Local Langlands Conjectures

Abdullah Naeem Malik

Contents

In this report, we will expand the material covered in class, keeping the same notation, to global class field theory. This is needed in order to formulate at least the global version of the conjectures of Langlands. Our emphasis is on characteristic zero fields. Although this report strives for a general treatment but we nevertheless keep on shifting between number fields (finite field extensions of $\mathbb{Q}$)), global fields (which is includes a number field, a function field) or their completions (i.e., a local field) where appropriate, utilizing special properties where afforded for each scenario, to validate a general phenomenon under discussion.

The same symbols are used through-out to divulge the possibility of a unified treatment. To avoid confusion, the assumptions are spelled out.

This report, like the paper in [4], motivates and sets down the stage for developments in theory of local and global fields. Courtesy of the function field analogy, the general framework, therefore, serves as a link between number theory and geometry. Our starting point is quadratic reciprocity, after which we move on to L-functions ~~and formulate the local Langlands Conjecture based on the material covered~~.

Relevant local field theory, most of which is covered in class, is typed up in a separate appendix.

1 Introduction

Local Field Theory covered in class was all about classifying all finite abelian extensions of a given local field K but a similar treatment can be given for global fields, as well. Remarks can be made with function field analogy in this case, as well, to shed light on its algebraic nature. The ties with geometry are also natural, given that both local fields and global fields admit a nice topology which sits well with their respective algebraic structure. For example, in the case of number fields, the binary operation of multiplication and addition are continuous under the usual metric: the lazy and easy way to justify this is to consider the identity function on $\mathbb{Q}$. This is, of course, continuous and the sum and product of continuous functions is continuous. This addition and product of functions corresponds, respectively, to the binary operation of addition and multiplication in $\mathbb{Q}$. And now, we extend linearly to the number field K.

This tie of algebra with topology is not restricted to $\mathbb{Q}$. The general concept here is that of a **valuation**. A **non-Archimedean valuation** on K is a function $|-| : K \longrightarrow \mathbb{R}_{\geqslant 0}$ such that (a) $|ab| = |a|\,|b|$, (b) $|a| = 0$ if and only if $a = 0$, and (c) $|a + b| \leqslant \max\{|a|, |b|\}$. If (c) is replaced

by $|a+b| \leqslant |a| + |b|$, then the valuation is an **Archimedean valuation**. These give rise to either a metric or an ultra-metric and hence a topology on K. It is with respect to these metrics that K is (Cauchy) completed. Two valuations $|.|_1$ and $|.|_2$ are called **equivalent** if $\exists \lambda \geqslant 1$ such that $|.|_1 = |.|_2^{\lambda}$. This is an equivalence relation.

Proof. For $\lambda = 1$, $|.|_1$ is related to itself. If $|.|_1 = |.|_2^{\lambda}$, then $|.|_1^{\sqrt{\lambda}} = |.|_2$ and because $\lambda \geqslant 1$, we must have $\sqrt{\lambda} \geqslant 1$ and so, we have symmetry. To show transitivity, let $|.|_1 = |.|_2^{\lambda_1}$ and $|.|_2 = |.|_3^{\lambda_2}$. Then, $\lambda_1, \lambda_2 \geqslant 1$ implies $\lambda = \lambda_1\lambda_2 \geqslant 1$ and so, $|.|_1 = |.|_2^{\lambda_1} = \left(|.|_3^{\lambda_2}\right)^{\lambda_1} = |.|_3^{\lambda_2\lambda_1} = |.|_3^{\lambda}$. ■

Each such class is called a **place**. Of course no Archimedean valuation is equivalent to a non-Archimedean valuation.

So, for example, we have seen (in class) valuations for each prime p on the field $K = \mathbb{Q}_p$ and the field K given by a finite extension of $\mathbb{Q}_p$. The p-adic valuation on $\mathbb{Q}$ is defined similarly. No two valuations on $\mathbb{Q}$ are equivalent to one another, for if there were two such norms, then we would have the blatant contradiction $p^{-m} = p^{-n\lambda}$ for distinct primes, unless $m = n$ and $\lambda = 1$. There can be more valuations on such fields. Borrowing from [3], for each $c \in (0,1)$, we can define the valuation on K as follows: for $a \in K$, $|a|_c = c^{-m}$ (and forcing $|0|_c = 0$) where $m = ord_{\mathfrak{p}}(a)$ is given by the unique factorization. Thus, in case $K = \mathbb{Q}$, we have the usual p-adic norm on $\mathbb{Q}$. If K is a finite degree extension of $\mathbb{Q}_p$, the exponent m is given by the exponent in the factorization $a = u\pi^m$. If $K = \mathbb{Q}_p$, then the exponent is given by the factorization $a = up^m$.

