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.)

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.

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

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 $n \leqslant p$.

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.

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.

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 $a \in R^\times$.

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

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

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

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

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 $(k_1, \ldots, k_r)$.

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

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).