Math 286X: Arithmetic Statistics

Spring 2020

Problem set #7

Problem 1. Let K be any field and $n \geqslant 3$. Consider the action of $\mathrm{PGL}_{n-1}(K) = \mathrm{GL}_{n-1}(K)/K^\times$ on the projective space $\mathbb{P}^{n-2}(K) = K^{n-1}/K^\times$ given by $[M].[v] = [Mv]$ for $M \in \mathrm{GL}_{n-1}(K)$ and $v \in K^{n-1}$. We say that n points $P_1, \ldots, P_n \in \mathbb{P}^{n-2}(K)$ are *in general position* if any $n-1$ of the points span $\mathbb{P}^{n-2}(K)$. (For $n = 3$, this simply means that the three points $P_1, P_2, P_3 \in \mathbb{P}^1(K)$ are distinct.)

a) Show that for any n points $P_1, \ldots, P_n \in \mathbb{P}^{n-2}(K)$ in general position and any n points $Q_1, \ldots, Q_n \in \mathbb{P}^{n-2}(K)$ in general position, there is exactly one $g \in \mathrm{PGL}_{n-1}(K)$ such that $gP_i = Q_i$ for all $i = 1, \ldots, n$. (In other words, $\mathrm{PGL}_{n-1}(K)$ acts simply transitively on the set of n-tuples of points in $\mathbb{P}^{n-2}(K)$ in general position.)

   Solution. It suffices to prove this for $P_1 = [1 : 0 : \cdots : 0]$, $\ldots$, $P_{n-1} = [0 : \cdots : 0 : 1]$, $P_n = [1 : \cdots : 1]$. Let $Q_i = [v_i]$ with $v_i \in K^{n-1}$. Write $g = [M]$, where $M \in \mathrm{GL}_{n-1}(K)$ has columns $w_1, \ldots, w_{n-1} \in K^{n-1}$. We have $gP_i = Q_i$ for all i if and only if $[w_i] = [v_i]$ for $i = 1, \ldots, n-1$ and $[w_1 + \cdots + w_{n-1}] = [v_n]$. The first $n-1$ conditions can be written as $w_i = \lambda_i v_i$ with $\lambda_i \in K^\times$. The last condition then means that $[\lambda_1 v_1 + \cdots + \lambda_{n-1} v_{n-1}] = [v_n]$. Scaling the matrix M by an element of $K^\times$, we can assume $\lambda_1 v_1 + \cdots + \lambda_{n-1} v_{n-1} = v_n$. Since $v_1, \ldots, v_{n-1}$ form a basis of K^{n-1}, there are unique $\lambda_1, \ldots, \lambda_{n-1} \in K$ satisfying this equation. Since any $n-1$ of the points $v_1, \ldots, v_n$ are linearly independent, we in fact have $\lambda_i \neq 0$ for all i. Since $v_1, \ldots, v_{n-1}$ are linearly independent, the resulting (unique) matrix M lies in $\mathrm{GL}_{n-1}(K)$. □

b) Consider the action of $\mathrm{PGL}_{n-1}(K)$ on the set of sets X of n points in $\mathbb{P}^{n-1}(K)$ in general position. Show that the stabilizer of any such set X is isomorphic to S_n.

   Solution. By a), there is exactly one element of $\mathrm{PGL}_{n-1}(K)$ for any permutation of the n points. □

Problem 2. Consider the trivial cubic extension $S = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ of $\mathbb{Z}$. Find all cubic subextensions $S' \subset S$ of $\mathbb{Z}$ of index $[S : S'] \in \{p, p^2, p^3\}$, where p is prime.
Hint: Use the appropriate normal form

