Euclid	300 BC
Diophantus	300 AD
Fermat	1601-1665
Euler	1707-1783
Lagrange	1736-1836
Legendre	1752-1833
Fourier	1768 - 1830
Cauchy	1789 - 1857
Abel	1802 - 1829
Jacobi	1804-1851
Dirichlet	1805 - 1859
Liouville	1809-1882
Kummer	1810 - 1893
Galois	1811 - 1832
Hermite	1822-1901
Eisenstein	1823 - 1859
Riemann	1826 - 1866
Dedekind	1831 - 1916
Weber	1842 - 1913
Hurwitz	1859 - 1919
Minkowski	1869-1909
Hilbert	1863 - 1943
Takagi	1875 - 1960
Hecke	1887 - 1947
Artin	1898 - 1962
Hasse	1898 - 1979

The history of number theory is the history of mathematics.

Where's Gauss? Gotta look it up.

Fermat looked at all sorts of things.

1. Quadratic equations. Here are some Fermatian assertions.

$$\begin{aligned} p = x^2 + y^2 &\iff p \equiv 1 \bmod 4 \\ p = x^2 + 2y^2 &\iff p \equiv 1 \text{ or } 3 \bmod 8 \\ p = x^2 + 3y^2 &\iff p = 3 \text{ or } p \equiv 1 \bmod 3 \end{aligned}$$

These are all binary quadratic forms.

2. Consider

$$x^3 + y^3 = z^3.$$

Or, for that matter,

$$x^4 + y^4 = z^2.$$

The question is, figure out if there are [integer] solutions. Nowadays, we'd call these elliptic curves. If you go to higher degree, you don't have an elliptic curve. But it turns out that Fermat usually just worried about curves of genus 1 or 2.

3.

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \zeta(s).$$

Euler had messed around with this, and found out [inter alia] that $\zeta(2) = \frac{\pi^2}{6}$. Euler also showed that $\zeta(2n) = \pi^{2n}\cdot$ rational, where the rational number is essentially a Bernoulli number. We have the Euler product,

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Back to binary quadratic forms. Euler conjectured several things, like $p = x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20$; and $2p = x^2 + 5y^2 \iff p \equiv 3, 7 \bmod 20$. There are similar things for $x^2 + 7y^2$, etc. So Euler up and asks whether p divides $x^2 + ny^2$ for suitable x and y not both divisible by p [nontrivially]. And he sets $\chi_p(n) = \begin{cases} 1 & p | x^2 - ny^2 \\ -1 & p \not| x^2 - ny^2 \end{cases}$. In other words, 1 or -1 depending on whether or not n is a quadratic residue mod p. We now can see that $n \mapsto \chi_p(n)$ is a character. Slightly more surprising is that $p \mapsto \chi_p(n)$ is a homomorphism as well, in that it only depends on $p \in (\mathbb{Z}/4n)^\times$.

Let's briefly treat with the other two themes.

27 January 1752 – Birthday of the theory of elliptic functions. Some dude named Fagnano wrote a book, sent it to the Berlin Academy, and Euler got stuck with reading it. In this two-volume book, Fagnano observes that

$$\frac{dx}{\sqrt{1 - x^4}} = \frac{dy}{\sqrt{1 - y^4}}$$

has a general solution which looks algebraic. So Euler starts replacing the denominator with an arbitrary quartic polynomial; and he can change dx to mdx, and dy to ndy.

Why can he do this? Well, for instance, $u^2 = 1 - x^4$ gives an elliptic curve. You wind up thinking about the product of two elliptic curves, $E \times E$. And the various sides of the equation give invariant forms on E. Call this thing ω. Then we're really asking for the zero locus of the holomorphic 1-form $p_1^*\omega - p_2^*\omega$ on $E \times E$. This thing is translation invariant. The diagonal gives the solution $x = y$. So the diagonal sits in as the solution; and any translate must work. So all translates work, and that's all the solutions.

After this, the theory of elliptic functions takes off. Moving right along....

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{-\infty}^{\infty}(-1)^n q^{\frac{n(3n+1)}{2}}.$$

Euler decided to prove the four-square theorem by considering this identity; he's using generating functions. For you wind up with

$$(\sum q^{n^2})^4 = \sum_{R(n)} q^n.$$

If you have $\sum_{-\infty}^{\infty} q^{n^2}$ and let $q = e^{\pi i \tau}$, you wind up with $\theta(\tau)$. One reason we can handle functions of this sort is that they are modular forms, which in turn are about elliptic curves.

On to the third theme, ζ and L-functions.

So Dirichlet's hanging out, worrying about arithmetic progressions, and primes mod m. He realizes that the write thing to do is consider functions of the sort $\sum_{(n,m)=1} \frac{\chi(n)}{n^s}$, where $\chi : (\mathrm{Z}/m\mathrm{Z})^\times \to \mathrm{C}^\times$. This is usually denoted $L(\chi, s)$. There are exactly $\phi(m)$ such L-functions. Anyways, $L(\chi, s) = \prod_{(p,m)=1} \frac{1}{1-\chi(p)p^{-s}}$.

If you take $\chi = \chi_0$ the trivial character, you get the ζ function except for some fudge factors for the primes dividing m.

It turns out that Gauss lived from 1777 to 1855.

Last time, we were sketching Dirichlet's theorem on primes in arithmetic progression. We define the L-function $L(\chi, s)$ where $\chi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}^*$ is a character. We set

$$L(\chi, s) = \sum_{(n,m)=1} \frac{\chi(n)}{n^2} = \prod_{p \not| m} (1 - \chi(p)p^{-s})^{-1}.$$

Each of the terms in the product is called an Euler factor; and here, it's said to be of degree one.[1] We know [by Abel summation] that the series is conditionally convergent when $\Re s > 1$ if χ is nontrivial; and it's absolutely convergent for $\Re s \geq 1$. Something about dealing with the spectrum of a number field of dimension one. The key step is that for every nontrivial χ, $L(\chi, 1) \neq 0$.

Taking logarithms, we have [assume $s \downarrow 1$]

$$\begin{aligned}
\log L(\chi, s) &= \sum_{(p,m)=1; n \geq 1} \frac{\chi(p^n)}{np^{ns}} \\
&= \sum_{(p,m)=1} \frac{\chi(p)}{p^s} + O(1) \\
\frac{1}{\phi(m)} \sum_{\chi} \chi(n_0^{-1}) \log L(\chi, s) &= \sum_p \frac{1}{\phi(m)} \sum_{\chi} \frac{\chi(pn_0^{-1})}{ps} + O(1).
\end{aligned}$$

At this point, we use the fact that if A is a finite group, then $\sum_{\chi \in \widehat{A}} \chi(a) = \sum_{\chi} \chi\chi_1(a) = (\sum_{\chi \in \widehat{A}} \chi(a))\chi_1(a)$ for all χ_1. So the thing is either one or zero depending on whether χ is or isn't trivial. We thus get

$$= \sum_{(p,m)=1; p \equiv n_0 \bmod m} \frac{1}{p^s} + O(1).$$

Uh-oh, I blinked. We just got a contradiction.$\diamond$

Moving along. Riemann had this paper in which he defined $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$. It was natural for him to consider this as a holomorphic function. This is absolutely convergent for $\Re s > 1$, and it's uniformly convergent on $\Re s > c > 1$. He derived a number of functional equations. For instance,

