18.785 Number theory I **Fall 2015**
Lecture #12 **10/22/2015**

12 Ramification, Haar measure, the product formula

12.1 Ramification in terms of the different and discriminant

We conclude our discussion of the different and discriminant by analyzing the information they give us about the primes that ramify in an extension. Recall our standard $AKLB$ setup, where A is a Dedekind domain, K is its fraction field, L is a finite separable extension of K, and B is the integral closure of A in L (a Dedekind domain with fraction field L). We wish to understand the primes (nonzero prime ideals) $\mathfrak{p}$ of A that *ramify* in B, meaning that there is a prime $\mathfrak{q}|\mathfrak{p}$ lying above $\mathfrak{p}$ (recall that this means either the ramification index $e_{\mathfrak{q}}$ is greater than 1, or the residue field extension is inseparable; in other words, $\mathfrak{p}$ is unramified if and only if $B/\mathfrak{p}B$ is an étale $(A/\mathfrak{p})$-algebra). We say that the extension L/K is *unramified at* $\mathfrak{p}$ if the prime $\mathfrak{p}$ is unramified (in which case all the primes $\mathfrak{q}|\mathfrak{p}$ are unramified), and that it is *unramified at* $\mathfrak{q}$ if the prime $\mathfrak{q}$ is unramified.

Theorem 12.1. *Assume $AKLB$, let $\mathfrak{q}$ be a prime of B lying above a prime $\mathfrak{p}$ of A. The extension L/K is unramified at $\mathfrak{q}$ if and only if $\mathfrak{q}$ does not divide $\mathcal{D}_{B/A}$, and it is unramified at $\mathfrak{p}$ if and only if $\mathfrak{p}$ does not divide $D_{B/A}$.*

Proof. We first consider the different ideal $\mathcal{D}_{B/A}$. By Proposition 11.11, the different respects completion, so it suffices to consider the case that A and B are complete DVRs (complete K at $\mathfrak{p}$ and L at $\mathfrak{q}$ and apply Theorem 11.4). We then have $[L:K] = e_{\mathfrak{q}}f_{\mathfrak{q}}$, where $e_{\mathfrak{q}}$ is the ramification index and $f_{\mathfrak{q}}$ is the residue field degree, and $\mathfrak{p}B = \mathfrak{q}^{e_{\mathfrak{q}}}$.

Since B is a DVR with maximal ideal $\mathfrak{q}$, we must have $\mathcal{D}_{B/A} = \mathfrak{q}^m$ for some $m \ge 0$. Apply Theorem 11.23 to compute the discriminant $D_{B/A}$, we have

$$D_{B/A} = N_{B/A}(\mathcal{D}_{B/A}) = N_{B/A}(\mathfrak{q}^m) = \mathfrak{p}^{fm}.$$

Thus $\mathfrak{q}|\mathcal{D}_{B/A}$ if and only if $\mathfrak{p}|D_{B/A}$. Since A is a PID, B is a free A-module and we may choose an A-module basis $e_1,\ldots,e_n$ for B that is also a K-vector space for L. Let $k = A/\mathfrak{p}$ and let $\overline{e}_1$ denote the reduction of e_i in k-algebra $B/\mathfrak{p}B$ (which is not necessarily a field).

Since B has an A-module basis, we may compute its discriminant as

$$D_{B/A} = (\operatorname{disc}(e_1,\ldots,e_n)) = (\det[\mathrm{T}_{L/K}(b_ib_j)]_{ij}).$$

Thus $\mathfrak{p}|D_{B/a}$ if and only if $\det[\mathrm{T}_{L/K}(b_ib_j)]_{ij} \in \mathfrak{p}$, equivalently, the discriminant of the basis $\overline{e}_1,\ldots,\overline{e}_n$ for the k-algebra $B/\mathfrak{p}B$ is zero. By Lemma 12.2 below, $\operatorname{disc}(\overline{e}_1,\ldots,\overline{e}_n) \neq 0$ if and only if the k-algebra $B/\mathfrak{p}B$ is finite étale.

If $e_{\mathfrak{q}} > 1$ then $B/\mathfrak{p}B = B/\mathfrak{q}^{e_{\mathfrak{q}}}$ contains nonzero nilpotents (take any uniformizer for $\mathfrak{q}$) and cannot be finite étale; in this case $\mathfrak{q}|\mathcal{D}_{B/A}$ and $\mathfrak{q}$ is ramified.