To show that (b) is satisfied, observe that $|ab|_c = |u_1\pi^{m_1}u_2\pi^{m_2}|_c = |u\pi^{m_1+m_2}|_c = c^{-(m_1+m_2)} = c^{-m_1}c^{-m_2} = |a|_c\,|b|_c$ where $u = u_1u_2 \in \mathcal{O}_K^{\times}$. To show that (c) is satisfied, we break the problem down into cases $m_1 \gtrless m_2$ given by the Trichotomy law. If $m_1 = m_2$, then $|a+b|_c = |(u_1+u_2)\,\pi^m| = c^m = \max\{c^m, c^m\}$. If $m_1 < m_2$, then let $m_1 + k = m_2$ and so

$$\begin{aligned} |a+b|_c &= \left|u_1\pi^{m_1} + u_2\pi^{m_1+k}\right|_c \\ &= \left|\pi^{m_1}\left(u_1 + u_2\pi^k\right)\right|_c = |\pi^{m_1}|_c\left|\left(u_1 + u_2\pi^k\right)\right|_c \\ &= c^{m_1}\left|\left(u_1 + u_2\pi^k\right)\right|_c < c^{m_1+k} = \max\left\{c^{m_1}, c^{m_1+k}\right\} \end{aligned}$$

For any c, $d \in (0,1)$, the valuations $|.|_c$ and $|.|_d$ are patently equivalent.

If $K = \mathbb{Q}_p$ or a finite extension thereof, the completion for it is itself. Number fields K admit a non-trivial completion, depending on the valuation chosen. The only way one can levy the Archimedean norm to K is by successfully embedding it in either $\mathbb{R}$ or $\mathbb{C}$. If there are r_1 ways to embed K in $\mathbb{R}$ and r_2 ways to embed K into $\mathbb{C}$, then there are $r_1 + r_2$ ways to come up with an Archimedean norm on K. This makes sense once we understand the following:

Proposition 1 *Let $K/\mathbb{Q}$ be a finite extension with $n = [K:\mathbb{Q}]$. Then, the number of places v of K which restrict to u does not exceed n.*

An easy proof of this fact may be found in the student summer paper found in [5]. In fact, **Proposition 1** pins down all valuations we know on a local or global field K:

Theorem 2 (Ostrowski) *Every nontrivial absolute value on K is either p-adic for a given prime p or an Archimedean absolute value associated to a real or complex-conjugate pair of embeddings.*

Local fields are locally compact under topology generated by their metric. Global fields, on the other hand, are not locally compact. The easiest example of such an object is $K/\mathbb{Q}$, which may happen to be a finite, abelian extension. That is, $\mathrm{Gal}(K/\mathbb{Q})$ is an abelian group. That makes K Galois, a number field and hence a global field since K is incomplete (the completion of $\mathbb{Q}$ is the

infinite field extension $\mathbb{R}$). This shortcoming is one reason why there are two different versions (viz. local and global) of the Langlands conjectures.

Regardless of this shortcoming, the goal of class field theory to classify all abelian extensions can be masterfully accomplished via Artin's quadratic reciprocity law in a unified manner. To get to that point, and ultimately to the Langlands Conjectures, our journey has to start with Fermat.

2 Quadratic Reciprocity

As hinted above, one of the driving factors for the Langlands Program is the idea of quadratic reciprocity. Among others statements, a modern formulation of the quadratic reciprocity is that for distinct odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

where for $0 \neq a, n \in \mathbb{Z}$, we say that $\left(\frac{a}{n}\right) = 1$ if there exists x such that $x^2 \equiv a \pmod{n}$, and $\left(\frac{a}{n}\right) = -1$ otherwise. This statement was hypothesised by Leonhard Euler (1707 – 1783) and augmented by Adrien-Marie Legendre (1752 – 1833) with the introduction of the Legendre symbol $\left(\frac{\cdot}{\cdot}\right)$, and proved by Carl Gauss (1777 – 1855). Such an x is called a **quadratic residue** of n. Numerous instances of Quadratic Reciprocity Formula were known before Euler. For example, an equivalent statement is that for an odd prime p, the congruence $x^2 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{4}$. This version is today known as Fermat's Theorem. Note that Pierre de Fermat (1607 – 1665) proposed the following equivalent statement: p can be written as a sum of squares if and only if $p \equiv 1 \pmod{4}$.