[1] And that's because we have an abelian representation of degree one.

$$\pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$$

is invariant under $s \leftrightarrow 1-s$. Of course, here

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt.$$

In the functional equation above, $\pi^{-s/2}\Gamma(s/2)$ is often denoted $\Gamma_{\mathbb{R}}(s)$. It becomes clear that this has a lot to do with the Jacobi theta function

$$\theta(z) = \sum_{-\infty}^{\infty} e^{\pi\sqrt{-s}n^2z}$$

where $\Im z > 0$. He showed that, more or less, there's a relation between $\theta(z)$ and $\theta(-\frac{1}{z})$. It's the frac linear transformation defined by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Riemann also studied the number of primes less than a given number. He related the zeros of $\zeta(s)$ to the distribution of primes. Here, we're studying $\pi(x) = \sum_{p\leq x} 1$. The prime number theorem says that

$$\pi(x) \sim \frac{x}{\log x}.$$

The prime number theorem says that there are no zeros on the critical line, $\Re s = 1$; and actually, there are no zeros in some small neighborhood [but this neighborhood isn't rectangular!]. This brings us to Riemann's hypothesis, which says that $Z = \zeta^{-1}(0) \subseteq \Re s = \frac{1}{2}$.

Define $\Lambda(n) = \begin{cases} \log p & n = p^e \\ 1 & \end{cases}$. Riemann's hypothesis is equivalent to the statement

$$\sum_{n\leq X} \Lambda(n) = X + O(X^{\frac{1}{2}}(\log X)^2).$$

The prime number theorem says that $\exists c > 0$ so that

$$\sum_{n\leq X} \Lambda(n) = X + O(Xe^{-c\sqrt{\log X}}).$$

And it turns out that the function field analogue of this is true.

Okay, so let's begin the course already. Consider $K = \mathbb{Q}(\sqrt{-5})$. Its ring of integers is $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Note that $O_K^\times = \{\pm 1\}$. Let $\alpha = 1 + 2\sqrt{-5}$, and $\alpha' = 1 - 2\sqrt{-5}$. And the norm is $\alpha\alpha' = 21 = 3 \cdot 7 = \beta \cdot \rho$. One can check that $\alpha, \alpha', \beta, \rho$ are all irreducible in O_K, but they are not associates of each other. Compute $\alpha^2 = -19 + 4\sqrt{-5}$ and $\beta^2 = 0$. Both are divisible by $\lambda = 2 + \sqrt{-5}$. So then $\alpha^2 = (2 + \sqrt{-5})(-2 + 3\sqrt{-5})$, and $\beta^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Thus, $\frac{\alpha^2}{\lambda}$ and $\frac{\beta^2}{\lambda}$ are both integral. Now, $\frac{\alpha}{\sqrt{\lambda}}$ isn't in K, but it's certainly integral [i.e., an algebraic integer]. Ditto for $\beta/\sqrt{\lambda}$. If you conjugate everything, you get $\alpha'^2 = (-2 + \sqrt{-5})(2 + 3\sqrt{-5})$, and $\rho^2 = (2 - 3\sqrt{-5})(2 + 3\sqrt{-5})$. Let $\chi = 2 + 3\sqrt{-5}$. Then $\alpha'/\sqrt{\chi}$ and $\rho/\sqrt{\chi}$ are integers. We now have

$$
\begin{aligned}
\alpha\alpha' &= \beta\rho \\
\sqrt{\lambda}\sqrt{-\chi}\sqrt{\lambda'}\sqrt{-\chi} &= \sqrt{\lambda}\sqrt{\lambda'}\sqrt{\chi}\sqrt{\chi}.
\end{aligned}
$$

This should start to explain the problem of nonunique factorization. Now, $\sqrt{\lambda} = \gcd(\alpha, \beta)$. We think of ideal numbers as adjoining the gcd's of numbers. This is the sort of thing Kummer did. Note the connection with $\alpha O_K + \beta O_K$.

Dedekind domains and discrete valuations This is going to be review; don't be surprised by the lack of proofs.

Definition A is a discrete valuation ring $\iff$, well, hold on. It's a valuation ring if there's a map $A - \{0\} \to \mathrm{N}$. As always, let K be the fraction field of A. Then this valuation extends to $v : K^\times \to \mathrm{Z}$. It has to satisfy a number of properties. In particular, we insist that

1. $v(xy) = v(x) + v(y)$.
2. $v(x+y) \geq \min(v(x), v(y))$.

You can get an absolute value from a valuation, as follows. Fix some $a > 1$, and set $\|x\| = a^{-v(x)}$. We get $\|x+y\| \leq \max(\|x\|, \|y\|)$. The units have valuation zero; $A^\times = v^{-1}(0)$.

Anyways, A is a discrete valuation ring $\iff$ A is a noetherian local ring with maximal ideal $\mathfrak{m}$ principal. π is a uniformizer if $v(\pi) = 1$; for all $x \in K^\times$, $x = \pi^{v(x)}u$ for $u \in A^\times$. The definition of DVR is equivalent to A is noetherian integrally closed (normal) of dimension ≤ 1.

Definition A is a Dedekind domain $\iff$ A is noetherian, normal of dim ≤ 1 $\iff$ for all prime ideal $\mathfrak{p} \neq (0)$, then the localization $A_\mathfrak{p}$ is a discrete valuation ring.

"Geometry is too easy." Shubin wants an example of a noetherian local ring with $\mathfrak{m}$ not principal. It's suggested that we look at $\mathrm{Z}[\sqrt{5}]$.

Proposition [Unique factorization of ideals] A fractional ideal is a nonzero finitely generated A-submodule of K. Every fractional ideal $J \subseteq K$ [nonzero] has a unique factorization

$$J = \prod_i \mathfrak{p}_i^{e_i}$$

where the $\mathfrak{p}_i$ are distinct primes.

Example

1. Let K be an algebraic number field, O_K the ring of integers of K; all elements of K integral over Z. This is a Dedekind domain.
2. $\mathrm{Z}_{(p)}$, Z_p.
3. k a field, C a smooth curve over k. Set $Z \subsetneq C$ closed and nonempty. Then $\Gamma(C - Z, O_C)$ is a Dedekind domain.

Approximation / Chinese remainder Let A be a Dedekind domain, $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ distinct non-zero primes, $a_1, \cdots, a_m \in A$, $n_1, \cdots, n_m \in \mathrm{N}$. Then there's an $x \in A$ so that $v_{\mathfrak{p}_i}(x - a_i) \geq n_i$ for all $i = 1, \cdots, m$. And once you've proven this, you see that you can replace A by K.

Extensions From now on, A a Dedekind domain, K its fraction field, L a finite extension of K. Let B be the integral closure of A in L. Assume B is a finite A-module.[2] We can look at $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$. The latter is finite over the former, since finitude is a local property. Then

1. B is a Dedekind domain.
2. $B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank $[L : K]$.

Definition Let $\mathfrak{P}$ lie over $\mathfrak{p}$, that is, $\mathfrak{P} \cap A = \mathfrak{p}$. Then $e_{\mathfrak{P}} = v_{\mathfrak{P}}(\pi_{\mathfrak{p}})$, where $\pi_{\mathfrak{p}}$ is a uniformizer downstairs. In other words, $\pi_{\mathfrak{p}} = \pi_{\mathfrak{P}}^{e_{\mathfrak{P}}} \cdot(\text{unit})$. This number $e_{\mathfrak{P}}$ is called the ramification index. Let $\kappa_{\mathfrak{P}}$ and $\kappa_{\mathfrak{p}}$ be the associated residue fields. There's a uniquely defined map between them, $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \to B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}}$. Anyways, $f_{\mathfrak{P}/\mathfrak{p}} = [\kappa_{\mathfrak{P}} : \kappa_{\mathfrak{p}}]$.