If $e_{\mathfrak{q}} = 1$ then $B/\mathfrak{p} = B/\mathfrak{q}$ is a field and (by definition) $\mathfrak{q}$ is unramified if and only if $B/\mathfrak{q}$ is a separable extension of k, equivalently, a finite étale k-algebra, which we have shown occurs if and only if $\mathfrak{q}$ does not divide $\mathcal{D}_{B/A}$.

We now consider the discriminant $D_{B/A}$ in the general case, where A is not necessarily a complete DVR. Let $\mathcal{D}_{B/A} = \prod_i \mathfrak{q}_i^{m_i}$ be the factorization of the different ideal. By Theorem 11.23 we have

$$D_{B/A} = N_{B/A}(\mathcal{D}_{B/A}) = N_{B/A}\left(\prod_i \mathfrak{q}_i^{m_i}\right) = \prod \mathfrak{p}_i^{f_i\mathfrak{m}_i},$$

Lecture by Andrew Sutherland

where $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ is the prime below $\mathfrak{q}_i$. If $\mathfrak{p}$ divides $D_{B/A}$ then $\mathfrak{p} = \mathfrak{p}_i$ for some $\mathfrak{q}_i$ dividing $D_{B/A}$, and this can occur only if some $\mathfrak{q}|\mathfrak{p}$ divides $\mathcal{D}_{B/A}$, which we have already shown is equivalent to $\mathfrak{q}$ being ramified. Thus $\mathfrak{p}$ divides $D_{B/A}$ if and only if $\mathfrak{p}$ is ramified. □

Lemma 12.2. *Let k be a field and let R be a commutative k-algebra that is a finite dimensional k-vector space with basis $r_1, \ldots, r_n$. Then R is a finite étale k-algebra if and only if the discriminant* $\operatorname{disc}(r_1, \ldots, r_n) = \det[\mathrm{T}_{R/k}(r_i r_j)]_{ij} \in k$ *is nonzero.*

Proof. We first note that the choice of basis is immaterial, changing the basis will not change whether the discriminant is zero or nonzero.

Suppose R contains a nonzero nilpotent r (meaning $r^m = 0$ for some $m > 1$). In this case R cannot be finite étale (a product of fields has no nonzero nilpotents). We can extend $\{r\}$ to a basis, so we assume $r_1 = r$ is nilpotent. Every multiple of r is also nilpotent, and it follows that the first row of the matrix $[\mathrm{T}_{R/k}(r_i r_j)]_{ij}$ is zero and therefore has zero determinant. Here we have used the fact that the trace of any nilpotent element is zero (if a is nilpotent the eigenvalues of the multiplication-by-a map must all be zero).

Suppose R contains no nonzero nilpotents. Then R is isomorphic to a product $\prod_i L_i$ of finite extensions L_i/k, and we can assume our basis contains bases for each, grouped together so that $[\mathrm{T}_{R/k}(r_i r_j)]_{ij}$ is block diagonal. The determinant is then nonzero if and only if the determinant of each block is nonzero, so we can reduce to the case where R/k. The proof then follows from the fact that the trace pairing $\mathrm{T}_{R/k}$ is nondegenerate if and only if R/k is separable (this follows from Proposition 4.58 and Problem 4 of Problem Set 2). □

We now note an important corollary of Theorem 12.1.

Corollary 12.3. *Assume AKLB. Only finitely many primes of A (or B) ramify.*

Proof. Both A and B are Dedekind domains, so the ideals $D_{B/A}$ and $\mathcal{D}_{B/A}$ both have unique factorizations into prime ideals in which only finitely many primes appear. □

Example 12.4. Consider $A = \mathbb{Z}$, $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$. What is $B = \mathcal{O}_L$? We know that $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$, and that it has finite index m. We can compute the absolute discriminant of $\mathbb{Z}[\alpha]/\mathbb{Z}$ as

$$\operatorname{disc}(1, \alpha, \alpha^2) = \operatorname{disc}(x^3 - x - 1) = -4(-1)^3 - 27(-1)^2 = -23.$$

The $\mathbb{Z}$-ideal $D_{\mathbb{Z}[\alpha]/\mathbb{Z}}$ is principal (because $\mathbb{Z}$ is a PID) and therefore must be generated by the integer $-23/m^2$; this implies $m = 1$ and $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

We now note a number of results that allow us to explicitly compute the discriminant and different.

