Math 129: Algebraic Number Theory

Lecture 13: Galois Extensions

William Stein

Thursday, March 8, 2004

1 The Decomposition and Inertia Groups

Suppose K is a number field that is Galois over $\mathbf{Q}$ with group $G = \mathrm{Gal}(K/\mathbf{Q})$. Fix a prime $\mathfrak{p} \subset \mathcal{O}_K$ lying over $p \in \mathbf{Z}$.

Definition 1.1 (Decomposition group). The *decomposition group* of $\mathfrak{p}$ is the subgroup

$$D_{\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\} \leq G.$$

(Note: The decomposition group is called the "splitting group" in Swinnerton-Dyer. Everybody I know calls it the decomposition group, so we will too.) Recall that G acts on the set of primes $\mathfrak{p}$ lying over p. Thus the decomposition group is the stabilizer in G of $\mathfrak{p}$. The orbit-stabilizer theorem implies that $[G : D_{\mathfrak{p}}]$ equals the orbit of $\mathfrak{p}$, which we proved last time equals the number g of primes lying over p, so $[G : D_{\mathfrak{p}}] = g$.

Lemma 1.2. *The decomposition subgroups $D_{\mathfrak{p}}$ corresponding to primes $\mathfrak{p}$ lying over a given p are all conjugate in G.*

Proof. We have $\tau(\sigma(\tau^{-1}(\mathfrak{p}))) = \mathfrak{p}$ if and only if $\sigma(\tau^{-1}(\mathfrak{p})) = \tau^{-1}\mathfrak{p}$. Thus $\tau\sigma\tau^{-1} \in D_p$ if and only if $\sigma \in D_{\tau^{-1}\mathfrak{p}}$, so $\tau^{-1}D_p\tau = D_{\tau^{-1}\mathfrak{p}}$. The lemma now follows because, as we proved before, G acts transitively on the set of $\mathfrak{p}$ lying over p. $\square$

The decomposition group is extremely useful because it allows us to see the extension $K/\mathbf{Q}$ as a tower of extensions, such that at each step in the tower we understand well the splitting behavior of the primes lying over p. Now might be a good time to glance ahead at Figure 1.2 on page 5.

We characterize the fixed field of $D = D_{\mathfrak{p}}$ as follows.

Proposition 1.3. *The fixed field K^D of D*

$$K^D = \{a \in K : \sigma(a) = a \textit{ for all } \sigma \in D\}$$

is the smallest subfield $L \subset K$ such that $\mathfrak{p} \cap L$ does not split in K (i.e., $g(K/L) = 1$).

Proof. First suppose $L = K^D$, and note that by Galois theory $\mathrm{Gal}(K/L) \cong D$, and by the theorem we proved on Tuesday, the group D acts transitively on the primes of K lying over $\mathfrak{p} \cap L$. One of these primes is $\mathfrak{p}$, and D fixes $\mathfrak{p}$ by definition, so there is only one prime of K lying over $\mathfrak{p} \cap L$, i.e., $\mathfrak{p} \cap L$ does not split in K. Conversely, if $L \subset K$ is such that $\mathfrak{p} \cap L$ does not split in K, then $\mathrm{Gal}(K/L)$ fixes $\mathfrak{p}$ (since it is the only prime over $\mathfrak{p} \cap L$), so $\mathrm{Gal}(K/L) \subset D$, hence $K^D \subset L$. □

Thus p does not split in going from K^D to K—it does some combination of ramifying and staying inert. To fill in more of the picture, the following proposition asserts that p splits completely and does not ramify in $K^D/\mathbf{Q}$.

Proposition 1.4. *Let $L = K^D$ for our fixed prime p and Galois extension $K/\mathbf{Q}$. Let $e = e(L/\mathbf{Q}), f = f(L/\mathbf{Q}), g = g(L/\mathbf{Q})$ be for $L/\mathbf{Q}$ and p. Then $e = f = 1$ and $g = [L : \mathbf{Q}]$, i.e., p does not ramify and splits completely in L. Also $f(K/\mathbf{Q}) = f(K/L)$ and $e(K/\mathbf{Q}) = e(K/L)$.*