There's a map of the groups of fractional ideals, $\iota : I_A \to I_B$. It need only be defined on primes; and we say that $\mathfrak{p} \mapsto \prod_{\mathfrak{P}_i | \mathfrak{p}} \mathfrak{P}_i^{e_i} = \mathfrak{p}B$. We can also make one that goes backwards, $N_{L,K} : I_B \to I_A$. This one is given by $\mathfrak{P} \mapsto \mathfrak{p}^{f_{\mathfrak{P}}}$.

Let M be an A-module of finite length, i.e., M has a composition series $M = M_m \supseteq M_{m-1} \supseteq \cdots \supseteq M_1 \supseteq M_0 = (0)$, where $M_i/M_{i-1} \cong A/\mathfrak{p}_i$. We define a character by $\chi_A(M) = \prod_i \mathfrak{p}_i$. This is a sort of Euler characteristic. And it turns out that $\chi(\kappa_{\mathfrak{P}}) = N(\mathfrak{P})$.

One last thing. If you have an element $x \in B$, then $N(xB) = N_{L,K}(x)A$.

[2] Crucial assumption; see problem 14.

Let A be a Dedekind domain, K its field of fractions, L a finite extension of K. Let B be the integral closure of A in L. We make the assumption $(*)$ that B is a finite A-module.[3]

Lemma $(*)$ is satisfied when L is separable over K.

Proof $\mathrm{tr}_{L,k} : L \times L \to K$ is nondegenerate. We need to show that $\mathrm{tr}(B) \subseteq A$. So this tells us that $B \supseteq B^\vee$ with respect to trace. So this says that it's $\{y \in L : \mathrm{tr}(xy) \in A \forall x \in B\}$. And this is a finite A-module. Nondegeneracy was crucial in saying that $B^\vee$ is a finite A-module.$\diamond$

Definition If $\mathfrak{p} \subseteq A$, and $\mathfrak{P} \subseteq B$ lies over it,[4] last time we defined $e_\mathfrak{P}$ and $f_\mathfrak{P}$. B is unramified at $\mathfrak{P}$ if $e_\mathfrak{P} = 1$ *and* $\kappa_\mathfrak{P}/\kappa_\mathfrak{p}$ is separable.

Proposition $\sum e_i f_i = [L : K]$.

Proof We have B an A-module of finite type. And there's no torsion, so B is a free A-module of rank $n = [L : K]$. Consider $A/\mathfrak{p}$ and $B/\mathfrak{p}B$. The latter is still a free $A/\mathfrak{p} = \kappa_\mathfrak{p}$ module of rank n. Write $\mathfrak{p}B = \prod_i \mathfrak{P}^{e_i}$, and $\cap_i \mathfrak{P}_i^{e_i} = \mathfrak{p}B$. There's a map

$$B/\mathfrak{p}B \to \prod_i B/\mathfrak{P}_i^{e_i}.$$

The surjectivity follows immediately from the approximation theorem; an element on the right is represented by some finite number of elements, and we know we can pick an element from B to approximate arbitrarily well. So now we know that it's an isomorphism, and we win; for $\dim_{\kappa_\mathfrak{p}}(B/\mathfrak{P}_i^{e_i}) = \sum_{0 \le j \le e_i - 1} \dim_{\kappa_\mathfrak{p}} \mathfrak{P}^j/\mathfrak{P}^{j+1} = e_i f_i$, since the thing you're summing up is a copy of $\kappa_\mathfrak{P}$.

Examples

1. Unramified extensions. Assume we have an extension of local rings, $B_\mathfrak{P}$ over $A_\mathfrak{p}$. This gives an extension of residue fields, $\lambda_\mathfrak{P}$ over $\kappa_\mathfrak{p}$, of degree n. Assume that $B_\mathfrak{p} = B_\mathfrak{P}$

[3] Apparently life is hellish without this assumption.

[4]
$$\begin{array}{ccc} \mathfrak{P} & \subseteq & B \\ | & & | \\ \mathfrak{p} & \subseteq & A \end{array}$$

is local. Let $\overline{x} \in \lambda_{\mathfrak{P}}$ be a generator of λ/κ. Get $x \in B_{\mathfrak{p}}$, a lift of $\overline{x}$. Let $\overline{f}(T)$ be the minimal polynomial of $\overline{x}$ over κ, of degree n. Let $f(T)$ be the minimal polynomial of x over K. We want to show that $\overline{f(T)} = \overline{f}(T)$. And one can see that $\overline{f}(T)|\overline{f(T)}$. On the other hand, we know that $\deg f(T) \leq n$. Together, this implies the equality we were after.

By Nakayama's lemma, $B_{\mathfrak{P}} = A_{\mathfrak{p}}[x]$; since both sides are equal if reduced mod $\mathfrak{p}$, and thus must be the same.

Conversely, assuming that $\overline{f}(T)$ is an irreducible monic separable polynomial over κ, let $f(T) \in A_{\mathfrak{p}}[T]$ be a monic lifting of $\overline{f}(T)$. Then let x be a root of $f(T)$. Consider the ring $A[x] \subseteq K(x)$ its field of fractions, a finite extension of K. Furthermore, we know that $[K(x) : K] = \deg f = n$. Let B be the integral closure of A in $K(x)$. Clearly, we have $A[x] \subseteq B$; let's prove the other inclusion, and conclude that they're equal. Well, we certainly have

$$0 \to A[x] \to B \to (B/A[x]) \to 0.$$

Tensor with $A/\mathfrak{p}$, and get

$$\kappa[x] \to (B \otimes A/\mathfrak{p}) \to (B/A[x]) \otimes (A/\mathfrak{p}) \to 0.$$

One can see that the first arrow is an isomorphism, so the last thing is zero. By Nakayama's lemma, $B/A[x] = 0$.

Thus, we've seen that unramified extensions come from residue field extensions. Moreover, the ring of integers is generated by a single element.

2. Totally ramified extension. As before, we have $B_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$, everthing is local. $B_{\mathfrak{P}} = B_{\mathfrak{p}}$. Assume that $e = n$; the ramification index is equal to the degree. Take a uniformizer $\pi \in B_{\mathfrak{P}}$. Look at $f(T)$, the minimal polynomial of π. Its degree is n, we hope. Consider $1, \pi, \pi^2, \cdots, \pi^{n-1}$. Look at the A-submodule generated by 'em. We can't have any nontrivial relation among them; look at $A + A\pi + A\pi^2 + \cdots A\pi^{n-1} \subseteq B$. All of them have different valuations mod$n$, so they can't all cancel out. Claim that $A_{\mathfrak{p}}[\pi] = B_{\mathfrak{p}}$ (the maximal ideal is principal). Furthermore, $f(T) = T^n a_{n-1} T^{N-1} + \cdots + a_1 T + a_0$. We know that $f(\pi) = 0 = \pi^n + a_{n-1}\pi^{n-1} + \cdots + a_1\pi + a_0$ with $a_i \in A$. Now, look at all the terms a_i in the middle. All of their valuations are different mod$n$. The ones on the end have valuations $\equiv 0 \bmod n$. So in order to have some sort of linear relation, π^n and a_0 must have the same valuation; $v_B(\pi^n) = v_B(a) = n$. Therefore, $v_A(a_0) = 1$. So a_0 is a uniformizer in A. And all the other $a_i \in \mathfrak{m}_A$. We call $f(T)$ an Eisenstein polynomial. In contrast to the unramified case, a totally ramified extension has to come from an Eisenstein polynomial.