Proposition 12.5. *Assume AKLB. If $B = A[\alpha]$ for some $\alpha \in L$ and $f \in A[x]$ is the minimal polynomial of α, then*

$$\mathcal{D}_{B/A} = (f'(\alpha))$$

is the B-ideal generated by $f'(\alpha)$.

Proof. See Problem Set 6. □

The assumption $B = A[\alpha]$ in Proposition 12.5 does not always hold, but if we want to compute the power of $\mathfrak{q}$ that divides $\mathcal{D}_{B/A}$ we can complete L at $\mathfrak{q}$ and K at $\mathfrak{p} = \mathfrak{q} \cap A$ so that A and B become complete DVRs, in which case $B = A[\alpha]$ does hold (by Lemma 10.15), so long as the residue field extension is separable (always true if K and L are global fields, since the residue fields are then finite, hence perfect). The following definition and proposition give an alternative approach.

Definition 12.6. Assume $AKLB$ and let $\alpha \in B$ have minimal polynomial $f \in A[x]$. The *different of* α is defined by

$$\delta_{B/A}(\alpha) = \begin{cases} f'(\alpha) & \text{if } L = K(\alpha), \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 12.7. *Assume $AKLB$. Then $\mathcal{D}_{B/A} = \big(\delta_{B/A}(\alpha) : \alpha \in B\big)$.*

Proof. See [2, Thm. III.2.5]. □

We can now more precisely characterize the ramification information given by the different ideal.

Theorem 12.8. *Assume $AKLB$ and let $\mathfrak{q}$ be a prime of L lying above $\mathfrak{p} = \mathfrak{q} \cap A$ for which the residue field extension $(B/\mathfrak{q})/(A/\mathfrak{p})$ is separable. Let $s = v_{\mathfrak{q}}(\mathcal{D}_{B/A})$, let $e = e_{\mathfrak{q}}$ be the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$, and let p be the characteristic of $A/\mathfrak{p}$. If $p \nmid e$ then*

$$s = e - 1$$

and if $p|e$ then

$$e \le s \le e - 1 + e v_{\mathfrak{p}}(e)$$

Proof. See Problem Set 6. □

We also note the following proposition, which shows how the discriminant and different behave in a tower of extensions.

Proposition 12.9. *Assume $AKLB$ and let M/L be a finite separable extension and let C be the integral closure of A in M. Then*

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B} \cdot \mathcal{D}_{B/A}$$

(where the product on the right is taken in C), and

$$D_{C/A} = (D_{B/A})^{[M:L]} N_{B/A}(D_{C/B}).$$

Proof. See [3, Prop. III.8]. □

If $M/L/K$ is a tower of finite separable extensions, we note that the primes $\mathfrak{p}$ of K that ramify are precisely those that divide either $D_{L/K}$ or $N_{L/K}(D_{M/L})$.

12.2 Haar measure

We now return to our discussion of local and global fields. Recall that local fields are fields with a nontrivial absolute value that are locally compact in the corresponding topology. A key feature of local fields, and more generally, locally compact groups, is that they can be equipped with a *Haar measure*. In this section we briefly review Haar measures and show that they give us a canonical way to normalize absolute values on nonarchimedean local fields; this explains, for example, why we define the p-adic absolute value to be $|\cdot|_p := p^{-v(\cdot)}$; for any $0 < c < 1$, replacing $p^{-v(\cdot)}$ with $c^{v(\cdot)}$ would give an equivalent absolute value that defines the same topology on $\mathbb{Q}_p$, but it would not be compatible with the Haar measure on $\mathbb{Q}_p$ in a sense that will made clear below (see Proposition 12.14).

Definition 12.10. Let X be a locally compact Hausdorff space. The σ-algebra Σ of X is the collection of subsets of X generated by the open and closed sets under countable unions and countable intersections. Its elements are called *Borel sets*, or simply *measurable sets*. A *Borel measure* on X is a countably additive function

$$\mu\colon \Sigma \to \mathbb{R}_{\geq 0} \cup \{\infty\}.$$

A *Radon measure* on X is Borel measure that additionally satisfies

1. $\mu(S) < \infty$ if S is compact,
2. $\mu(S) = \inf\{\mu(U) | S \subseteq U, U \text{ open}\}$,
3. $\mu(S) = \sup\{\mu(C) | C \subseteq S, C \text{ compact}\}$,

for all Borel sets S.[1]

Definition 12.11. A topological group that is both locally compact and Hausdorff is called a *locally compact group*. A (*left*) *Haar measure* μ on a locally compact group (written additively) is a nonzero Radon measure that is *translation invariant*, meaning that

$$\mu(E) = \mu(x + E)$$

for all $x \in X$ and Borel sets E.