Proof. As mentioned right after Definition 1.1, the orbit-stabilizer theorem implies that $g(K/\mathbf{Q}) = [G : D]$, and by Galois theory $[G : D] = [L : \mathbf{Q}]$. Thus

$$\begin{aligned} e(K/L) \cdot f(K/L) = [K : L] &= [K : \mathbf{Q}]/[L : \mathbf{Q}] \\ &= \frac{e(K/\mathbf{Q}) \cdot f(K/\mathbf{Q}) \cdot g(K/\mathbf{Q})}{[L : \mathbf{Q}]} = e(K/\mathbf{Q}) \cdot f(K/\mathbf{Q}). \end{aligned}$$

Now $e(K/L) \leq e(K/\mathbf{Q})$ and $f(K/L) \leq f(K/\mathbf{Q})$, so we must have $e(K/L) = e(K/\mathbf{Q})$ and $f(K/L) = f(K/\mathbf{Q})$. Since $e(K/\mathbf{Q}) = e(K/L) \cdot e(L/\mathbf{Q})$ and $f(K/\mathbf{Q}) = f(K/L) \cdot f(L/\mathbf{Q})$, the proposition follows. □

1.1 Galois groups of finite fields

Each $\sigma \in D = D_{\mathfrak{p}}$ acts in a well-defined way on the finite field $\mathbf{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$, so we obtain a homomorphism

$$\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p).$$

We pause for a moment and derive a few basic properties of $\mathrm{Gal}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$, which are in fact general properties of Galois groups for finite fields. Let $f = [\mathbf{F}_\mathfrak{p} : \mathbf{F}_p]$.

The group $\mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$ contains the element Frob_p defined by

$$\mathrm{Frob}_p(x) = x^p,$$

because $(xy)^p = x^p y^p$ and

$$(x+y)^p = x^p + px^{p-1}y + \cdots + y^p \equiv x^p + y^p \pmod{p}.$$

By a homework problem, the group $\mathbf{F}_\mathfrak{p}^*$ is cyclic, so there is an element $a \in \mathbf{F}_\mathfrak{p}^*$ of order $p^f - 1$, and $\mathbf{F}_\mathfrak{p} = \mathbf{F}_p(a)$. Then $\mathrm{Frob}_p^n(a) = a^{p^n} = a$ if and only if $(p^f - 1) \mid p^n - 1$ which is the case preciselywhen $f \mid n$, so the order of Frob_p is f. Since the order of the automorphism group of a field extension is at most the degree of the extension, we conclude that $\mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$ is generated by Frob_p. Also, since $\mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$ has order equal to the degree, we conclude that $\mathbf{F}_\mathfrak{p}/\mathbf{F}_p$ is Galois, with group $\mathrm{Gal}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$ cyclic of order f generated by Frob_p. (Anther general fact: Up to isomorphism there is exactly one finite field of each degree. Indeed, if there were two of degree f, then both could be characterized as the set of roots in the compositum of $x^{p^f} - 1$, hence they would be equal.)

1.2 The Exact Sequence

As mentioned above, there is a natural reduction homomorphism

$$\varphi : D_\mathfrak{p} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p).$$

Theorem 1.5. *The homomorphism φ is surjective.*

Proof. Let $\tilde{a} \in \mathbf{F}_\mathfrak{p}$ be an element such that $\mathbf{F}_\mathfrak{p} = \mathbf{F}_p(a)$. Lift $\tilde{a}$ to an algebraic integer $a \in \mathcal{O}_K$, and let $f = \prod_{\sigma \in D_p}(x - \sigma(a)) \in K^D[x]$ be the characteristic polynomial of a over K^D. Using Proposition 1.4 we see that f reduces to the minimal polynomial $\tilde{f} = \prod(x - \widetilde{\sigma(a)}) \in \mathbf{F}_p[x]$ of $\tilde{a}$ (by the Proposition the coefficients of $\tilde{f}$ are in $\mathbf{F}_p$, and $\tilde{a}$ satisfies $\tilde{f}$, and the degree of $\tilde{f}$ equals the degree of the minimal polynomial of $\tilde{a}$). The roots of $\tilde{f}$ are of the form $\tilde{\sigma}(a)$, and the element $\mathrm{Frob}_p(a)$ is also a root of $\tilde{f}$, so it is of the form $\widetilde{\sigma(a)}$. We conclude that the generator Frob_p of $\mathrm{Gal}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$ is in the image of φ, which proves the theorem. $\square$

Definition 1.6 (Inertia Group). The *inertia group* is the kernel $I_\mathfrak{p}$ of $D_\mathfrak{p} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$.

Combining everything so far, we find an exact sequence of groups

$$1 \to I_{\mathfrak{p}} \to D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p) \to 1. \tag{1.1}$$

The inertia group is a measure of how p ramifies in K.

