Math 129: Algebraic Number Theory
Lecture 14: Galois Representations, Absolute Values

William Stein

Thursday, March 23, 2004

We start with a quick review of last time:

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 $p \in \mathbf{Z}$. The *decomposition group* of $\mathfrak{p}$ is the subgroup

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

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 $[G : D_{\mathfrak{p}}] = g$. (This clarifies the key point that was confusing me last time.)

We proved:

Lemma 0.1. *The decomposition subgroups $D_{\mathfrak{p}}$ corresponding to primes $\mathfrak{p}$ lying over a given p are all conjugate in G.*

Proposition 0.2. *The fixed field K^D of D*

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

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

Proposition 0.3. *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 $e(K/\mathbf{Q}) = e(K/L)$.*

There is a natural reduction homomorphism

$$\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p), \tag{0.1}$$

and we proved last time that it is surjective. The key point was that the reduction of the characteristic polynomial of a certain lift of a generator of $\mathbf{F}_{\mathfrak{p}}$ was in $\mathbf{F}_p[x]$. Now, back to our story....

1 The Inertia Group

Definition 1.1 (Inertia Group). The *inertia group* is the kernel $I_{\mathfrak{p}}$ of $D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$.

Thus we have 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 1.2. *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 0.2–0.3, 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. □

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

Proposition 1.3. *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 $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. □

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 (0.1) is a canonical isomorphism $D_{\mathfrak{p}} \cong \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p)$. 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 1.3.) Just as the primes $\mathfrak{p}$ and decomposition groups D are all conjugate, the Frobenius elements over a given prime are conjugate.

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. □

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 Major Conjecture of Artin

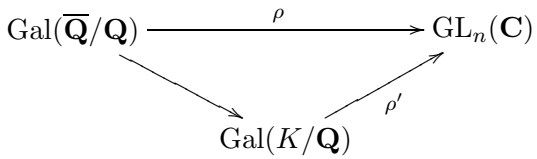
The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is an object of central importance in number theory, and I've often heard that in some sense number theory is the study of this group. A good way to study a group is to study how it acts on various objects, that is, to study its representations.

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 $\mathrm{Gal}(K/\mathbf{Q})$:



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

$$R_p(x) = x^{\deg(F_p)} \cdot F_p(1/x) = 1 + \cdots + \mathrm{Det}(\mathrm{Frob}_p) \cdot x^{\deg(F_p)}$$

be the polynomial obtain by reversing the order of the coefficients of F_p. Following E. Artin, set

$$L(\rho, s) = \prod_{p \text{ unramified}} \frac{1}{R_p(p^{-s})}. \tag{3.1}$$

(Note: Please change what's in the handout for day13 to (3.1).) 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 some way to analytically continue $L(\rho, s)$ to the whole complex plane, except possibly at 1. (A standard fact from complex analysis is that this analytic continuation must be unique.) 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), which played a crucial roll in Wiles's proof of Fermat's Last Theorem. 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.

4 Absolute Values

We will now move onto something different: absolute values, completions, local fields, adeles, and ideles. A common technique in mathematics is to "reduce to the local case" in order to gain a much clearer understanding of what is going on, and the methods we will introduce next, which are basic to much modern number theory, allow us to do that for number fields.

Fix a field K for the rest of this section.

Definition 4.1 (Absolute Value). An *absolute value* on K is a map $\|\cdot\| : K \to \mathbf{R}$ such that there is some $\alpha > 0$ such that for all $a, b \in K$, we have

- $\|a\| \geq 0$ and $\|a\| = 0$ if and only if $a = 0$,
- $\|a\| \cdot \|b\| = \|ab\|$, and
- $\|a + b\|^\alpha \leq \|a\|^\alpha + \|b\|^\alpha$.

Example 4.2. Suppose $\sigma : K \hookrightarrow \mathbf{C}$. Let $\|a\| = |\sigma(a)|$, where $|\sigma(a)|$ is the usual absolute value on $\mathbf{C}$.

On any field K, the *trivial absolute value* is the one given by

$$\|a\| = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0. \end{cases}$$

Definition 4.3 (Places). Two absolute values $\|\cdot\|_1$ and $\|\cdot\|_2$ on a field K are *equivalent* if there exists a $c > 0$ such that $\|\cdot\|_1 = \|\cdot\|_2^c$. A *place* for a field K is an equivalence class of absolute values on K.

Recall that a metric space is a set X equipped with a metric $d : X \times X \to \mathbf{R}_{\geq 0}$, which is a function such that there is an α so that for all $x, y, z \in X$ we have $d(x, x) = 0$, $d(x, y) = d(y, x)$, $d(x, z)^\alpha \leq d(x, y)^\alpha + d(y, z)^\alpha$, and $d(x, y) = 0 \implies x = y$. A metric on a space induces a topology, in which a basis of open sets is the collection of all open balls

$$B(a, r) = \{x \in K : d(x, a) < r\}.$$

If $\|\cdot\|$ is an absolute value on a field K, then $d(x, y) = \|x - y\|$ is a metric on K, and hence $\|\cdot\|$ induces a topology on K. For example, the trivial absolute value induces the discrete topology, since every point set is open, as $B(a, \frac{1}{2}) = \{a\}$.

Proposition 4.4. *Two valuations $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent if and only if they induce the same topology on K.*

Proof. ($\Longrightarrow$) First suppose $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent. Then there is a $c > 0$ such that $\|\cdot\|_1 = \|\cdot\|_2^c$. Thus

$$\begin{aligned} B_1(a, r) &= \{x \in K : \|x - a\|_1 < r\} \\ &= \{x \in K : \|x - a\|_2 < r^{1/c}\} = B_2(a, r^{1/c}). \end{aligned}$$

Thus the collection of all open balls for $\|\cdot\|_1$ is exactly the same as the set of open balls for $\|\cdot\|_2$, hence the topologies are the same.