One defines a right Haar measure analogously, but in most cases they coincide and in our situation we are working with an abelian group (the additive group of a field), in which case they necessarily do. The key result on Haar measures, is that they exist and are unique up to scaling. For compact groups existence was proved by Haar and uniqueness by von Neumann; the general result for locally compact groups was proved by Weil.

Theorem 12.12 (Weil)**.** *Every locally compact group G has a Haar measure. If μ and μ' are two Haar measure on G then there is a positive real number λ for which $\mu'(S) = \lambda\mu(S)$ for all measurable sets S.*

Proof. See [1, §7.2]. □

Example 12.13. The standard Euclidean measure on $\mathbb{R}^n$ is the unique Haar measure on $\mathbb{R}^n$ for which the unit cube has measure 1.

[1] Some authors additionally require X to be σ-compact (a countable union of compact sets). Local fields are σ-compact so this distinction will not concern us.

The additive group of a local field K is a locally compact group (it is a metric space, so it is automatically Hausdorff). For compact groups G, it is standard to normalize the Haar measure so that $\mu(G) = 1$, but local fields are never compact and we will always have $\mu(K) = \infty$. However, the valuation ring $A = B_{\le 1}(0)$ of a local field is compact, and it is natural to normalize the Haar measure so that $\mu(A) = 1$.

For local fields with a discrete valuation, the Haar measure gives us a natural way to define a corresponding absolute value, independent of how we normalize the Haar measure.

Proposition 12.14. *Let K be a local field with discrete valuation v, residue field k, and absolute value*

$$|\cdot|_v := (\#k)^{-v(\cdot)},$$

and let μ be a Haar measure on K. For every $x \in K$ and measurable set $S \subseteq K$ we have

$$\mu(xS) = |x|_v \mu(S).$$

Moreover, the absolute value $|\ |_v$ is the unique absolute value compatible with the topology on K for which this is true.

Proof. Let A be the valuation ring of K with maximal ideal $\mathfrak{p}$. The proposition clearly holds for $x = 0$, so let $x \neq 0$. The map $\phi_x\colon y \mapsto xy$ is an automorphism of the additive group of K, and it follows that the composition $\mu_x = \mu \circ \phi_x$ is a Haar measure on K, hence multiple of μ. Define the function $\chi\colon K^\times \to \mathbb{R}_{\ge 0}$ by $\chi(x) = \mu_x(A)/\mu(A)$, so that $\mu_x = \chi(x)\mu$. We have

$$\chi(xy) = \frac{\mu_{xy}(A)}{\mu(A)} = \frac{\mu_x(yA)}{\mu(A)} = \frac{\chi(x)\mu_y(A)}{\mu(A)} = \frac{\chi(x)\chi(y)\mu(A)}{\mu(A)} = \chi(x)\chi(y),$$

so χ is multiplicative.

We claim that $\chi(x) = |x|_v$ for all $x \in K^\times$. Since both χ and $|\cdot|_v$ are multiplicative, it suffices to consider $x \in A\backslash\{0\}$. For any such x, the A-ideal xA is equal to $\mathfrak{p}^{v(x)}A$, since A is a DVR. The residue field $k := A/\mathfrak{p}$ is finite, hence A/xA is also finite; indeed it is a k-vector space of dimension $v(x)$ and has cardinality $[A : xA] = (\#k)^{v(x)}$. We can thus write A as a finite disjoint union of cosets of xA, and this implies that

$$\mu(A) = [A : xA]\mu(xA) = (\#k)^{v(x)}\chi(x)\mu(A),$$

and therefore $\chi(x) = (\#k)^{-v(x)} = |x|_v$, as claimed.

To prove uniqueness, note that every absolute value $|\ |$ on K that induces the same topology is equivalent to $|\ |_v$, hence of the form $|\ |_v^c$ for some $c > 0$. If $c \neq 1$ we can choose $x \in K$ with $|x|_v \neq 1$ and $S \subseteq K$ with $\mu(S) \neq 0$ so that

$$|x| = |x|_v^c = \left(\frac{\mu(xS)}{\mu(S)}\right)^c \neq \frac{\mu(xS)}{\mu(S)},$$

and then $\mu(xS) \neq |x|\mu(S)$ (we have used the fact that $|\ |_v$ is nontrivial and μ is nonzero). □