Such problems of number theory admit an easy translation in terms of Modern Algebra. We go through a particularly enlightening enterprise covered in Section V.6 of [1] by setting up the machinery of a valuation norm $N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_{\geqslant 0}$ defined for Gaussian integers $\mathbb{Z}[i]$ via $N(a+ib) = (a+ib)(a-ib) = a^2+b^2$. This turns $\mathbb{Z}[i]$ into a Euclidean Domain and thus a unique factorization domain (UFD), allowing us the luxury of primes in $\mathbb{Z}[i]$. Call (usual) prime p split in $\mathbb{Z}[i]$ if it is not a prime in $\mathbb{Z}[i]$. That is, if the ideal $p\mathbb{Z}[i] = (p)$ in $\mathbb{Z}[i]$ is not prime. Recall that an element p in a ring R is called prime if the principal ideal (p) generated by p is a prime ideal of R, where ideal (p) is called prime if $R/(p)$ is an integral domain (equivalently, if $ab \in (p)$ implies $a \in (p)$ or $b \in (p)$).

Proposition 3 *A prime $p \in \mathbb{Z}$ is splits $\mathbb{Z}[i]$ if and only if p is the sum of two squares*

Proof. ($\Longrightarrow$) If $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, then $p = N(a \pm ib) \neq 1$. Moreover, p is not a unit since the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. This is because if u is a unit, then for some $v \in \mathbb{Z}[i]$ with $uv = vu = 1$, we must have $N(uv) = N(1) = N(u)N(v) = 1$ so $N(u)$ is a unit in $\mathbb{Z}$. That is, $N(u) = 1$. The only such u are ± 1 and $\pm i$. Neither of the factors $p = a^2 + b^2 = (a+ib)(a-ib)$ are, therefore, units. Thus, for $p \in (p)$, both $a+ib$ and $a-ib \in (p)$ and so, (p) is not prime.

($\Longleftarrow$) Assume (p) is not a prime ideal of $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a UFD, we may then assume that p is not an irreducible element of $\mathbb{Z}[i]$. Thus, we are allowed to assume that existence of an irreducible factor $q = a + ib$ of p with $(p) \neq (q)$ so let $p = qc$. This tells us that $p^2 = N(p) = N(q)N(c)$. This is an equation of natural numbers and, therefore, by primality of p, either $N(c) = p$ or $N(c) = 1$. The latter cannot happen since $N(c) = 1$ tells us that c is a unit and so $(q) = (p)$. Thus, $N(c) = p = N(q) = a^2 + b^2$. ■

Proposition 4 *A (usual) prime $p \in \mathbb{Z}$ splits in $\mathbb{Z}[i]$ if and only if $\left(\frac{-1}{p}\right) = 1$*

Proof. $p \in \mathbb{Z}$ is not a prime in $\mathbb{Z}[i] \iff \mathbb{Z}[i]/(p)$ is not an integral domain. Observe that $\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}[X]/(X^2+1)}{(p)} \cong \frac{\mathbb{Z}[X]}{(p,X^2+1)} \cong \frac{\mathbb{Z}[X]}{(p,X^2+1)} \cong \frac{\mathbb{Z}[X]/(p)}{(X^2+1)} \cong \frac{\mathbb{Z}/p\mathbb{Z}[X]}{(X^2+1)}$. Thus, $p \in \mathbb{Z}$ is not a prime in $\mathbb{Z}[i] \iff \frac{\mathbb{Z}/p\mathbb{Z}[X]}{(X^2+1)}$ is not an integral domain $\iff X^2+1$ has a root in $\mathbb{Z}/p\mathbb{Z} \iff \left(\frac{-1}{p}\right) = 1$ ■

In fact, the above is also equivalent to $p \equiv 1 \pmod 4$ (cf. Theorem V.6.11 of [1]. That is, Fermat's Theorem.

2.1 Modern Developments

To move forward with a further generalization of the above trend, David Hilbert focused on finite algebraic extensions of $\mathbb{Q}$. The treatment of this subject, as covered in [4], is for both local and global fields K.

Hilbert's emphasis laid on writing out quadratic reciprocity law in terms of ideals themselves. To this end, we must at least require ideals to be written as product of prime ideals with positive and negative exponents, corresponding to the intuition in fundamental theorem of arithmetic or fundamental theorem of finite abelian groups. Let us talk about how ideals can be broken down into their constituents. Material for this is taken from [2] where more information may be found.

To begin with, there is a notion of divisibility of ideals in a ring: let I_1, I_2 be ideals. We say that $I_1 \mid I_2$ if there exists another ideal I_3 such that $I_2 = I_1 I_3$, where the product of ideals is defined in the usual manner via ideal generated by finite sums of elements of the form $i_1 i_3$. This also allows us to define positive powers of an ideal. To be able to talk about "irreducible ideals", we would need to define a "unit ideal". Let us weaken the requirement for now and make use of already existing definition of a prime ideal.