Corollary 1.7. *We have $\#I_{\mathfrak{p}} = e(\mathfrak{p}/p)$, where $\mathfrak{p}$ is a prime of K over p.*

Proof. The sequence (1.1) implies that $\#I_{\mathfrak{p}} = \#D_{\mathfrak{p}}/f(K/\mathbf{Q})$. Applying Propositions 1.3–1.4, we have

$$\#D_{\mathfrak{p}} = [K : L] = \frac{[K : \mathbf{Q}]}{g} = \frac{efg}{g} = ef.$$

Dividing both sides by $f = f(K/\mathbf{Q})$ proves the corollary. $\square$

We have the following characterization of $I_{\mathfrak{p}}$.

Proposition 1.8. *Let $K/\mathbf{Q}$ be a Galois extension with group G, let $\mathfrak{p}$ be a prime lying over a prime p. Then*

$$I_{\mathfrak{p}} = \{\sigma \in G : \sigma(a) = a \pmod{\mathfrak{p}} \text{ for all } a \in \mathcal{O}_K\}.$$

Proof. By definition $I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : \sigma(a) = a \pmod{\mathfrak{p}} \text{ for all } a \in \mathcal{O}_K\}$, so it suffices to show that if $\sigma \notin D_{\mathfrak{p}}$, then there exists $a \in \mathcal{O}_K$ such that $\sigma(a) = a \pmod{\mathfrak{p}}$. If $\sigma \notin D_{\mathfrak{p}}$, we have $\sigma^{-1}(\mathfrak{p}) \neq \mathfrak{p}$, so since both are maximal ideals, there exists $a \in \mathfrak{p}$ with $a \notin \sigma^{-1}(\mathfrak{p})$, i.e., $\sigma(a) \notin \mathfrak{p}$. Thus $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. $\square$

Figure 1.2 is a picture of the splitting behavior of a prime $p \in \mathbf{Z}$.

2 Frobenius Elements

Suppose that $K/\mathbf{Q}$ is a finite Galois extension with group G and p is a prime such that $e = 1$ (i.e., an unramified prime). Then $I = I_{\mathfrak{p}} = 1$ for any $\mathfrak{p} \mid p$, so the map φ of Section 1.2 is a canonical isomorphism $D_{\mathfrak{p}} \cong \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$. By Section 1.1, the group $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$ is cyclic with canonical generator Frob_p. The *Frobenius element* corresponding to $\mathfrak{p}$ is $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$. It is the unique element of G such that for all $a \in \mathcal{O}_K$ we have

$$\mathrm{Frob}_{\mathfrak{p}}(a) \equiv a^p \pmod{\mathfrak{p}}.$$

(To see this argue as in the proof of Proposition 1.8.) Just as the primes $\mathfrak{p}$ and decomposition groups D are all conjugate, the Frobenius elements over a given prime are conjugate.