12.3 Places of a global field

Definition 12.15. A *place* of a global field K is an equivalence class of non-trivial absolute values on K. We may use M_K to denote the set of places of K. We will often identify places v with representatives $|\ |_v$ of their equivalence class. The place v is *archimedean* if the absolute value $|\ |_v$ is archimedean (this does not depend on our choice of representative), and otherwise v is *nonarchimedean.*

Example 12.16. As proved in Problem Set 1, for $\mathbb{Q}$ we have

$$M_{\mathbb{Q}} = \{|\ |_p : \text{primes } p \le \infty\},$$

where $|\ |_\infty$ denotes the archimedean absolute value on $\mathbb{Q}$, and for $\mathbb{F}_q(t)$ we may identify $M_{\mathbb{F}_q(t)}$ with the set of irreducible polynomials in $\mathbb{F}_q[t]$ together with the (nonarchimedean) absolute value $|r|_\infty = q^{\deg r}$.

Remark 12.17. In contrast with $\mathbb{Q}$, there is nothing special about the absolute value $|\ |_\infty$ on $\mathbb{F}_q(t)$, it is an artifact of our choice of the transcendental variable t. If we put $z = 1/t$ and rewrite $\mathbb{F}_q(t)$ as $\mathbb{F}_q(z)$, the absolute value $|\ |_\infty$ is the same as the absolute value $|\ |_z$ corresponding to the irreducible polynomial $z \in \mathbb{F}_q[z]$.

Definition 12.18. If L/K is an extension of global fields, for every place w of L, any absolute value $|\ |_w$ that represents the equivalence class w restricts to an absolute value on K that represents a place v of K; this v is independent of the choice of $|\ |_w$. We write $w|v$ to indicate this relationship and say that w *extends* v.

Example 12.19. If v is a place of a number field then $v|p$ for some $p \le \infty$. The place v is archimedean if $v|\infty$, and otherwise it is nonarchimedean.

Definition 12.20. Let K be a global field. For any place v of K we use K_v to denote the completion of K with respect to $|\ |_v$ (the field K_v does not depend on our choice of $|\ |_v$).

Example 12.21. If K is a number field and $v|p$ is a nonarchimedean place of K, then K_v is a finite separable extension of $\mathbb{Q}_p$. If we write

$$K \simeq \mathbb{Q}[x]/(f(x)),$$

then

$$K_v \simeq \mathbb{Q}_p[x]/(g(x)),$$

for some irreducible $g \in \mathbb{Q}_p[x]$ appearing in the factorization of f in $\mathbb{Q}_p[x]$. When $v|\infty$ is archimedean, there are only two possibilities: either $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$.

Definition 12.22. Let K be a number field and let $v|\infty$ be a place of K. If $K_v \simeq \mathbb{R}$ then v is a *real place* of K. If $K_v \simeq \mathbb{C}$ then v is a *complex place* of K.

Theorem 12.23. *Let L/K be a finite separable extension of global fields and let v be a place of K. Then there is an isomorphism of finite étale K_v-algebras*

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$$

defined by $\ell \otimes x \mapsto (\ell x, \ldots, \ell x)$.

Proof. If v is nonarchimedean this is just part (v) of Theorem 11.4, but we will give a topological proof that works for both archimedean and nonarchimedean v.

By Proposition 4.34, $L \otimes_K K_v$ is finite étale K_v-algebra of dimension $n = [L : K]$ and therefore isomorphic to a product $\prod_i L_i$ of finite separable extensions L_i/K_v; we just need to show that there is a one-to-one correspondence between the L_i and the completions L_w of L at the places $w|v$ extending v.

Each L_i is a local field, since it is a finite extension of K_v, and has a unique absolute value $|\ |_w$ that extends the absolute value $|\ |_v$ on K_v (for any choice of $|\ |_v$ representing the place v); this follows from Theorem 9.25 when v is nonarchimedean and is obviously the case if $K_v \simeq \mathbb{R}, \mathbb{C}$ is archimedean.[2] The map $L \hookrightarrow L \otimes_K K_v \simeq \prod_i L_i \twoheadrightarrow L_i$ allows us to view L as a subfield of each L_i.