Recall that an equivalent way to define a prime element $p \in R$ is by requiring $p \mid ab \implies p \mid a$ or $p \mid b$, where, for $r_1, r_2 \in R$, we say that $r_1 \mid r_2$ holds if there exists $c \in R$ such that $r_1 = r_2 c$. One way to reconcile this divisibility notion with the notion of a prime ideal is by observing that $I_1 \mid I_2$ implies $I_2 \subset I_1$. In fact, we have the following:

Proposition 5 *$\mathfrak{p}$ is a prime ideal of a commutative ring R if and only if for all ideals I, J, $\mathfrak{p} \supset IJ \implies \mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$*

Proof. ($\implies$) Let $\mathfrak{p} \supset IJ$. Because of symmetry of the situation, without loss of generality, we can assume that $\mathfrak{p} \not\supset I$. Then, we are allowed to pick $x \in I \backslash \mathfrak{p}$. For every $y \in J$, $xy \in IJ \subset \mathfrak{p}$ but since $\mathfrak{p}$ is prime, either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. The former is not true by assumption and hence $y \in \mathfrak{p}$. Since y was arbitrary, we have that $\mathfrak{p} \supset J$.

($\impliedby$) Let $\mathfrak{p}$ be a fixed ideal such that for all ideals I, J, $\mathfrak{p} \supset IJ \implies \mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$. In particular, consider the principle ideals $I = (x)$ and $J = (y)$ for arbitrary $x, y \in R$. If $xy \in \mathfrak{p}$, then $\mathfrak{p} \supset (x)(y) = IJ$ and so $\mathfrak{p} \supset I = (x)$ or $\mathfrak{p} \supset J = (y)$. That is, either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. ■

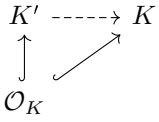
Thus, if for a prime ideal $\mathfrak{p}$, $\mathfrak{p} \supset \mathfrak{p}_1 ... \mathfrak{p}_n$, we have, by **Proposition 5**, $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. Thus, prime ideals can be viewed analogues of prime elements. However, the story doesn't end here, since we need to talk about negative exponents of prime ideals:

Definition 6 *Let R be a commutative integral domain and K be its field of fractions. The **fractional ideal** $\mathfrak{U}$ of R is an R-submodule $\mathfrak{U}$ of K such that $d\mathfrak{U} \subset R$ for some $d \in R \backslash \{0\}$.*

Observe that $d\mathfrak{U} \subset R$ is an ideal of R and that the exclusion of 0 ensures we do not have $\mathfrak{U} = \{0\}$. Note that the equivalent condition $\mathfrak{U} \subset d^{-1}R$ essentially creates an ideal of the form $\left(d^{-1}\right)$. This d is called the **common denominator**.

If K is either a local or global field with valuation $|-|_K$, the field of fractions of $\mathcal{O}_K$ is K itself.

Proof. Let K' be the field of fractions of $\mathcal{O}_K$. By its universal property, we have the map $K' \longrightarrow K$, an injection because K' is a field and the ideal $\ker(K' \longrightarrow K)$ is trivial



So we have a copy of K' inside K. To show the other side of the inclusion $K' \subset K$, let $x \in K$. If $|x|_K \leqslant 1$, then $x \in \mathcal{O}_K$ and hence $x \in K'$ by construction of K'. If $|x|_K > 1$ then $\left|x^{-1}\right|_K < 1$ and so $x^{-1} \in \mathcal{O}_K$ and hence $x^{-1} \in K'$. But since K' is a field, $\left(x^{-1}\right)^{-1} = x \in K$ ■

Thus, the fractional ideal $\mathfrak{U}$ of $\mathcal{O}_K$ is an $\mathcal{O}_K$-submodule of K such that $d\mathfrak{U} \subset \mathcal{O}_K$ for some $d \in \mathcal{O}_K \backslash \{0\}$ *. For every such $\mathfrak{U}$, there exists another fractional ideal $\mathfrak{V}$ such that $\mathfrak{UV} = \mathcal{O}_K$ and this is the inverse of $\mathfrak{U}$.

Proof. Let $\mathfrak{V} = \{x \in K : x\mathfrak{U} \subset \mathcal{O}_K\}$. We first show that $\mathfrak{V}$ is a fractional ideal by first showing that $\mathfrak{V}$ is a $\mathcal{O}_K$-submodule of K. $\mathfrak{V}$ is non-empty since $0 \in \mathfrak{V}$ (since $0 \in \mathcal{O}_K$ and $0\mathfrak{U} \subset \mathcal{O}_K$) and $d \in \mathfrak{V}$. For any scalar $\alpha \in \mathcal{O}_K$ and $x \in \mathfrak{V}$, we have $\alpha x\mathfrak{U} = x(\alpha\mathfrak{U}) \subset x\mathfrak{U} \subset \mathcal{O}_K$, where the first inclusion follows since $\mathfrak{U}$ is an $\mathcal{O}_K$-module and the second follows by definition of $\mathfrak{V}$. Thus, $\alpha x \in \mathfrak{V}$ and we have for ourselves an $\mathcal{O}_K$-submodule.