Solution. The trivial extension S of $\mathbb{Z}$ corresponds to the cubic form $f(X, Y) = XY(Y - X) \in \mathcal{V}(\mathbb{Z})$. The cubic subextensions $S' \subseteq S$ correspond to orbits $\mathrm{GL}_2(\mathbb{Z})M$ in $\mathrm{GL}_2(\mathbb{Z})\backslash(M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q}))$ such that $M.f \in \mathcal{V}(\mathbb{Z})$. Each such orbit contains exactly one matrix M in Hermite normal form: $M = \left(\begin{smallmatrix} a_1 & b \\ 0 & a_2 \end{smallmatrix}\right)$ for $1 \leqslant a_1, a_2 \in \mathbb{Z}$ and $b \in \{0, \dots, a_2 - 1\}$. The index is $[S : S'] = a_1 a_2$. We have

$$M.f(X, Y) = \frac{(a_1X)(bX + a_2Y)(bX + a_2Y - a_1X)}{a_1a_2}$$
$$= \frac{-a_1b + b^2}{a_2} \cdot X^3 + (-a_1 + 2b) \cdot X^2Y + a_2XY^2,$$

so $M.f \in \mathcal{V}(\mathbb{Z})$ if and only if $a_2 \mid b(b - a_1)$.

Hence, subextensions of index d are in bijection with triples (a_1, a_2, b) with $a_1, a_2 \geqslant 1$, $0 \leqslant b \leqslant a_2 - 1$, $a_1 \cdot a_2 = d$, and $a_2 \mid b(b - a_1)$.

For $d = p$, the three possible triples are $(p, 1, 0)$, $(1, p, 0)$, $(1, p, 1)$. They correspond to the subextensions $\{(x, y, z) \mid x \equiv y \mod p\}$, $\{x \equiv z \mod p\}$, $\{y \equiv z \mod p\}$.

For $d = p^2$, the four possible triples are $(p^2, 1, 0)$, $(p, p, 0)$, $(1, p^2, 0)$, $(1, p^2, 1)$. They correspond to the subextensions $\{x \equiv y \mod p^2\}$, $\{x \equiv z \mod p^2\}$, $\{y \equiv z \mod p^2\}$, $\{x \equiv y \equiv z \mod p\}$.

For $d = p^3$, the $p + 4$ possible triples are $(p^3, 1, 0)$, $(p^2, p, 0)$, $(1, p^3, 0)$, $(1, p^3, 1)$, (p, p^2, b) with $b = 0, p, \dots, p(p-1)$. They correspond to the subextensions $\{x \equiv y \mod p^3\}$, $\{x \equiv z \mod p^3\}$, $\{y \equiv z \mod p^3\}$, $\{x \equiv y \equiv z \mod p \text{ and } a(x - y) + b(x - z) \equiv 0 \mod p^2\}$ for $[a : b] \in \mathbb{P}^1(\mathbb{F}_p)$. □

Definition. We call a degree n extension S of a Dedekind domain R *monogenic* if the R-algebra S is generated by one element: $S = R[\alpha]$ for some $\alpha \in S$.

Problem 3. a) Show that the trivial degree n extension $S = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ of $\mathbb{Z}_p$ is monogenic if and only if $n \leqslant p$.

Solution. An element $\alpha = (\alpha_1, \dots, \alpha_n) \in S$ generates S if and only if the matrix $M = (\alpha_i^j)_{1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant n-1} \in M_n(\mathbb{Z}_p)$ with columns $1, \alpha, \dots, \alpha^{n-1}$

is invertible. It determinant is $\pm \prod_{i<j}(\alpha_i - \alpha_j)$, which is invertible if and only if the residues $\alpha_i \bmod p$ for $i = 1, \ldots, n$ are distinct. Of course, that's possible if and only if $n \leqslant p$. $\square$

b) Let K be a degree n field extension of $\mathbb{Q}$ in which some (unramified) prime $p < n$ splits completely. Show that the extension $\mathcal{O}_K$ of $\mathbb{Z}$ is not monogenic.

Solution. The prime p splits completely if and only if $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$. This means that $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is (isomorphic to) the ring of integers $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, which according to a) is not monogenic. Hence, $\mathcal{O}_K$ is not monogenic. $\square$

c) Show that for any $n \geqslant 1$ and any prime number p, there is a degree n field extension of $\mathbb{Q}$ in which the (unramified) prime p splits completely.