($\Longleftarrow$) Next suppose $\|\cdot\|_1$ and $\|\cdot\|_2$ induce the same topology on K. To deduce that the two absolute values are equivalent, we prove a lemma.

Lemma 4.5. *For any sequence $\{x_n\}$ in K we have*

$$\|x_n\|_1 \to 0 \iff \|x_n\|_2 \to 0.$$

Proof. It suffices to prove that if $\|x_n\|_1 \to 0$ then $\|x_n\|_2 \to 0$, since the proof of the other implication is the same. Let $\varepsilon > 0$. The topologies induced by the two absolute values are the same, so $B_2(0, \varepsilon)$ can be covered by open balls $B_1(a_i, r_i)$. One of these open balls $B_1(a, r)$ contains 0, and using the triangle inequality we see that there is $\varepsilon' > 0$ such that

$$B_1(0, \varepsilon') \subset B_1(a, r) \subset B_2(0, \varepsilon).$$

Since $\|x_n\|_1 \to 0$, there exists N such that for $n \geq N$ we have $\|x_n\|_1 < \varepsilon'$. For such n, we have $x_n \in B_1(0, \varepsilon')$, so $x_n \in B_2(0, \varepsilon)$, so $\|x_n\|_2 < \varepsilon$. Thus $\|x_n\|_2 \to 0$. □

If $x \in K$ and $i = 1, 2$, then $\|x^n\|_i \to 0$ if and only if $\|x\|_i^n \to 0$, which is the case if and only if $\|x\|_i < 1$. Thus Lemma 4.5 implies that $\|x\|_1 < 1$ if and only if $\|x\|_2 < 1$.

If there is no nonzero $x \in K$ with $\|x\|_1 < 1$, then $\|x\|_1 = 1$ for all $x \neq 0$ (otherwise $\|x\|_1 > 1 \implies \|1/x\|_1 < 1$), so $\|\cdot\|_1$ induces the discrete topology. Since $\|\cdot\|_1$ and $\|\cdot\|_2$ induce the same topology, $\|\cdot\|_2$ also induces the discrete topology. If $\|\cdot\|_2$ is nontrivial then there exists a nonzero $x \in K$ with $\|x\|_2 < 1$. Then $\|x^n\|_2 \to 0$, so for all $\varepsilon > 0$ there exists N such that for $n \geq N$ we have $x^n \in B(0, \varepsilon)$. In the discrete topology every point is open, so there exists $\varepsilon > 0$ such that $B(0, \varepsilon) = \{0\}$. But then $x^n = 0$ for n sufficiently large, hence $x = 0$, a contradiction. This completes the proof of the proposition when $\|\cdot\|_1$ is trivial.

We may assume there is a nonzero $x_0 \in K$ with $\|x_0\|_1 < 1$. As mentioned above $\|x_0\|_2 < 1$ as well. We will use this x_0 to show that $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent. Let $\gamma > 0$ be the real number such that $\|x_0\|_2 = \|x_0\|_1^\gamma$, so

$\gamma = \log(\|x_0\|_2)/\log(\|x_0\|_1)$. For any nonzero $x \in K$ with $\|x\|_1 < 1$, let λ be such that $\|x\|_1 = \|x_0\|_1^\lambda$. We now prove that $\|x\|_2 = \|x_0\|_2^\lambda$. If a/b is any nonzero rational number with $a/b > \lambda$, then

$$\left\| \frac{x_0^a}{x^b} \right\|_1 = \frac{\|x_0\|_1^a}{\|x\|_1^b} = \frac{\|x_0\|_1^a}{\|x_0\|_1^{\lambda b}} = \|x_0\|_1^{a-\lambda b} < 1$$

(since $a - \lambda b > 0$ and $\|x_0\|_1 < 1$), so $\left\|x_0^a/x^b\right\|_2 < 1$ also. Hence $\|x_0\|_2^a < \|x\|_2^b$, so $\|x_0\|_2^{a/b} < \|x\|_2$. Likewise, if a/b is a nonzero rational number with $a/b < \lambda$, arguing as above we see that $\|x_0\|_2^{a/b} > \|x\|_2$. Combining these two facts, we see that $\|x\|_2 = \|x_0\|_2^\lambda$. Thus

$$\|x\|_2 = \|x_0\|_2^\lambda = \|x_0\|_1^{c\lambda} = \|x\|_1^c \,,$$

hence $\|\cdot\|_1$ is equivalent to $\|\cdot\|_2$, as claimed. □

Assume henceforth that K has characteristic 0.

Definition 4.6 (Archimedean). An absolute value is *archimedean* if there is an integer $n \in K$ such that $\|n\| > 1$. An absolute value is *non-archimedean* if it is not archimedean.

Proposition 4.7. *Let K be a number field. The archimedean valuations are all of the form $\|a\| = |\sigma(a)|^c$, where $\sigma : K \hookrightarrow \mathbf{C}$ is an embedding, $c > 0$, and $|\cdot|$ is the usual absolute value on $\mathbf{C}$.*

Proof. □

Proposition 4.8. *Suppose $\|\cdot\|$ is a non-archimedean valuation on a number field K. Then there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ and a constant $C > 1$ such that*

$$\|a\| = C^{-\operatorname{ord}_\mathfrak{p}(a)},$$

where $\operatorname{ord}_\mathfrak{p}(a)$ is the largest power of $\mathfrak{p}$ that divides the ideal $a\mathcal{O}_K$. (Note that when $a = 0$, $\|a\| = C^{-\infty} = 0$, as expected.)

5 Completions and Local Fields

Completion of K at $\mathfrak{p}$. Hensel's Lemma. Weak Approximation.