Conversely, let $f(T)$ be an Eisenstein polynomial. By the usual Eisenstein criterion, f is irreducible. Consider $A[T]/(f(T))$. Claim that this is local. Well, any maximal ideal must lie over a maximal ideal downstairs. So tensor, and get

$$\begin{aligned} A[T]/(f(T)) \otimes (A/\mathfrak{m}_A) &= \kappa[T]/(\overline{f}(T)) \\ &= \kappa[T]/T^n. \end{aligned}$$

And in fact, we see that $A[T]/(f(T))$ is a discrete valuation ring. And $v(\overline{T}^n) = v(a_0)$.

As always, we have A a Dedekind domain, $K = \mathrm{Frac}(A)$, L/K a finite extension, and B the integral closure of A in L. Assume $(*)$ B is a finite A-module. We further assume that L/K is Galois, and let $G = \mathrm{Gal}(L, K)$. Fix $\mathfrak{p} \subseteq A$ prime, and $\mathfrak{P}_i$ lie over it. G takes B to itself, fixing A. G permutes the $\mathfrak{P}_i$ lying over $\mathfrak{p}$.

Proposition G operates transitively on $\{\mathfrak{P}_i\}$.

Proof Follows from approximation. Fix, say, $\mathfrak{P}_1$. Assume there's a $\mathfrak{P}_2$ so that $\sigma(\mathfrak{P}_1) \neq \mathfrak{P}_2$ for all $\sigma \in G$. We get [at least] two distinct orbits. Take $x \in \mathfrak{P}_1$ so that $x \notin \mathfrak{P}_i$ if $i \neq 1$. Then $N(x) \in A \cap \mathfrak{P}_1 = \mathfrak{p}$. But $N(x) = \prod_{\sigma \in G} \sigma(x) \notin \mathfrak{P}_2$, a contradiction.$\diamond$

We'll look at the decomposition group $D_{\mathfrak{P}} = \{\sigma \in G | \sigma(\mathfrak{P}) = \mathfrak{P}\}$. Inside this, there's the inertia group $I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} : \sigma|_{\mathfrak{P}} \equiv \mathrm{id}_{\mathfrak{P}}\}$. This is an automorphism of the residue field $\lambda_{\mathfrak{P}}$. There's an exact sequence,

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(\lambda_{\mathfrak{P}}, \kappa_{\mathfrak{p}}).$$

We have no idea if $\lambda_{\mathfrak{P}}/\kappa_{\mathfrak{p}}$ is separable. All we know is that it's a finite extension. Now, for every such finite extension, we know that there's a subextension $\kappa_{\mathfrak{p}} \subseteq \lambda^s_{\mathfrak{P}} \subseteq \lambda_{\mathfrak{P}}$, so that $\lambda^s_{\mathfrak{P}}$ is separable, and $\lambda_{\mathfrak{P}}/\lambda^s_{\mathfrak{P}}$ is purely inseparable. The degree of the inseparable extension is p to some power s, p^s. Let $f_s = [\lambda^s_{\mathfrak{P}} : \kappa_{\mathfrak{p}}]$; so $[\lambda_{\mathfrak{P}} : \kappa_{\mathfrak{p}}] = f = f_s p^s$.

$\lambda_{\mathfrak{P}}/\kappa_{\mathfrak{p}}$ is a *normal* extension. For all $\overline{x} \in \lambda_{\mathfrak{P}}$, let x be a lift of $\overline{x}$ to $B_{\mathfrak{P}}$. Let

$$f(T) = \prod_{\sigma \in G/\mathrm{stab}_x} (T - \sigma(x)) \in A[T].$$

Then $\overline{f}(T) \in \kappa[T]$ has $\overline{x}$ as a root.

Now, we want to claim that the sequence given above is surjective, i.e., we really have

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(\lambda_{\mathfrak{P}}, \kappa_{\mathfrak{p}}) \to 1.$$

But the proof is pretty much the same. Take $\overline{x}$ to be a generator of $\lambda^s_{\mathfrak{P}}$ over $\kappa_{\mathfrak{p}}$.

Uh-oh. It's diagram time.

$$\begin{array}{ccccc} \mathfrak{P}_i & \subseteq & B & \subseteq & L \\ | & & | & & | \\ \mathfrak{p} & \subseteq & A & \subseteq & K \end{array}$$

Suppose there are r ideals lying over $\mathfrak{p}$. Well, G acts transitively. So

$$\begin{aligned} efr = [L:K] &= \#(D_{\mathfrak{P}}) \cdot r \\ &= \#(I_{\mathfrak{P}}) \cdot r \cdot f_s \end{aligned}$$

But $\#(I_{\mathfrak{P}}) = ep^s$. Now, we can also get a tower

$$K \overset{r}{\subseteq} L^{D_{\mathfrak{P}}} \overset{f_s}{\subseteq} L^{I_{\mathfrak{P}}} \overset{ep^s}{\subseteq} L.$$

This finishes our elementary discussion of extensions. Next, we want to discuss

Completions The standard example is Q. Take all absolute values, up to equivalence. There's the usual one, ∞. Additionally, there are the p-adic valuations v_p. What's nice is that this is all of them. If you complete at one of these absolute values, you get either R or Q_p, depending. The main difference is that Q_p has a natural lattice inside, Z_p. So it's a discrete valuation ring.

We can play a similar game with any number field. The only difference is that you might get C instead of R. If A is a discrete valuation ring, then you can complete it. You can do this algebraically; let

$$\widehat{A} = \varprojlim_n A/\mathfrak{m}^n.$$

The field of fractions is $\widehat{K}$. If you know a little commutative algebra, you realize that there's a little problem; elements in the completion may not be algebraic over K. Philosophically, the right thing to do is use Henselizations of A. You more or less get the same thing. One reason is that $A \hookrightarrow \widehat{A}$ is faithfully flat; and the Artin approximation theorem is another reason.

So what does flatness mean? Hold on, you'll find out. If you have an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of finitely generated A-modules, and you tensor over $\widehat{A}$, then

$$0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$$

remains exact. You can prove this directly as an exercise. Just use the fundamental theorem of abelian groups, generalized to principal ideal domains; you can put everything into a standard position.

Recall the standard picture with A, B, $\mathfrak{P}_i$, etc. Before, we used localizations to explore $A_\mathfrak{p} \subseteq B_{\mathfrak{P}_i}$. There's also a localization $B_\mathfrak{p}$. If we take completions, then $\widehat{B_\mathfrak{p}}$ is a finite $\widehat{A_\mathfrak{p}}$ module. And we get

$$\widehat{B_\mathfrak{p}} = \prod_i \widehat{B_{\mathfrak{P}_i}}.$$

That's because

$$B/\mathfrak{p}^n = \prod_i B_{\mathfrak{P}_i}/\mathfrak{P}_i^{e_i n}.$$

Of course, this uses the usual factorization of $\mathfrak{p}B$. Thus,

$$\widehat{L_\mathfrak{p}} = \prod \widehat{L_{\mathfrak{P}_i}}.$$

For today, A is a complete discrete valuation ring, and K is $\mathrm{Frac}(A)$.