Now, let $x \in \mathfrak{U} \backslash \{0\}$. Then $x\mathfrak{U} \subset \mathcal{O}_K$ and so $x \in \mathfrak{V}$. Since $\mathfrak{V}$ is an $\mathcal{O}_K$-submodule, $x\mathfrak{V} \subset \mathcal{O}_K$. Thus, $\mathfrak{V}$ is a fractional ideal.

For last part, we will show a stronger result. Assume that for some ideal I, we have $\mathfrak{U}I = \mathcal{O}_K$. We will show that $I = \mathfrak{V}$. Let $x \in I$. Then, $x\mathfrak{U} \subset I\mathfrak{U} = \mathfrak{U}I = \mathcal{O}_K$ and so $x \in \mathfrak{V}$. That is, $I \subset \mathfrak{V}$.

Instead of reaching out for the other inclusion, let us observe that $x \in \mathfrak{V}$ justifies the inclusion $x\mathfrak{U} \subset \mathcal{O}_K$ by definition of $\mathfrak{V}$. Since x was arbitrary, therefore $\mathfrak{VU} = \mathfrak{VU} \subset \mathcal{O}_K$. Now observe that $I \subset \mathfrak{V} \implies I\mathfrak{U} \subset \mathfrak{UV} \implies \mathcal{O}_K \subset \mathfrak{UV} \implies \mathcal{O}_K = \mathfrak{UV} = \mathfrak{VU}$.

Hence $I = I\mathcal{O}_K = I\mathfrak{UV} = \mathcal{O}_K\mathfrak{V} = \mathfrak{V}$. ■

We are now able to at least state that any fractional ideal of an arbitrary ring R can be factored uniquely into products of exponents of prime ideals, from which it follows that every principal ideal (x) of $\mathcal{O}_K$ can be factored as prime ideals with positive and negative exponents. We skip a proof for the general case since, for now, we are only concerned with local and global number fields and we know how these behave.

In the context of local fields, since $\mathcal{O}_K$ is a principal ideal domain, every prime ideal is maximal. Since $\mathfrak{p}$ is maximal, we must have $\mathfrak{p} = \mathfrak{p}_i$. In the context of local number fields, recall that every ideal in $\mathcal{O}_K$ is principal. In fact, for a finite $K/\mathbb{Q}_p$, every ideal of $\mathcal{O}_K$ is of the form (π^m). Then the inverse of (π^m) can be constructed as follows: $(\pi^m)^{-1} = \{x \in K : x(\pi^m) \subset \mathcal{O}_K\} = \{x \in K : x \in (\pi^{-m})\mathcal{O}_K\} = (\pi^{-m})\mathcal{O}_K = (\pi^{-m})$. Moreover, since $\mathfrak{p} = (\pi) \subset \mathcal{O}_K$, we have $(1) = \mathcal{O}_K \subset (\pi)^{-1} = \left(\pi^{-1}\right)$. Thus, every ideal of $\mathcal{O}_K$ can be written out as an exponent of a prime ideal. In particular, the valuation of an element can be defined in terms of the exponent m as a power of a prime. For example, let $a \in K$. Then, $a = u\pi^m$ for some $u \in \mathcal{O}_K$, $\pi = p^{1/e}$ and $|a|_K = p^{-m/e}$, where e is the ramification index of K over $\mathbb{Q}$.

If (x) is any principal ideal of a ring $\mathcal{O}_K$ and if $(x) = \mathfrak{p}_1^{m_1} ... \mathfrak{p}_n^{m_n}$ where $\mathfrak{p}_i$ is prime, then we can define $|x|_{\mathfrak{p}_i} = (N\mathfrak{p})^{-m_i}$ where $N\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}_i|$which is an instance of a much more general **ideal norm**. This is a p-adic valuation.For $K/\mathbb{Q}_p$, this is easy to see since we have $N\mathfrak{p} = p^f$ where f is the inertia degree and for any $x \in \mathcal{O}_K$, we have $(x) = (\pi)^m = \mathfrak{p}^m = \{x \in K : |x|_K < 1\}^m$. The general notation for the exponent is also $ord_{\mathfrak{p}_i}(x)$. In case we have a finite extension $K/\mathbb{Q}$, we

*There is a typo in Gelbart's paper. The author assumes that the common denominator d is in the field of fractions. See page 26 of [4], first paragraph

know that $\mathcal{O}_K = \mathbb{Z}$ and that $(x) = \mathfrak{p}_1^{m_1}...\mathfrak{p}_n^{m_n}$ by the fundamental theorem of arithmetic, giving us $|x|_v = |x|_{\mathfrak{p}_i} = p_i^{-m_i}$ where $\mathfrak{p}_i = (p_i)$.