We may view $L \otimes_K K_v \simeq \prod_i L_i$ as an isomorphism of topological groups: on the LHS the étale K_v-algebra $L \otimes_K K_v$ is a finite dimensional K_v-vector space with a canonical topology induced by the sup norm, and on the RHS we have the product topology; these topologies coincide because the absolute value on each L_i restricts to the absolute value on K_v, allowing us to also view the RHS as a normed K_v-vector space, and all norms on a finite dimensional vector space over a complete field induce the same topology (Proposition 9.24). The image of the canonical embedding $L \hookrightarrow L \otimes_K K_v$ defined by $\ell \mapsto \ell \otimes 1$ is dense because $K \subseteq L$ is dense in K_v; for any nonzero $\ell \otimes x$ in $L \otimes_K K_v$ we can approximate it arbitrarily closely by $\ell/y \otimes y = \ell \otimes 1$ for some nonzero $y \in K$ (and we can similarly approximate sums of pure tensors). Thus the image of L is dense in $\prod_i L_i$, and in each L_i.

The restriction of $|\ |_w$ to L uniquely determines a place $w|v$ of L, and L_i is necessarily isomorphic to the completion L_w of L with respect to $|\ |_w$, because L_i is complete and L is dense in L_i. We thus have a map $\phi\colon \{L_i\} \to \{L_w : w|v\}$ that sends L_i to an isomorphic L_w.

For each $w|v$ we have a map $L \otimes_K K_v \to L_w$ induced by the inclusions $L, K_v \subseteq L_w$, and this map is surjective because the image is both dense and complete; it follows that ϕ is surjective. If ϕ is not injective then some L_w appears as two distinct L_i and L_j in $L \otimes_K K_v \simeq \prod L_i$, but this is impossible because the image of the diagonal embedding $L \to L_w \times L_w$ is not dense but the image of L is dense in $L_i \times L_j$. □

Corollary 12.24. *Let K be a number field and $p \le \infty$ a prime of $\mathbb{Q}$. There is a one-to-one-correspondence*

$$\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}_p)/\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longleftrightarrow \{v \in M_K : v|p\},$$

between $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbits of $\mathbb{Q}$-embeddings of K into $\overline{\mathbb{Q}}_p$ and the places $v|p$ of K.

Before proving the corollary, lets make sure we understand the set of Galois orbits on the LHS. Each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on a $\mathbb{Q}$-embedding $\tau\colon K \to \overline{\mathbb{Q}}_p$ by composition: $\sigma \circ \tau$ is also a $\mathbb{Q}$-embedding of K into $\overline{\mathbb{Q}}_p$.

Proof. Theorem 12.23 gives us an isomorphism $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \prod_{v|p} K_v$. We then have bijections of finite sets

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}_p) &\leftrightarrow \mathrm{Hom}_{\mathbb{Q}_p}(K \otimes_{\mathbb{Q}} \mathbb{Q}_p, \overline{\mathbb{Q}}_p)\\ &\leftrightarrow \bigsqcup_{v|p} \mathrm{Hom}_{\mathbb{Q}_p}(K_v, \overline{\mathbb{Q}}_p),\end{aligned}$$

Each $\mathrm{Hom}_{\mathbb{Q}_p}(K_v, \overline{\mathbb{Q}}_p)$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit, because if we write $K_v = \mathbb{Q}_p(\alpha)$ where $\alpha \in K_v$ has minimal polynomial $f \in \mathbb{Q}_p[x]$, we have a bijection between $\mathbb{Q}_p$-embeddings $K_v \to \overline{\mathbb{Q}}_p$ and roots of f in $\overline{\mathbb{Q}}_p$, and $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ must act transitively on both. □

[2] Note that K_v is a topological field, and the isomorphism $K_v \simeq \mathbb{R}$ or $K_v \simeq \mathbb{C}$ is an isomorphism of topological fields whose archimedean topology is induced by an absolute value; we are always viewing $\mathbb{R}$ and $\mathbb{C}$ as locally compact fields whose topology is induced by the standard Euclidean metric. There are plenty of nonarchimedean topologies on $\mathbb{R}$ and $\mathbb{C}$ (for each prime p the field isomorphism $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$ lets us put an extension of the p-adic absolute value on $\mathbb{C}$ which we can restrict to $\mathbb{R}$), but none correspond to local fields because they are not locally compact.

The corollary implies that $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})/\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ is in bijection with the set $\{v|\infty\}$ of archimedean places of K; note that $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ is just a group of order 2 whose non-trivial element is complex conjugation. We can partition $\{v|\infty\}$ into real and complex places, based on whether $K_v \simeq \mathbb{R}$ or $K_v \simeq \mathbb{C}$. Each real place corresponds to an element of $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{R})$; these are fixed by $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ and thus correspond to trivial $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-orbits of $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ (orbits of size one). Each complex place corresponds to $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-orbit of size two in $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})$; these are conjugate pairs of embeddings $K \to \mathbb{C}$ whose image does not lie in $\mathbb{R}$.

