How to determine the splitting type of a prime

Melanie Matchett Wood

February 17, 2011

Let E/K be an extension of number fields (or function fields?) of degree n, and let p be a prime of K. The goal of these notes is to explain how to determine the splitting type of p in E via information about decomposition and inertia groups. Many texts only treat the case when E/K is Galois, except for the section on "Factorization in Nonnormal Extensions" in [1, Chapter III, Section 2], which unfortunately only covers the unramified case.

Let L be the Galois closure of E/K. Let $G = \mathrm{Gal}(L/K) \subset S_n$ vis its permutation action on the n homomorphisms $E \to L$. Let H the subgroup of G corresponding to E via Galois theory (which is the intersection of G with the $S_{n-1} \subset S_n$ stabilizing the identity inclusion $E \to L$). If you weren't sure how G acts on the n homomorphisms $E \to L$, then I've just told you, because a transitive action is given by any stabilizer, and thus the permutation action $G \subset S_n$ above is just the action of G on cosets of H. We use $H\backslash G$ to denote the cosets $H\tau$ of H, but it is important to remember that H is not normal.

Let $\wp$ be a prime of L above p. Let $G(\wp) \subset G$ be the decomposition group of $\wp$ and $I(\wp) \subset G(\wp)$ be the inertia group. The group $G(\wp)$ acts on $H\backslash G$ (this action is given by the permutation representation $G(\wp) \subset G \subset S_n$), and the primes of E above p correspond to the orbits of $G(\wp)$ in this action (very easy to read off if you have written everythign inside S_n).

So if we now consider a single prime of E over p corresponding to an orbit of $G(\wp)$, we have that ef is the size of that orbit, and the ramification index e is the size of an orbit of $I(\wp)$ inside that orbit. (Since $I(\wp)$ is normal in $G(\wp)$, all the $I(\wp)$ orbits in one $G(\wp)$ orbit have the same size.)

Of course if we consider an unramified extension, the $G(\wp)$ is generated by Frobenius and we can speak of the orbit of a single element instead of the orbit of a group, and even it the extension is only tamely ramified then $I(\wp)$ is cyclic and then at least for the inertia group we can speak of the orbit of a single element. And if E is Galois, and H is trivial then the action is simple and we can talk about the size of groups instead of the size of their orbits. Which all explain why these cases are the ones we are usually taught about.

References

[1] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR 1362545 (96j:11137)