For example, $\kappa = A/\mathfrak{m}$ is finite. Then A is either $\mathbb{F}_q((t))$ or a finite extension of $\mathbb{Q}_p$. This corresponds to the topological situation where K is a locally compact, totally disconnected topological field.

Fact If K is a locally compact topological field, then either $K \cong \mathbb{R}$ or $\mathbb{C}$, or K is the fraction field of a complete discrete valuation ring with finite residue field. In each case we have a Haar measure on K. It's unique up to $\mathbb{R}_{>0}$. Call it μ. Then we have a canonical absolute value, namely,

$$\mu(xE) = \|x\|\,\mu(E)$$

where E is any measurable set. Let $q = \#\kappa$ the number of elements in the residue field. Then $\|x\| = q^{-v(x)}$. To verify this, just look at what happens when x is a uniformizer. Well,

$$\begin{aligned} \mu(A) &= \sum_{a_i \in A/\mathfrak{m}} \mu(a_i + \mathfrak{m}) \\ &= q\mu(\mathfrak{m}). \end{aligned}$$

We now return to the general situation, K is the fraction field of a complete DVR, L a finite extension of K. As always, B is the integral closure of A inside L. We'll see that B is a discrete valuation ring, and that it's a finite A-module. This is real nice; it's part of why we work with complete DVR's.[5]

So let's prove this stuff. We start off with a tower $\begin{array}{ll} L & \\ \mid & \text{pure insep} \\ L^s & \\ \mid & \text{sep} \\ K & \end{array}$.

Case 1: L/K is separable; show B finite over A. We have $\begin{array}{ccc} \mathfrak{P}_i & \subseteq & B \\ \mid & & \mid \\ \mathfrak{m} & \subseteq & A \end{array}$. We want to show that $r = 1$. Well, L is a finite dimensional vector space over K. Each $\mathfrak{P}_i$ gives some absolute value $\|\cdot\|_i$. For each i, $\|\cdot\|_i$ gives L a topology $\mathcal{T}_i$; so L becomes a finite dimensional topological vector space over K. We now invoke the following

[5]This is a consequence of the fact that a complete DVR is an excellent ring.

Fact If K is complete, then every finite dimensional vector space over K has a unique structure as a topological vector space over K.[6]

So now we know that all the topologies coincide. $\Rightarrow$ all the prime ideals are the same. So $r = 1$.

Case 2, L is purely inseparable over K. Then for all x, $x^{p^i} \in K$ for $i \gg 0$. We can choose i_0 so that $x^{i_0} \in K$ for all $x \in L$, since the extension is finite. There's a map

$$\begin{array}{ccccccc} L & \to & K & \stackrel{\|\cdot\|}{\to} & \mathrm{R} & \to & \mathrm{R} \\ x & \mapsto & p^{i_0} & & t & \mapsto & t^{p^{-i_0}} \end{array}$$

So now we've got this absolute value extending the one on K; $\|x\|_L = \left\|x^{p^{i_0}}\right\|_L^{p^{-i_0}} = \left\|x^{p^{i_0}}\right\|_K^{p^{-i_0}}$.

So now we look at $B/\pi B$. This is a module over $A/\pi A = \kappa$. Couple of claims.

First, $\overline{x_1}, \cdots, \overline{x_m} \in B/\pi B$ linearly independent over κ, then if we take [arbitrary] lifts x_i, the lifts are linearly independent over K. $\Rightarrow \dim_\kappa B/\pi B \leq [L : K]$.

How to do this? Assume $\sum a_i x_i = 0$. We may assume that that $a_i \in A$, by clearing denominators. We can also assume that $\overline{a_i}$ aren't all zero; divide out by uniformizer, if necessary. Then induction gives you a contradiction.

Now take $\overline{x_1}, \cdots, \overline{x_m}$ a κ basis of $B/\pi B$. Claim that $B = Ax_1 + \cdots + Ax_m$. Well, choose a_i so that $b - \sum a_{i,0} x_i \in \pi B$.[7] Then, take $\frac{1}{\pi}$ of that and subtract $\sum a_{i,1} x_i \in \pi B$. So $b - \sum (a_{i,0} + a_{i,1}\pi) x_i \in \pi^2 B$. Let $a_i^{(0)} = a_{i,0} + a_{i,1}\pi$, etc. Then by completeness, the $a_i^{(r)}$ go to a limit; call these $a_i \in A$. So $b = \sum a_i x_i$.$\diamond$

With the usual picture upstairs and downstairs, we have

$$B \otimes \widehat{A_{\mathfrak{p}}} = \prod_i \widehat{B_{\mathfrak{P}_i}}$$

and

$$\widehat{L_{\mathfrak{p}}} = L \otimes_K \widehat{K_{\mathfrak{p}}} = \prod_i \widehat{K_{\mathfrak{P}_i}}.$$

Hensel's Lemma Here's the setup; $f(T) \in A[T]$, $\overline{f}(T) \in \kappa[T]$, $\overline{x} \in \kappa$, $\overline{f}(\overline{x}) = 0$. Suppose $\overline{f}'(\overline{x}) \neq 0$. Then there's a unique $x \in A$ so that $x \equiv \overline{x} \bmod \pi$, and $f(x) = 0$.

[6] See Bourbaki, *Topological Vector Spaces*, chapter 1.
[7] This is a first approximation of B.

Proof Successive approximation; Newton's method; Taylor expansion.

Suppose we have two unramified extensions L_i of K. Then $\mathrm{Hom}_K^{\mathrm{alg}}(L_1, L_2) \to \mathrm{Hom}_\kappa^{\mathrm{alg}}(\lambda_1, \lambda_2)$; and actually, this is a bijection.

In particular, if we take $\mathrm{Gal}(K^{\mathrm{unr}}, K) \to \mathrm{Gal}(\kappa^{\mathrm{sep}}, \kappa)$, then this is an isomorphism. In a sense, the unramified extensions of a local field are easy, as long as you understand the Galois group of the residue field. For instance, if $\kappa = \mathrm{F}_q$, then $\mathrm{Gal}(\kappa^{\mathrm{sep}}, \kappa) \cong \widehat{\mathrm{Z}} = \varprojlim_n \mathrm{Z}/n\mathrm{Z} \cong \prod_p \mathrm{Z}_p$.

Today, K is a local field, L_1 and L_2 unramified finite extensions.[8] Then $\mathrm{Hom}_K^{\mathrm{alg}}(L_1, L_2) \to \mathrm{Hom}_\kappa^{\mathrm{alg}}(\lambda_1, \lambda_2)$ is a bijection. This implies that $\mathrm{Gal}(K^{\mathrm{unr}}, K) \cong \mathrm{Gal}(\kappa^{\mathrm{sep}}, \kappa)$. And actually, we need not assume L_2 unramified.

Lemma There's an $x \in O_{L_1}$ so that $A[x] = O_{L_1}$.