Definition 12.25. Let K be a number field. The elements of $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{R})$ are called *real embeddings*. The elements of $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ whose image does not lie in $\mathbb{R}$ are called *complex embeddings*.

There is a one-to-one correspondence between real embeddings and real places, but complex embeddings come in conjugate pairs that correspond to a single complex place.

Corollary 12.26. *Let K be a number field with r real places and s complex places. Then*

$$[K:\mathbb{Q}] = r + 2s.$$

Proof. Recall that $[K:\mathbb{Q}] = \#\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ (write $K = \mathbb{Q}[x]/(f(x))$ and note that the elements of $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ are determined by choosing a root of f in $\mathbb{C}$ to be the image of x). The action of $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ on $\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ has r orbits of size 1, and s orbits of size 2. □

Example 12.27. Let $K = \mathbb{Q}[x]/(x^3-2)$. There are three embeddings $K \hookrightarrow \mathbb{C}$, one for each root of x^3-2; explicitly:

$$(1)\ x \mapsto \sqrt[3]{2}, \qquad (2)\ x \mapsto e^{2\pi i/3}\cdot\sqrt[3]{2}, \qquad (3)\ x \mapsto e^{4\pi i/3}\cdot\sqrt[3]{2}.$$

The first embedding is real, while the second two are complex and conjugate to each other. Thus K has $r=1$ real place and $s=1$ complex place, and we have $[K:\mathbb{Q}] = 1\cdot 1 + 2\cdot 1 = 3$.

12.4 The product formula for global fields

Definition 12.28. Let K be a global field. For each place v of K the *normalized absolute value* $\|\ \|_v\colon K_v \to \mathbb{R}_{\ge 0}$ on the completion of K at v is defined by

$$\|x\|_v := \frac{\mu(xS)}{\mu(S)},$$

where μ is a Haar measure on K_v and S is any measurable set with $\mu(S) \ne 0$ (we can always take S to be the valuation ring $A_v := \{x \in K_v : |x|_v \le 1\}$ of K_v). Provided v is not a complex place of K, the normalized absolute value $\|\ \|_v$ is an absolute value on K_v (but otherwise not, see Warning 12.31 below).

This definition is independent of the choice of μ and S. Our standard normalization for the Haar measure on K_v is to set $\mu(A_v) = 1$ at nonarchimedean places, use the usual Euclidean measure on $\mathbb{R}$ at real places ($\mu(A_v) = 2$), and twice the usual Euclidean measure on $\mathbb{C}$ at complex places ($\mu(A_v) = 2\pi$). It follows from Proposition 12.14 that if the place v is nonarchimedean then

$$\|x\|_v = (\#k_v)^{-v(x)},$$

where k_v is the residue field of K_v and the discrete valuation $v(x)$ is uniquely determined by the place v.

Lemma 12.29. *Let L/K be a finite separable extension of global fields, let v be a place of K and let $w|v$ be a place of L. Then*

$$\|x\|_w = \|\mathrm{N}_{L_w/K_v}(x)\|_v.$$

Proof. The lemma is trivial if $[L : K] = 1$ so we assume $[L : K] > 1$. If v is archimedean then we must have $L_w \simeq \mathbb{C}$ and $K_v \simeq \mathbb{R}$, in which case for any $x \in L_w$ we have

$$\|x\|_w = \mu(xS)/\mu(S) = |x|_{\mathbb{C}}^2 = |\mathrm{N}_{\mathbb{C}/\mathbb{R}}(x)|_{\mathbb{R}} = \|\mathrm{N}_{L_w/K_v}(x)\|_v,$$

where $|\ |_{\mathbb{R}}$ and $|\ |_{\mathbb{C}}$ are the standard Euclidean absolute values on $\mathbb{R}$ and $\mathbb{C}$.

We now assume v is nonarchimedean. Let π_v and π_w be uniformizers for the local fields K_v and L_w, respectively, and let f be the degree of the residue field extension. Without loss of generality, we may assume $x = \pi_w^{w(x)}$. Theorem 6.9 and Proposition 12.14 imply

$$\|\mathrm{N}_{L_w/K_v}(\pi_w)\|_v = \|\pi_v^f\|_v = (\#k_v)^{-f},$$

so $\|\mathrm{N}_{L_w/K_v}(x)\|_v = (\#k_v)^{-fw(x)}$. Proposition 12.14 then implies

$$\|x\|_w = (\#k_w)^{-w(x)} = (\#k_v)^{-fw(x)} = \|\mathrm{N}_{L_w/K_v}(x)\|_v. \qquad \square$$

We now make two very important remarks about the normalized absolute value.