Let K_v denote the metric completion of K with respect to metric given by $|x-y|_v = |x-y|_{\mathfrak{p}_i} = d_i(x,y)$. Note that this is required for the case $K/\mathbb{Q}$. Hilbert's generalised quadratic reciprocity goes as follows: if $a, b \in K_i$, then $\left(\frac{a,b}{\mathfrak{p}_i}\right) = 1$ if $ax^2 + by^2 = 1$ admits a solution $x, y \in K_i$ and -1 otherwise. It can be shown that

$$\prod_{i=1}^{n} \left(\frac{a,b}{\mathfrak{p}_i}\right) = 1$$

Moreover, it can be shown that for $K = \mathbb{Q}$, the above reduces to

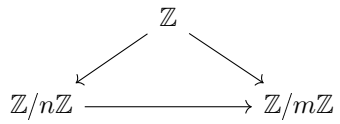
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{p,q}{2}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

2.2 Artin's Quadratic Reciprocity

Let us now move to Artin's treatment of the subject in 1927. A particular set up was discussed in class in the beginning lectures but we will delve into a little generality, beginning with norms on field extensions.

Let K/F be any finite field extension and let $\alpha \in K$. We can define a norm $N_{K/F}$ on K as $N(\alpha) = \det \lambda_\alpha$ where $\lambda_\alpha : K \longrightarrow K$ is an F-linear homomorphism given by $\lambda_\alpha(x) = \alpha x$. This map is clearly multiplicative since $\lambda_\alpha \lambda_\beta = \lambda_{\alpha\beta}$ and because the determinant is multiplicative. This can be further generalized in terms of ideles class groups, denote by C_K, which are defined using a particular quotient of ideles of course, which in turn are defined using ring of adeles, which in turn are defined using formal Archimedean completions of a number field K and an inverse limit. We discuss each component separately.

The **profinite completion** $\widehat{G}$ of a group G is defined via an inverse limit involving normal subgroups N of G such that $[G:N] < \infty$. We can order subgroups by inclusion $N_1 \subset N_2 \subset ...$ and this gives rise to natural homomorphisms $G/N_i \longrightarrow G/N_j$ if $N_i \subset N_j$. Then, $\widehat{G} = \varprojlim_i G/N_i$. For $G = \mathbb{Z}$, each normal subgroup $N_n = n\mathbb{Z}$ is of finite index. The natural homomorphism $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ exists when $m \mid n$ making the following diagram commute



Proof. The commutativity of the diagram will be clear once we prove that the function $[x]_n \longmapsto [x]_m$ is well-defined. Since $m \mid n$, we are guaranteed the existence of an element $k \in \mathbb{Z}$ such that $n = km$ and so, if $x \equiv y \mathrm{mod} n \iff x - y = nk'$ for some $j \in \mathbb{Z}$ implies $x - y = (km)k' = k''m$ where $k'' = kk' \iff x \equiv y \mathrm{mod} m$. ■.

The integral adeles $\mathbb{A}_{\mathcal{O}}$, for a global field K, is defined as the product of profinite completion $\widehat{\mathcal{O}}_K$ of its ring of integers $\mathcal{O}_K$ with a product of all Archimedean completions K_v for each place v. This product may be restricted. More formally, let P be the set of places of K and $S \subset P$ be subset of Archimedean places and

$$\mathbb{A}_{\mathcal{O}} := \widehat{\mathcal{O}}_K \times \prod_{v \in S} K_v$$

where $K_v \cong \mathbb{C}$ or $\mathbb{R}$ by Ostrowski's Theorem. The ring of adeles $\mathbb{A}_K$ is defined as

$$\mathbb{A}_K := K \otimes_{\mathcal{O}_K} \mathbb{A}_{\mathcal{O}}$$

and so actually embeds K into a Cartesian product of its Archimedean completions. The idele $\mathbb{I}_K$ of K is defined as the units of $\mathbb{A}_K$. That is, $\mathbb{I}_K = \mathbb{A}_K^{\times}$.

Thus, for $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$ and since there is only one Archimedean completion of $\mathbb{Q}$ viz. $\mathbb{R}$, the integral adeles $\mathbb{A}_{\mathbb{Z}} = \mathbb{R} \times \widehat{\mathbb{Z}}$ and $\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_{\mathbb{Z}}$ whereas $\mathbb{I}_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}^{\times}$. The quotient $\mathbb{I}_K / K^{\times} = C_K$ is called the idele class group of K[6].