Proof Take $\overline{x} \in \lambda_1$, so that $\lambda_1 = \kappa(\overline{x})$, and take any lift $x \in O_{L_1}$ of $\overline{x}$. Why does this work? Well, adjoin x, and use Nakayama's lemma. For the maximal ideal of $A[x]$ is certainly given by π; it's a local ring. Want to show both sides equal. By Nak, all you have to show is that by tensoring with $A/\pi A = \kappa$, you get the same thing. But that's the whole point of a lift. Note that this doesn't require that A be complete.

Proposition L/K both complete, B over A, assume that λ/κ is separable, L/K finite separable. Then there's an $x \in B$ so that $A[x] = B$.

Proof Take L^{unr} the maximal unramified subextension; correspondingly, you have A^{unr}. You have $\overline{x} \in \lambda$ so that $\kappa(\overline{x}) = \lambda$. Let x_1 be any lifting of $\overline{x}$ in B. Now let $\overline{f}(T)$ be the minimal polynomial of $\overline{x}$ over κ. Then take $f(T) \in A[T]$ a lifting of $\overline{f}(T)$. Let $f = [L^{\mathrm{unr}} : K]$. We know that $1, x_1, \cdots, x_1^{f-1}$ is basis of the residue field over κ. Now multiply each of these by suitable powers of the uniformizer $\widetilde{\pi} = \pi_B$; then

$$\{\widetilde{\pi}^a x_1^b\}_{0 \le a \le e-1, 0 \le b \le f-1}$$

is a set of generators of B as an A-module.[9]

Try this again. You have

$$B \supseteq \widetilde{\pi} B \supseteq \widetilde{\pi}^2 B \supseteq \cdots \supseteq \widetilde{\pi}^{e-1} B \supseteq \widetilde{\pi}^e B = \pi B \supseteq \cdots$$

The quotient at the end can be generated by $\widetilde{\pi}^{e-1}, \widetilde{\pi}^{e-1} x_1, \cdots, \widetilde{\pi}^{e-1} x_1^{f-1}$.

[8] They are separable by virtue of being unramified.

[9] Nakayama: $B \otimes_A (A/\pi) B/\pi_A B$. Let $\widetilde{\pi}$ be the uniformizer in B. Anyways, $\pi B = \widetilde{\pi}^e B$. So there's a filtration

$$B/\pi B \supseteq B/\widetilde{\pi}^{e-1} B \supseteq \cdots$$

If you look at this, it corresponds to the quotient $\widetilde{\pi}^{e-1} B / \widetilde{\pi}^e B$. And the set given above gives you generators for that quotient.

At the beginning, we can use $1, x_1, \cdots, x_1^{f-1}$ to generate the first quotient $B/\tilde{\pi}B$. And all this is Nakayama's lemma.

$\Rightarrow$ Look at $f(x_1)$. If this is a uniformizer in B, we win. Otherwise, change $x_1 \mapsto x_1 + \tilde{\pi}y$. If $f(x_1 + \tilde{\pi}y)$ is a uniformizer, then we're okay. Otherwise, take Taylor expansion

$$f(x_1 + \tilde{\pi}y) = f(x_1) + \tilde{\pi}yf'(x_1) + \tilde{\pi}^2(*)$$

We're assuming that $f(x_1) \equiv 0 \bmod \tilde{\pi}^2$. But $\overline{f'(x_1)} \neq 0$, since $\overline{x_1}$ is separable. So take $y \in B^\times$, some unit.

We're going back to the claim at the beginning of class. Take $x \in O_{L_1}$ so that $A[x] = O_{L_1}$. Let $f(T) \in A[T]$ be the minimal polynomial of x over K. Then we know that $\overline{f}$ is separable, as well, and is the minimal polynomial of $\overline{x}$, which generates λ_1 over κ. Let's think about $\mathrm{Hom}_K^{\mathrm{alg}}(L_1, L_2)$. Well, $L_1 = K[T]/(f(T))$. So $\mathrm{Hom}_K^{\mathrm{alg}}(L_1, L_2)$ is just the set of roots of $f(T)$ in L_2. Equivalently, this is the set of roots of $\overline{f}(T)$ in λ_2. Why is this last thing a bijection? Hensel's lemma!$\diamond$

Newton polygons K a complete local field. We have $f(T) \in K[T]$. Write it as $\sum^n a_i T^i$. What can you say about the roots? Well, Newton's polygon will tell you about the valuations of the roots.

Consider the collections $\{(i, v(a_i))\}0 \leq i \leq n \subseteq \mathrm{R}^2$. Take the convex hull of these points. It consists of a bunch of segments, with length m_i so that $\sum m_i = n$. Anyway, there are m_i roots with valuation $-s_i$, where s_i is the slope of the i^{th} segment.

Can remember this by looking at the polynomial $T - a$.

Proof Well, a hint of the proof, anyway. Let $x_1, \cdots, x_{r_1}; \cdots$ be the roots in order of decreasing values. Then $v(x_1) = \cdots = v(x_{r_1}) > v(x_{r_1+1}) = \cdots = v(x_{r_1+r_2}) > \cdots$. We may assume that $a_n = 1$, by dividing out by the uniformizer. Then $f(T) = \prod_i (T - x_i)$. Then see what you can say about the $v(x_i)$.

Ramification We'll be talking about the difference and discriminant. What we're trying to do is get a measure of how bad the ramification is.

For the time being, take A to be a Dedekind domain; K its field of fractions; L a finite separable extension;[10] B the integral closure of A in L.

Heuristic discussion follows. B/A is ramified means that this is not locally trivial. Local triviality means they're the same when you reduce mod the prime ideal. For $B/\pi B$ is a ring over the field $\kappa = A/\pi A$. We'll try to interpret not being locally trivial. We know that

$$B/\pi B = \prod_i B/\mathfrak{P}_i^{e_i} B.$$

This is the Wederburn factorization of this finite algebra extension. $B/\pi B$ separable over κ means that each $B/\mathfrak{P}_i^{e_i}$ is a separable field extension of κ; i.e., B is unramified over A.

Now, the trace is a way of measuring [non]separability. Specifically, $\operatorname{tr}_{(B/\pi B),\kappa}$ measures whether $B/\pi B$ is separable over κ. The trace is given by $\operatorname{tr}(\overline{b})$ where we view $\overline{b}$ as a linear operator. Then $\operatorname{tr}(\overline{b}) \in \kappa$. From elementary field theory we know that if we have a field extension of finite degree, then the trace gives a nondegenerate pairing $\iff$ the extension is separable.[11]

Consider the [nondegenerate] pairing $\operatorname{tr}_{L,K} : L \times L \to K$. This restricts to $B \times B \to A$. The trace here induces the trace on residue fields. For this trace map to be nondegenerate, well, it's $\iff$ $\operatorname{tr}_{(B/\pi B),\kappa} : (B/\pi B) \times (B/\pi B) \to \kappa$ is nondegenerate. $\iff$ B/A is unramified. And actually, the determinant will have to be a unit. If $\{e_i\}$ is a basis at $\mathfrak{p}$, then $\det(\operatorname{tr}(e_i e_j)) \in A_{\mathfrak{p}}^{\times}$.