Remark 12.30. Note that if v is a nonarchimedean place of K extended by a place $w|v$ of L/K, the absolute value $\|\ \|_w$ is **not** the unique absolute value on L_w that extends the absolute value on $\|\ \|_v$ on K_v given by Theorem 9.25, it differs by a power of $n = [L_w : K_v]$, but it is equivalent to it. It might seem strange to use a normalization here that does not agree with the one we used when considering extensions of local fields in Lecture 9. The difference is that here we are thinking about a single global field K that has many different completions K_v, and we want our normalized absolute values on the various K_v to be compatible (so that the product formula will hold). By contrast, in Lecture 9 we considered various extensions L_w of a single local field K_v and wanted to normalize the absolute values on the L_w compatibly so that we could work in K_v and any of its extensions (all the way up to $\overline{K}_v$) using the same absolute value. These two objectives cannot be met simultaneously and it is better to use the "right" normalization in each setting.

Remark 12.31. When v is a complex place the normalized absolute value $\|\ \|_v$ is **not** an absolute value, because it does not satisfy the triangle inequality. For example, if $K = \mathbb{Q}(i)$ and $v|\infty$ is the complex place of K then $\|1\|_v = 1$ but

$$\|1 + 1\|_v = \|\mathrm{N}_{\mathbb{C}/\mathbb{R}}(2)\| = 4 > 2 = \|1\|_v + \|1\|_v.$$

For a complex place v, the normalized absolute value $\|\ \|_v$ on $K_v \simeq \mathbb{C}$ is the square of the standard absolute value on $\mathbb{C}$ and does not satisfy the triangle inequality (this problem does not arise with nonarchimedean absolute values; every positive power of a nonarchimedean absolute value is also an absolute value). But $\|\ \|_v$ is multiplicative, and it is compatible with the topology on K_v in the sense that the open balls $B_{<r}(x) := \{y \in K_v : \|y - x\|_v < r\}$ are a basis for the topology on K_v; these are the properties that we care about for the product formula (and for the topology on the ring of adéles $\mathbb{A}_K$ that we will see later).

Theorem 12.32 (Product Formula). *Let L be a global field. For all $x \in L^\times$ we have*

$$\prod_{v \in M_L} \|x\|_v = 1,$$

where $\|\ \|_v$ denotes the normalized absolute value for each place $v \in M_L$.

Proof. The global field L is a finite separable extension of $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$.[3] Let p be a place of K. By Theorem 12.23, any basis for L as a K-vector space is also a basis for

$$L \otimes_K K_p \simeq \prod_{v|p} L_v.$$

Thus

$$\mathrm{N}_{L/K}(x) = \mathrm{N}_{(L \otimes_K K_p)/K_p}(x) = \prod_{v|p} \mathrm{N}_{L_v/K_p}(x).$$

Taking normalized absolute values on both sides,

$$\left\|\mathrm{N}_{L/K}(x)\right\|_p = \prod_{v|p} \|\mathrm{N}_{L_v/K_p}(x)\|_p = \prod_{v|p} \|x\|_v.$$

We now take the product of both sides over all places $p \in M_K$:

$$\prod_{p \in M_K} \|\mathrm{N}_{L/K}(x)\|_p = \prod_{p \in M_K} \prod_{v|p} \|x\|_v = \prod_{v \in M_L} \|x\|_v.$$

The LHS is equal to 1, by the product formula for K (proved on the first problem set). □

References

[1] Joe Diestel and Angela Spalsbury, *The joys of Haar measure*, American Mathematical Society, 2014.

[2] Jürgen Neukirch, *Algebraic number theory*, Springer-Verlag, 1999.

[3] Jean-Pierre Serre, *Local fields*, Springer, 1979.

[3] Here we are using the fact that if $\mathbb{F}_q$ is the field of constants of L (the largest finite field in L), then L is a finite extension of $\mathbb{F}_q(z)$ and we can choose some $t \in \mathbb{F}_q(z) - \mathbb{F}_q$ so that $\mathbb{F}_q(z) \simeq \mathbb{F}_q(t)$ and $L/\mathbb{F}_q(t)$ is separable (such a t is called a *separating element*).