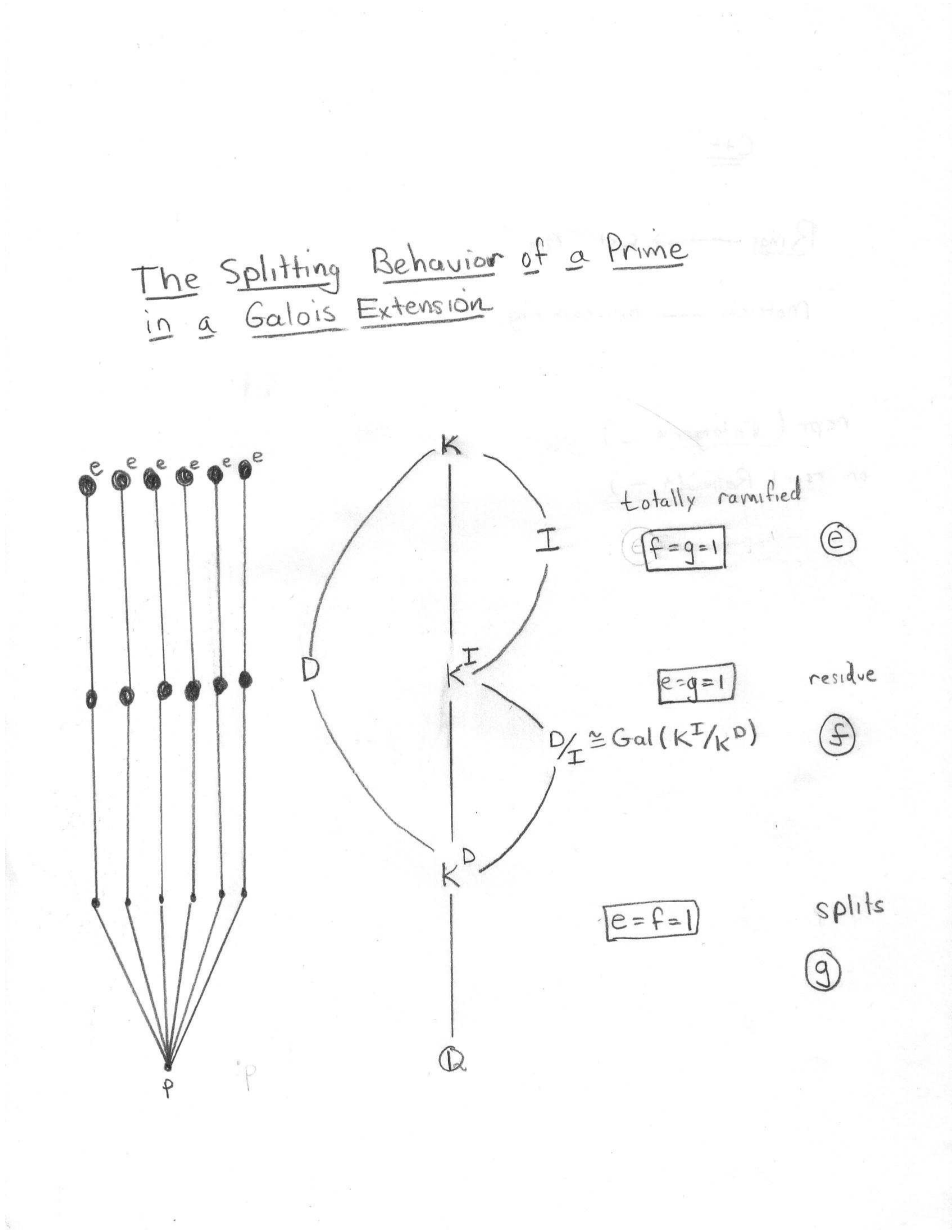

Figure 1.1: The Splitting of Behavior of a Prime in a Galois Extension

Proposition 2.1. *For each $\sigma \in G$, we have*

$$\mathrm{Frob}_{\sigma\mathfrak{p}} = \sigma \, \mathrm{Frob}_{\mathfrak{p}} \, \sigma^{-1}.$$

In particular, the Frobenius elements lying over a given prime are all conjugate.

Proof. Fix $\sigma \in G$. For any $a \in \mathcal{O}_K$ we have $\mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - \sigma^{-1}(a) \in \mathfrak{p}$. Multiply by σ we see that $\sigma \, \mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - a \in \sigma\mathfrak{p}$, which proves the proposition. $\square$

Thus the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ in G is a well defined function of p. For example, if G is abelian, then $\mathrm{Frob}_{\mathfrak{p}}$ does not depend on the choice of $\mathfrak{p}$ lying over p and we obtain a well defined symbol $\left(\frac{K/\mathbf{Q}}{p}\right) = \mathrm{Frob}_{\mathfrak{p}} \in G$ called the *Artin symbol*. It extends to a map from the free abelian group on unramified primes to the group G (the fractional ideals of $\mathbf{Z}$). Class field theory (for $\mathbf{Q}$) sets up a natural bijection between abelian Galois extensions of $\mathbf{Q}$ and certain maps from certain subgroups of the group of fractional ideals for $\mathbf{Z}$. We have just described one direction of this bijection, which associates to an abelian extension the Artin symbol (which induces a homomorphism). The Kronecker-Weber theorem asserts that the abelian extensions of $\mathbf{Q}$ are exactly the subfields of the fields $\mathbf{Q}(\zeta_n)$, as n varies over all positive integers. By Galois theory there is a correspondence between the subfields of $\mathbf{Q}(\zeta_n)$ (which has Galois group $(\mathbf{Z}/n\mathbf{Z})^*$) and the subgroups of $(\mathbf{Z}/n\mathbf{Z})^*$. Giving an abelian extension of $\mathbf{Q}$ is *exactly the same* as giving an integer n and a subgroup of $(\mathbf{Z}/n\mathbf{Z})^*$. Even more importantly, the reciprocity map $p \mapsto \left(\frac{Q(\zeta_n)/\mathbf{Q}}{p}\right)$ is simply $p \mapsto p \in (\mathbf{Z}/n\mathbf{Z})^*$. This is a nice generalization of quadratic reciprocity: for $\mathbf{Q}(\zeta_n)$, the efg for a prime p depends in a simple way on nothing but $p \mod n$.