Let $B^{\vee} = \{x \in L | \operatorname{tr}_{L,K}(xy) \in A \forall y \in B\}$. Clearly, $B \subseteq B^{\vee}$. And B/A unramified $\iff$ $B^{\vee} = B$. $B^{\vee}$ is a fractional ideal in L.

Hopefully this is enough to motivate the following

Definition

1. $(B^{\vee})^{-1} \stackrel{\text{def}}{=} \mathcal{D}_{B,A} = \mathcal{D}_{L,K}$, the difference.
2. The discriminant is $\operatorname{disc}_{B,A} = N_{L,K}(\mathcal{D}_{B,A}) = \chi_A(B/\mathcal{D}_{B,A})$. [12]

Reminder about the Euler characteristic. If you take M an A-module of finite length, then take a composition series $M = M_0 \supset M_1 \supset \cdots \supset M_m = (0)$ so that $M_i/M_{i+1} \cong A/\mathfrak{P}_i$. Then we define $\chi_A(M) = \prod_i \mathfrak{P}_i$. If M is a B-module of finite length, then $\chi_A(M) = N_{B,A}(\chi_B(M))$. If there's a short exact sequence $0 \to M' \to M \to M'' \to 0$, then $\chi_A(M) = \chi_A(M') \cdot \chi_A(M'')$.

[10] From now on, the extension of fraction fields will be separable.
[11] This is true for finite field extensions, and $\mathfrak{P}_i/\mathfrak{P}_i^{e_i} = \operatorname{rad}(B/\mathfrak{P}_i^{e_i})$.
[12] Recall that $N(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}}}$. And $\chi_B(B/\mathcal{D}_{B,A}) = \mathcal{D}_{B,A}$.

Proposition B/A is unramified $\iff$ $\mathcal{D}_{L,K} = B$ $\iff$ $\mathrm{disc}_{B,A} = A$. $\chi_B(B/\mathcal{D}_{B,A}) = \mathcal{D}_{B,A} = \chi_B(\mathcal{D}_{B,A}^{-1}/B)$.

Well, that's basically what we just did.

Proposition $\mathcal{D}$ and disc commute with localization and completion.

Proof Really, it's enough to show that the trace commutes.[13]

So how do you compute this stuff?

Lemma Assume that A is a discrete valuation ring. Let (b_i) be an A-basis for B. Look at $\mathrm{tr}(b_i b_j) \in M_{n\times n}(A)$. Observe that $\det(\mathrm{tr}(b_i b_j)) \in A$. Well, we claim that $\det(\mathrm{tr}(b_i b_j))A = \mathrm{disc}_{B,A}$.

It comes down to thinking about the length of $B^\vee/B$. But you can throw B into $B^\vee$ in a standard way. Let $x_1, \cdots, x_n$ be an A-basis for $B^\vee$; $(a_i x_i)$ is an A-basis for B. Well, $\det(\mathrm{tr}(b_i b_j)) = (\prod a_i)\cdot$unit. It's given by $\sum v_A(\prod_i a_i)$.

Let's try this again. Pick a basis, and look at $B \subseteq B^\vee$. Think about the bilinear pairing $B \times B \rightarrow$. We can choose basis u_i for one copy of B, and v_i for the other one. Then $\det(\mathrm{tr}(u_i v_j))A^\times \in A/A^\times$. So we can choose a basis appropriately, and compute in this fashion. Another way to compute is put $B \subseteq B^\vee$. $B^\vee/B \cong \oplus_i A/a_i A$.

When all is said and done, $\mathrm{disc}_{B,A} = \mathfrak{p}^{v(\prod a_i)}$.

[13] It's because these two operations are flat.

As always, we have A a discrete valuation ring, B a finite extension. Choose an A-basis $e_1, \cdots, e_n$ of B. Consider the matrix $\mathrm{tr}(e_i e_j)$; and then take its determinant. This will be the discriminant. If e_i' is another basis, then $\det(\mathrm{tr}(e_i e_j)) \cdot A^\times = \det(\mathrm{tr}(e_i e_j')) \cdot A^\times$. This ideal is the discriminant ideal.

Recall that $B^\vee \supset B$. Can choose an A-basis $x_1, \cdots, x_n$ so that there are a_i with $\{x_i\}$ an A-basis for $B^\vee$, and $\{a_i x_i\}$ is an A-basis for B.[14] Then as A-modules, we have

$$B^\vee / B \cong \oplus_i A/a_i A.$$

This gives us $\chi_A(B^\vee/B) = (\prod_i a_i) \cdot A$. Let $\{x_j^*\}$ be the dual of the $\{x_j\}$[15] and compute

$$\det \mathrm{tr}(a_i x_i \cdot x_j^*) = \prod_i a_i.$$

Now assume A not necessarily local, with field of fractions K; L an extension of K. If B is a free A-module, $\{e_1, \cdots, e_n\}$ a basis, then $\mathrm{disc}_{B,A} = \det(\mathrm{tr}(e_i e_j))$.

Observation: If $\{e_i\}$ an A-basis for B, let $\sigma_i : L \to \overline{K}$ be the n embeddings of L into the algebraic closure of K. Then

$$(\det(\sigma_i(e_j)))^2 = \det(\mathrm{tr}(e_i e_j)).$$

Let X be the matrix $(\sigma_i(e_j))$. Then ${}^tX \cdot X = (\mathrm{tr}(e_i e_j))$; for the trace of $e_i e_j$ is the sum of all its conjugates.

When $K = \mathbb{Q}$, $A = \mathbb{Z}$, then the assumption that B is a free A-module is always satisfied. So for every L a number field, let $e_1, \cdots, e_n$ be a $\mathbb{Z}$-basis for $O_L = B$. We can define the absolute discriminant as

$$\mathrm{disc}_{L,Q} = \det(\mathrm{tr}(e_i e_j)).$$

This is well-defined, since the only units in $\mathbb{Z}$ are ± 1, and $(\pm 1)^2 = 1$. This number is the discriminant.

[14] Fundamental theorem for finitely generated modules over a principal ideal domain.
[15] with respect to the trace

Lemma

1. $\mathrm{disc}_{L,\mathbb{Q}} \equiv 0$ or $1 \bmod 4$. This is the information from the prime 2.
2. $\mathrm{sgn}(\mathrm{disc}_{L,\mathbb{Q}}) = (-1)^{r_2}$ where r_2 is the number of complex embeddings. In other words,

$$r_2 = \#\{\sigma : L \to \mathbb{C} | \sigma(L) \not\subset \mathbb{R}\}.$$

   Alternately, one could say it's the σ so that $\sigma \neq \iota \circ \sigma$, where ι is complex conjugation. This is the information from the prime at ∞.

Proof

1. Write $\det X$ as $P - N$ where P is the sum of terms with $+$ signs, and N is the terms with $-$ signs. One can see that $P + N, PN \in \mathbb{Z}$. So the discriminant is $(P-N)^2 = (P+N)^2 - 4PN$.
2. How do we get a hold of the sign? Think of L as sitting inside $\mathbb{C}$. Hmmm. We know that $\det(X)^2 = \mathrm{disc}_{L,Q}$. Look at what complex conjugation does: $\iota(\det(X))$. Well,

$$\begin{aligned} \iota(\det(X)) &= \det(\iota(X)) \\ &= (-1)^{r_2} \det X. \end{aligned}$$

   The last follows since ι will interchange r_2 pairs of rows of X.