Now, for a finite extension K_w/F_v, where K_w (resp. F_v) is the completion of K with place w (resp., completion of F with place v) and norm $N_{K_w/F_v} : K_w \longrightarrow F_v$ given by $N_{K_w/F_v}(\alpha) = \det \lambda_\alpha$, we define the idele norm $N_{K/F} : \mathbb{I}_K \longrightarrow \mathbb{I}_F$ by

$$N_{K/F}(\alpha) = \prod_{w|v} N_{K_w/F_v}(\alpha)$$

which induces a quotient norm $\widehat{N}_{K/F} : C_L \longrightarrow C_F$. For places w and v, the notation $w|v$ means that $|x|_v = |x|_w$ for all $x \in F$. This ties back to Proposition 3 and is the generalization of the norm map in §2 of **Appendix B** (cf. p. 29 of [4]).

Artin proved[†] that for every abelian extension K/F, there is a surjective homomorphism $C_F \longrightarrow Gal(K/F)$ with kernel $\widehat{N}_{K/F}(C_L)$. How this ties up with quadratic reciprocity is the subject of the next section but for now, we mention, without proof, that the existence of this homomorphism proves Kronecker-Weber Theorem. That is, it shows that every finite, abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\varsigma_n)$ for some n-th primite root of unity ς_n.

3 Enter L-functions

How does this tie up with quadratic reciprocity? The answer lies in particular functions called L-functions, associated with idele class characters C_K for a field K of characteristic 0. Observe the analogies with just the preceding topic as we go through its details.

Like Fermat's Theorem and Euler's proposal, these functions have their roots in proposals by the giants viz. Euler again with his proof of

$$\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6,$$

Bernhard Riemann (1826 – 1866) with his zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

and by Dirichlet (1805 – 1859) with his series

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

[†]Detailed proof may be found in Lecture 25 of [7].

with both defined for $\mathcal{R}e(s) > 1$ and $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ is function that (a) has periodicity k (that is, $\chi(a) = \chi(b)$ if $a \equiv b \pmod{k}$ (b) $\chi(n) = 0$ for n not coprime to k and 1 otherwise, and (c) is completely multiplicative for all integers. Riemann was interested in studying prime-counting function and, similarly, Dirichlet was interested in proving that there were infinitely many primes in any arithmetic sequence $a_n = a + nd$ for coprime a and d. Hecke's L-functions subsumed all cases:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

but let us step aside analytic considerations and focus on field theoretic ones. In order to be able to define L-functions for a number field, we need a few definitions first.

Definition 7 *Let K be a field of characteristic 0. A **character** of K with respect of v is a homomorphism $\chi_v : K_v^{\times} \longrightarrow \mathbb{C}^{\times}$. A character is **unitary** is a homomorphism $\chi_v : K_v^{\times} \longrightarrow \mathbb{S}^1$, **unramified** if $\mathcal{O}_{K_v}^{\times} = \{1\}$ and ramified otherwise. A **Hecke character** is a homomorphism $\chi : C_K \longrightarrow \mathbb{C}^{\times}$ given by the product of a family of characters χ_v*

$$\chi(x) = \prod_v \chi_v(x_v)$$

where the places v of K vary over all but finite unramified characters subject to $\chi(x) = 1$ for $x \in K^{\times}$

So, for example, if $K_v = \mathbb{R}$, barring the trivial homomorphism, one unitary character is given by $\chi_v : \mathbb{R}^{\times} \longrightarrow \mathbb{S}^1$ given by $\chi_v(x) = \frac{x}{|x|_v}$. We can define a similar character if $K_v = K$ is any finite degree extension of $\mathbb{Q}_p$. Then $\mathcal{O}_{K_v}^{\times} = \mathcal{O}_K \backslash \mathfrak{p}$ so there might not be unramified characters of K with respect to v. Observe the similarity with unramified extensions K over $\mathbb{Q}_p$, which is reflected in the choice of the terminology. If $K_v = \mathbb{C}$, then $\mathcal{O}_{K_v}^{\times} = S^1$ so, again, no character is unramified but there are uncountably many (continuous) characters $\chi_v\left(re^{i\theta}\right) = r^c e^{ci\theta}$ for each $c \in (0, 1)$ and unitary ones $\chi_v\left(re^{i\theta}\right) = e^{ci\theta}$.

For now, we record the following, to be used later once we invoke ideles: let $x \in K_v^{\times}$. Then, we can write $x = |x|_v \frac{x}{|x|_v}$ to place $\frac{x}{|x|_v} \in \mathcal{O}_{K_v}^{\times}$ and so $K_v^{\times} \cong O_{K_v}^{\times} \times |K^{\times}|_v$. In the unramified case, this takes a special place.