Solution. Consider the monic degree n polynomial $f(X) = \prod_{i=1}^{n}(X - i)$. Choose e large enough so that $e > 2v_p(f'(i))$ for $i = 1, \ldots, n$. Also, choose a prime $q \neq p$. By the Chinese remainder theorem, there is a monic degree n polynomial $g(X) \in \mathbb{Z}[X]$ such that $g(X) \equiv f(X) \mod p^e$ and $g(X) \equiv X^n + q \mod q^2$. The second condition shows that $g(X)$ is an Eisenstein polynomial at q and therefore irreducible. The first condition shows that $g(i) \equiv 0 \mod p^e$ and $v_p(g'(i)) = v_p(f'(i))$ for $i = 1, \ldots, n$. By Hensel's lemma, this implies that each $i = 1, \ldots, n$ lifts modulo p^e to a unique root in $\mathbb{Z}_p$. Furthermore, it implies that $i \not\equiv j \mod p^e$ for any $i \neq j$ with $1 \leqslant i, j \leqslant n$. In particular, $g(X)$ splits completely into n distinct linear factors. Therefore, $K = \mathbb{Q}[X]/(g(X))$ is a degree n field extension of $\mathbb{Q}$ in which p splits completely. $\square$

Problem 4. 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 $a \in R^\times$.

Solution. By construction, we have $\omega_1^2 = -ac - b\omega_1 + a\omega_2$. Hence, $1, \omega_1, \omega_1^2$ forms a basis of $S = \langle 1, \omega_1, \omega_2 \rangle_R$ if and only if the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -ac & -b & a \end{pmatrix}$$

is invertible over R, which is equivalent to $a \in R^\times$. $\square$

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

Solution. If $f(x, y) \in R^\times$, then x, y are in particular relatively prime. This implies there is a matrix $M \in \mathrm{GL}_2(R)$ of the form $\left(\begin{smallmatrix} x & y \\ * & * \end{smallmatrix}\right)$. By definition, $M.f(X, Y) = a'X^3 + \cdots + d'Y^3$ satisfies $a' = (M.f)(1, 0) = f(x, y)/\det(M) \in R^\times$. But f corresponds to the same cubic extension as $M.f$, which is monogenic by part a).

Conversely, if S is monogenic, then there is some $\omega_1' \in S$ such that $1, \omega_1', \omega_1'^2$ is a basis of S. By part a), this shows that there is a base change matrix $M \in \mathrm{GL}_2(R)$ such that $M.f(X, Y) = a'X^3 + \cdots + d'Y^3$ satisfies $a' \in R^\times$. If the first row of M is $\begin{pmatrix} x & y \end{pmatrix}$, it follows as above that $f(x, y) \in R^\times$. □

Problem 5. Order the cubic field extensions $K|\mathbb{Q}$ by $|D_K|$.

a) Show that a random K is totally real with probability $1/4$.

Solution. Let $E = \mathbb{R}\times\mathbb{R}\times\mathbb{R}$ or $E = \mathbb{R}\times\mathbb{C}$. If you look back at the computation of the number of cubic field extensions $K|\mathbb{Q}$ with $|D_K| \leqslant T$ (in particular the computation of the volume of a fundamental domain), you realize that $K \otimes_\mathbb{Q} \mathbb{R} \cong E$ with probability proportional to $\frac{1}{\#\mathrm{Aut}_\mathbb{R}(E)}$. We have $\#\mathrm{Aut}(\mathbb{R}\times\mathbb{R}\times\mathbb{R}) = 6$ and $\#\mathrm{Aut}(\mathbb{R}\times\mathbb{C}) = 2$. Hence, $K \otimes_\mathbb{Q} \mathbb{R} \cong \mathbb{R}\times\mathbb{R}\times\mathbb{R}$ with probability $\frac{1/6}{1/6+1/2} = \frac{1}{4}$. □

b) For a fixed prime number p, show that a random K is unramified at p with probability $1/(1 + p^{-1} + p^{-2})$.

