence, the valuation of the sum is $\min_{1 \leqslant i \leqslant n}(v_K(i a_i) + \frac{i-1}{n})$, so

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

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

Solution. Let $\operatorname{char}(K) \nmid n$. By part a), we have $v_K(\operatorname{disc}(f)) \leqslant n v_K(n) + n - 1 < \infty$ for any monic Eisenstein polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K$. This implies that separable totally ramified field extensions L of degree n have bounded discriminant. Therefore, in Serre's mass formula

$$\sum_{\substack{L \subset K^{\mathrm{sep}} \\ \text{tot. ram.} \\ \text{of deg. } n}} |D_{L|K}| = \frac{1}{q^{n-1}},$$

the summands are bounded from below by a positive constant. Hence, there are only finitely many summands.

On the other hand, if $\operatorname{char}(K) \mid n$, then $n v_K(n) + n - 1 = \infty$, so the discriminant of a monic Eisenstein polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K$ satisfies $v_K(\operatorname{disc}(f)) = \min_{1 \leqslant i \leqslant n-1}(n v_K(i a_i) + i - 1)$. By choosing $a_1, \ldots, a_{n-1} \neq 0$ of sufficiently high valuation, we can make $v_K(\operatorname{disc}(f))$ arbitrarily large (but finite). Hence, there are infinitely many possible discriminants, and in particular infinitely many separable totally ramified extensions. $\square$

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

Solution. Let $\operatorname{char}(K) \nmid n$. Any degree n extension L of K has a maximal unramified subextension F. Then, L is a totally ramified extension of F. There are only finitely many unramified extensions F of K of degree dividing n (one for each degree). By part a), any such extension F has only finitely many totally ramified extensions of degree $n/[F : K]$. $\square$

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 $l \equiv d + 1 \mod n$.

Solution. Let us compute the possible values of $b_i(f) = i - 1 + n v_K(i a_i)$ for each i, where $f(X) = a_n X^n + \cdots + a_0$ is a monic Eisenstein polynomial as in part a). For $i = n$, we always have $b_i(f) = n - 1 + n v_K(n)$. For $1 \leqslant i \leqslant n - 1$, the set of possible values for $b_i(f)$ is $\{i - 1 +$

$nv_K(i) + n \cdot t \mid t \in \mathbb{Z},\ t \geqslant 1\}$. Since $b_i(f)$ only depends on a_i, we can choose $b_1(f), \ldots, b_n(f)$ independently. Since $b_i(f) \equiv i-1 \mod n$, we have $d = v_K(\mathrm{disc}(f)) = \min_{1 \leqslant i \leqslant n} b_i(f)$ if and only if $d = b_l(f) \leqslant b_i(f)$ for all i. It is easy to see that this can be arranged if and only if $n \cdot v_K(l) \leqslant d - n + 1 \leqslant n \cdot v_K(n)$. ☐

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

Solution. Assume that the condition in d) is satisfied, so there is at least one such extension.

Let $P_{n,d} \subset \mathcal{O}_K^n$ be the set of monic degree n Eisenstein polynomials such that $v_K(\mathrm{disc}(f)) = d$. As in the proof of Serre's mass formula discussed in class, it follows that

$$\sum_{\substack{L \subset K^{\mathrm{sep}} \\ \text{tot. ram.} \\ \text{of deg. } n \\ \text{with } v_K(D_{L|K}) = d}} q^{-1}(1 - q^{-1})|D_{L|K}| = n \cdot \mathrm{vol}(P_{n,d}).$$

Note that $|D_{L|K}| = q^{-v_K(D_{L|K})} = q^{-d}$, so all summands on the left-hand side are $(1-q^{-1})q^{-d-1}$. Staring at a) and d) for a while (see Serre's paper), you can show that $\mathrm{vol}(P_{n,d}) = (1-q^{-1})\alpha q^{-n-\beta}$, where

$$\alpha = \begin{cases} 1, & d+1 \equiv 0 \mod n, \\ q-1, & d+1 \not\equiv 0 \mod n, \end{cases}$$

and

$$\beta = \sum_{i=1}^{n-1} \max\left(0, \left\lfloor \frac{d+1-i}{n} \right\rfloor - v_K(i)\right).$$

Hence, the number of L as above is

$$\alpha q^{d-n+1-\beta}.$$ ☐

Problem 4. Let S_1 be a degree n_1 extension and let S_2 be a degree n_2 extension of a Dedekind domain R.

a) Show that the tensor product $S = S_1 \otimes_R S_2$ is a degree $n_1 \cdot n_2$ extension of R.

Solution. The tensor product of finitely generated modules is clearly finitely generated. The tensor product of torsion-free modules is torsion-free. The tensor product of vector spaces of dimensions n_1, n_2 is a vector space of dimension $n_1 \cdot n_2$. $\square$

b) Show that $\operatorname{disc}(S|R) = \operatorname{disc}(S_1|R)^{n_2} \cdot \operatorname{disc}(S_2|R)^{n_1}$. (Hint: Look up the discriminant of a Kronecker product of matrices or the proof of Proposition I.2.11 in [Neu99]. First show the claim for principal ideal domains R.)

Solution. If R is a principal ideal domain, then S_1, S_2 are free R-modules, so they have R-bases $(\omega_i)_{1\leqslant i\leqslant n_1}$ and $(\theta_{i'})_{1\leqslant i'\leqslant n_2}$. Then, $S = S_1 \otimes S_2$ has R-basis $(\omega_i\theta_{i'})_{1\leqslant i\leqslant n_1,\ 1\leqslant i'\leqslant n_2}$. The discriminants of S_1, S_2, S are the ideals generated by the determinants of $A_1 = (\operatorname{Tr}(\omega_i\omega_j))_{i,j}$, $A_2 = (\operatorname{Tr}(\theta_{i'}\theta_{j'}))_{i',j'}$, $A = (\operatorname{Tr}(\omega_i\omega_j\theta_{i'}\theta_{j'}))_{(i,i'),(j,j')}$. The third matrix A is the Kronecker product of the first two matrices A_1 and A_2. Therefore, we have $\det(A) = \det(A_1)^{n_2}\det(A_2)^{n_1}$, proving the claim.

For general Dedekind domains R, it suffices to show that two sides of the claimed equality are divisible by any (nonzero) prime ideal $\mathfrak{p}$ of R the same number of times. To prove this, we can base change to the localization of R at $\mathfrak{p}$ (or to its completion at $\mathfrak{p}$ if you prefer), which is a principal ideal domain. $\square$

References

[Bha07] Manjul Bhargava. "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants". In: *Int. Math. Res. Not. IMRN* 17 (2007), Art. ID rnm052, 20. ISSN: 1073-7928. DOI: `10.1093/imrn/rnm052`. URL: `https://doi.org/10.1093/imrn/rnm052`.

[Neu99] Jürgen Neukirch. *Algebraic number theory.* Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. DOI: `10.1007/978-3-662-03983-0`. URL: `https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/978-3-662-03983-0`.

[Ser78] Jean-Pierre Serre. “Une “formule de masse” pour les extensions totalement ramifiées de degré donné d'un corps local”. In: *C. R. Acad. Sci. Paris Sér. A-B* 286.22 (1978), A1031–A1036. ISSN: 0151-0509.