3 Galois Representations and a Conjecture of Artin

The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is an object of central importance in number theory, and I've often heard that in some sense number theory is the study of this group. A good way to study a group is to study how it acts on various objects, that is, to study its representations.

Endow $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ with the topology which has as a basis of open neighborhoods of the origin the subgroups $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$, where K varies over finite Galois extensions of $\mathbf{Q}$. (Note: This is **not** the topology got by taking as a basis of open neighborhoods the collection of finite-index normal subgroups of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) Fix a positive integer n and let $\mathrm{GL}_n(\mathbf{C})$ be the group of $n \times n$ invertible matrices over $\mathbf{C}$ with the discrete topology.

Definition 3.1. A *complex n-dimensional representation* of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(\mathbf{C}).$$

For ρ to be continuous means that there is a finite Galois extension $K/\mathbf{Q}$ such that ρ factors through $\mathrm{Gal}(K/\mathbf{Q})$:

$$\begin{tikzcd}
\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{GL}_n(\mathbf{C}) \\
& \mathrm{Gal}(K/\mathbf{Q}) \arrow[ur, "\rho'"'] &
\end{tikzcd}$$

For example, one could take K to be the fixed field of $\ker(\rho)$. (Note that continous implies that the image of ρ is finite, but using Zorn's lemma one can show that there are homomorphisms $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \{\pm 1\}$ with finite image that are not continuous, since they do not factor through the Galois group of any finite Galois extension.)

Fix a Galois representation ρ and a finite Galois extension K such that ρ factors through $\mathrm{Gal}(K/\mathbf{Q})$. For each prime $p \in \mathbf{Z}$ that is not ramified in K, there is an element $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbf{Q})$ that is well-defined up to conjugation by elements of $\mathrm{Gal}(K/\mathbf{Q})$. This means that $\rho'(\mathrm{Frob}_p) \in \mathrm{GL}_n(\mathbf{C})$ is well-defined up to conjugation. Thus the characteristic polynomial $F_p \in \mathbf{C}[x]$ is a well-defined invariant of p and ρ. Let $R_p(x) = x^{\deg(F_p)} \cdot F_p(1/x)$ be the polynomial obtain by reversing the order of the coefficients of F_p. Following E. Artin, let $n = [K : \mathbf{Q}]$ and set

$$L(\rho, s) = \prod_{p \text{ unramified}} \frac{1}{R_p(p^{-s})}.$$

We view. $L(\rho, s)$ as a function of a single complex variable s. One can prove that $L(\rho, s)$ is holomorphic on some right half plane, and extends to a meromorphic function on all $\mathbf{C}$.

Conjecture 3.2 (Artin). *The L-series of any continuous representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(\mathbf{C})$ is an entire function on all $\mathbf{C}$, except possibly at 1.*

This conjecture asserts that there is a way to analytically continue $L(\rho, s)$ to the whole complex plane, except possibly at 1. The simple pole at $s = 1$

corresponds to the trivial representation (the Riemann zeta function), and if $n \geq 2$ and ρ is irreducible, then the conjecture is that ρ extends to a holomorphic function on all $\mathbf{C}$.

The conjecture follows from class field theory for $\mathbf{Q}$ when $n = 1$. When $n = 2$ and the image of ρ in $\mathrm{PGL}_2(\mathbf{C})$ is a solvable group, the conjecture is known, and is a deep theorem of Langlands and others (see *Base Change for* GL_2). When $n = 2$ and the projective image is not solvable, the only possibility is that the projective image is isomorphic to the alternating group A_5. Because A_5 is the symmetric group of the icosahedron, these representations are called *icosahedral*. In this case Joe Buhler's Harvard Ph.D. thesis gave the first example, there is a whole book (Springer Lecture Notes 1585, by Frey, Kiming, Merel, et al.), which proves Artin's conjecture for 7 icosahedral representation (none of which are twists of each other). Kevin Buzzard and I (Stein) proved the conjecture for 8 more examples. Subsequently, Richard Taylor, Kevin Buzzard, and Mark Dickinson proved the conjecture for an infinite class of icosahedral Galois representations (disjoint from the examples). The general problem for $n = 2$ is still open, but perhaps Taylor and others are still making progress toward it.