Solution. The computation of $\mathrm{vol}(\mathcal{V}^{\max}(\mathbb{Z}_p))$ in class shows that for a fixed nondegenerate cubic extension L of $\mathbb{Q}_p$, we have $K \otimes_\mathbb{Q} \mathbb{Q}_p \cong L$ with probability proportional to $\frac{|D_{L|\mathbb{Q}}|}{\#\mathrm{Aut}(L)}$. We have shown that

$$\sum_{L \text{ nondeg. cubic ext. of } \mathbb{Q}_p} \frac{|D_{L|\mathbb{Q}}|}{\#\mathrm{Aut}(K)} = 1 + p^{-1} + p^{-2},$$

so the probability is

$$\frac{\frac{|D_{L|\mathbb{Q}}|}{\#\mathrm{Aut}(L)}}{1 + p^{-1} + p^{-2}}.$$

We have furthermore shown in class that (cf. extensions of finite field)

$$\sum_{k \text{ nondeg. cubic ext. of } \mathbb{F}_p} \frac{1}{\# \operatorname{Aut}(k)} = 1.$$

By the correspondence between unramified extensions of a local field and extensions of its residue field, it follows that

$$\sum_{L \text{ unram. nondeg. cubic ext. of } \mathbb{Q}_p} \frac{1}{\# \operatorname{Aut}(L)} = 1. \qquad \square$$

c) For a fixed prime number p, consider only those K which are unramified at p. Fix a partition $n = k_1 + \cdots + k_r$. Show that the (conditional) probability that K has splitting type $(k_1, \ldots, k_r)$ at p equals the probability that a random $\pi \in S_n$ has cycle type $(k_1, \ldots, k_r)$.

Solution. We have shown in class that (cf. extensions of finite fields)

$$\frac{1}{\# \operatorname{Aut}(\mathbb{F}_{p^{k_1}} \times \cdots \times \mathbb{F}_{p^{k_r}})} = \mathbb{P}(\pi \text{ has cycle type } (k_1, \ldots, k_r) \mid \pi \in S_n)$$

The result again follows from the correspondence between unramified extensions of a local field and extensions of its residue field. $\square$

d) For a fixed prime number p, show that a random K is totally ramified at p with probability $1/(1 + p + p^2)$.

Solution. We have shown in class that (cf. Serre's mass formula)

$$\sum_{L \text{ tot. ram. field ext. of } \mathbb{Q}_p} \frac{|D_{L|\mathbb{Q}_p}|}{\# \operatorname{Aut}(L)} = p^{-2},$$

so the probability is $\frac{p^{-2}}{1+p^{-1}+p^{-2}} = 1/(1 + p + p^2)$. $\square$

e) Fix some $s \geqslant 0$. Show that a random K is ramified at only s primes with probability zero (just like a random integer is only divisible by s primes with probability zero).

Solution. Fix some $P \geqslant 2$ and some primes $p_1 < \cdots < p_s \leqslant P$. The same sieve as in class and the argument from b) shows that that K is ramified at $p_1, \ldots, p_s$, but at no other primes $p \leqslant P$ with probability

$$\prod_{p \leqslant P} \frac{1}{1+p^{-1}+p^{-2}} \cdot \prod_{i=1}^{s} \frac{1-\frac{1}{1+p_i^{-1}+p_i^{-2}}}{\frac{1}{1+p_i^{-1}+p_i^{-2}}} = \prod_{p \leqslant P} \frac{1}{1+p^{-1}+p^{-2}} \cdot \prod_{i=1}^{s} \frac{1+p_i^{-1}}{p_i}.$$

Hence, K is unramified at exactly s primes $p \leqslant P$ with probability

$$\begin{aligned} &\prod_{p \leqslant P} \frac{1}{1+p^{-1}+p^{-2}} \cdot \sum_{p_1 < \cdots < p_s \leqslant P} \prod_{i=1}^{s} \frac{1+p_i^{-1}}{p_i} \\ &\leqslant \left(\prod_{p \leqslant P} \frac{1}{1+p^{-1}+p^{-2}} \right) \cdot \left(\sum_{p \leqslant P} \frac{1+p^{-1}}{p} \right)^{s} \end{aligned} \tag{1}$$

For large P, we have

$$\prod_{p \leqslant P} (1+p^{-1}+p^{-2}) \asymp \prod_{p \leqslant P} \frac{1}{1-p^{-1}} \asymp \log P$$

and

$$\sum_{p \leqslant P} \frac{1+p^{-1}}{p} \asymp \sum_{p \leqslant P} \frac{1}{p} \asymp \log \log P,$$

so the upper bound in (1) goes to 0 as $P \to \infty$. $\square$