Recall that we stated, without proof, that for any finite extension K, for any principal ideal (x) of $\mathcal{O}_K$ we have $(x) = \mathfrak{p}_1^{m_1} ... \mathfrak{p}_n^{m_n}$ where $\mathfrak{p}_i$'s are prime and $m_1 \in \mathbb{Z}$. For $N\mathfrak{p}_i = |\mathcal{O}_K/\mathfrak{p}_i|$, we define the uniformizing parameter by $N\mathfrak{p}_i^{-1}$. In this case, $\chi(\mathfrak{p}_i) := \chi_v(\overline{w}_v)$ where $\overline{w}_v \in K_v$ such that $|\overline{w}_v|_v = N\mathfrak{p}_i^{-1}$. Since any ideal of $\mathcal{O}_K$ can be written out as a product of prime ideals with integer exponents, we can then extend by linearity the above definition.

Thus, for an unramified local field with a degree extension of n and, therefore, of inertia degree $n = f$ over $\mathbb{Q}_p$, this is $N\mathfrak{p}_i^{-1} = \pi$, the generator for the unique maximal ideal $\mathfrak{p}$ (because $e = 1$).

We are now ready to define L-functions! Let $\mathfrak{p}_i$ be a prime ideal of $\mathcal{O}_K$. For a given character χ, **Hecke's L-function** is defined as

$$L(s, \chi) = \prod_i \frac{1}{1 - \frac{\chi(\mathfrak{p}_i)}{(N\mathfrak{p}_i)^s}}$$

where the product is over all prime ideals. Thus, for a local field in the unramified case would give us $L(s, \chi) = \frac{1}{1 - \chi(\mathfrak{p})}$.

Artin's definition of L-functions generalise Hecke's L-functions. From there, we would need to talk about how a representation is the generalization of a character but this would require the

understanding of how general linear groups are related to ideles. For $K_v^\times$, it is easy to see that $GL_1(K_v) = K_v^\times$ for an Archimedean place v. Artin's reciprocity stems from the existence of a special representation π_σ (called automorphic cuspidal reprsentation) based off of the representation $\sigma : Gal(K/F) \longrightarrow GL_1(\mathbb{C}) = \mathbb{C}^\times$. This is a special case for $n = 1$ of the following:

Conjecture 8 (Langlands) *Let K/F be finite Galois and $\sigma : Gal(K/F) \longrightarrow GL_n(\mathbb{C})$ be an irreducible representation of $Gal(K/F)$. Then, there exists an automorphic cuspidal representation π_σ on GL_n over F such that $L(s, \pi_\sigma) = L(s, \sigma)$.*

References

[1] P. Aluffi. *Algebra: Chapter 0*, volume 104. American Mathematical Soc., 2009.

[2] K. Conrad. Ideal factorization. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf`.

[3] K. Conrad. Ostrowski for number fields. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf`.

[4] S. S. Gelbart. Class field theory, the Langlands program, and its application to number theory. In L. Ji, K. Liu, S.-T. Yau, and Z.-J. Zheng, editors, *Automorphic Forms and the Langlands Program*, volume 9 of *Advance Lectures on Mathematics*, chapter 2, pages 21–67. International Press, China, 2010.

[5] M. J. Lieberman. Hecke L-functions on Algebraic Number Fields, Summer 2002. `http://www-users.math.umn.edu/~garrett/students/reu/lieberman`.

[6] nLab authors. group of ideles. `http://ncatlab.org/nlab/show/group%20of%20ideles`, May 2020. Revision 14.

[7] A. Sutherland. Lecture Notes on 18.785 Number Theory I. `https://math.mit.edu/classes/18.785/2015fa/`, Fall 2015.

Appendix A

The following proof was given by Euler himself for

$$\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$$

It is included in the report because it was the first thing that sparked my curiosity when I was learning series expansions of functions.

Since $\sin x = x - x^3/3! + x^5/5! - x^7/7! + ...$ we have

$$\frac{\sin x}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + ...$$

Now, since roots of this polynomial occur at $\pm n\pi$ for $n \in \mathbb{N}$, Euler claimed that this allows us to factor this polynomial as follows:

$$\begin{aligned}\frac{\sin x}{x} &= \left(1-\frac{x}{\pi}\right)\left(1+\frac{x}{\pi}\right)\left(1-\frac{x}{2\pi}\right)\left(1+\frac{x}{2\pi}\right)... \\ &= \left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{(2\pi)^2}\right)\left(1-\frac{x^2}{(3\pi)^2}\right)...\end{aligned}$$

Now, we expand these out and compare coefficients with the series expansion of sin. The coefficient for x^0 is only 1. The coefficient for x^2 is

$$-\frac{1}{\pi^2}\left(\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^3}+...\right)$$

Comparing this with $-1/3!$, we have $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/3!$.