How do we compute a discriminant? A and B as before:

$$\begin{tikzcd} & L \\ B \arrow[ur] & \\ & K \arrow[uu] \\ A \arrow[uu] \arrow[ur] & \end{tikzcd}$$

Let $L = K[x]$, $x \in B$, $B \supseteq A[x]$. Let $f(T)$ be the monic minimal polynomial of x in $A[T]$. Write $A[x] = C$. We want to determine the dual of C, $C^\vee$, with respect to the trace. Well, $C \cong A[T]/(f(T))$, and so

$$C = A \oplus Ax \oplus \cdots \oplus Ax^{n-1}.$$

Out of our butt, we pull the following:

$$\frac{1}{f(T)} = \sum_{i=1}^{n} \frac{1}{f'(x_i)(T - x_i)}$$

where x_i are the roots of f, that is, the conjugates of X.

Expand everything as a power series in $\frac{1}{T}$.

$$\begin{aligned}
\frac{1}{f(T)} &= \frac{1}{T^n} + O(\frac{1}{T^{n+1}}) \\
\frac{1}{f'(x_i)(T - x_i)} &= \frac{1}{f'(x_i)} \frac{1}{T(1 - \frac{x_i}{T})} \\
\sum_i \frac{1}{f'(x_i)(T - x_i)} &= \sum_i \frac{1}{f'(x_i)} \frac{1}{T(1 - \frac{x_i}{T})} \\
&= \sum_i \sum_{m=0}^{\infty} \frac{1}{f'(x_i)} \frac{x_i^m}{T^{m+1}} \\
&= \sum_m (\sum_i \frac{x_i^m}{f'(x_i)}) \frac{1}{T^{m+1}} \\
&= \sum_{m=0}^{\infty} \mathrm{tr}(\frac{x^m}{f'(x)}) \frac{1}{T^{m+1}}.
\end{aligned}$$

The conclusion from all this is that

$$\mathrm{tr}(\frac{x^m}{f'(x)}) = \begin{cases} 0 & m = 0, \cdots, n-2 \\ 1 & m = n-1 \end{cases}.$$

And so

$$\begin{aligned} C^\vee &= \{y \in L \,|\, \mathrm{tr}_{L,K}(yz) \in A \forall z \in C\} \\ &= \frac{1}{f'(x)} \cdot C. \end{aligned}$$

To prove this last bit, we have to work with the matrix $\mathrm{tr}(x^i \frac{x^j}{f'(x)})_{0 \le i,j \le n-1}$. It looks like $\begin{pmatrix} 0 & \cdots & 1 \\ \vdots & \cdots 1 \cdots & \\ 1 & & * \end{pmatrix}$. From this, we know that it's determinant is ± 1; it's really $(-1)^{\frac{n(n+1)}{2}}$.

Proposition

1. $\mathcal{D}_{B,A} \subseteq f'(x) \cdot B$.
2. If $B = A[x]$, then $\mathcal{D}_{B,A} = f'(x)B$.
3. The conductor $\mathrm{cond}(A[x] : B) \stackrel{\text{def}}{=} \{y \in L : yB \subseteq A[x]\}$ is given by $f'(x) \cdot \mathcal{D}_{B,A}^{-1}$.

Proof Let $z \in (C : B)$; that is, $zB \subseteq C$. This is the same as $zf'(x)^{-1}B \subseteq C^\vee$. $\iff$ $\mathrm{tr}(f'(x)^{-1}BC) \subseteq A$; but $BC = B$. By definition, $zf'(x)^{-1} \in \mathcal{D}_{B,A}^{-1}$. So $z \in f'(x)\mathcal{D}_{B,A}^{-1}$.

We've decided that problem sessions will be Mondays at 10:00.

We're now trying to measure how much $A[x]$ differs from the whole ring of integers. Or at least, that's what we were doing.

Tamely ramified extensions

Proposition A a [complete] discrete valuation ring, K its field of fractions, L/K a finite separable extension, B the integral closure of A in L, p is the residue characteristic. Then $v(\mathcal{D}_{B,A}) \geq e-1$, and the following are equivalent.

1. $\mathcal{D}_{B,A} = \mathfrak{P}^{e-1}$.
2. $\operatorname{tr}_{B,A}(B) = A$.
3. $p \not| e$, λ/κ separable.

Proof Well, $\operatorname{tr}(\mathfrak{P}) \subseteq \mathfrak{p}$. $\Rightarrow \operatorname{tr}(\mathfrak{p}^{-1}\mathfrak{P}) = \operatorname{tr}\mathfrak{P}^{1-e} \subseteq A$. For the trace is a linear map over A. This proves the first statement.

On to the second part. Say that $\mathcal{D}_{B,A} = \mathfrak{P}^{e-1}$. Then the inverse different cannot possibly be bigger than $\mathfrak{P}^{1-e}$. If it is bigger, then $\operatorname{tr}(\mathfrak{P}^{-e}) \not\subseteq A$; $\operatorname{tr}(\mathfrak{P}^{-e}) = \mathfrak{p}^{-1}\operatorname{tr}(B)$. Therefore, $\mathcal{D}_{B,A} = \mathfrak{P}^{e-1} \iff \operatorname{tr}(B) = A$.

Look at the third [last] condition. Nakayama's lemma tells us that this is equivalent to $\operatorname{tr}_{(B/\mathfrak{p}B),\kappa}(B/\mathfrak{p}B) = \kappa$. Think about $B/\mathfrak{p}B$. There's a filtration

$$B/\mathfrak{p}B = B/\mathfrak{P}^e B \supseteq \mathfrak{P}/\mathfrak{P}^e \supseteq \mathfrak{P}^2/\mathfrak{P}^e \supseteq \cdots \supseteq \mathfrak{P}^{e-1}/\mathfrak{P}^e.$$

This is a filtration by B-submodules. Take any $\overline{b} \in B/\mathfrak{p}B$. Think about its trace. This means, take the characteristic polynomial of multiplication by $\overline{b}$, and look at the coefficient of the term whose degree is one less than the top. This tells us that, given such a filtration,

$$\operatorname{tr}_{B/\mathfrak{p}B}(\overline{b}) = \sum_{i=0}^{e} \operatorname{tr}_{\mathfrak{P}^i/\mathfrak{P}^{i+1}}(\overline{\overline{b}})$$

where we have $\overline{b} \mapsto \overline{\overline{b}} \in \lambda$. But these successive quotients are all isomorphic as B-modules; all the traces are the same. So

$$\operatorname{tr}_{B/\mathfrak{p}B}(\overline{b}) = e \cdot \operatorname{tr}_{\lambda,\kappa}(\overline{\overline{b}}).$$

The trace is surjective $\iff p \not| e$; for otherwise the trace would be zero;and $\operatorname{tr}_{\lambda,\kappa} : \lambda \to \kappa$ is surjective. That last thing is just a fancy way of saying that λ is separable.

Remark Assume λ/κ is a separable extension.[16] Then we know that $B = A[x] \cong A[T]/(f(T))$, where $f(T)$ is the minimal polynomial of x over K. $\Rightarrow$

$$\begin{aligned}
\Omega^1_{B,A} &\cong \frac{B \cdot dT}{f'(T) B dT} \\
&\cong B/(f'(T)). \\
&\cong \frac{B}{\mathcal{D}_{B,A}} \\
&\cong \frac{\mathcal{D}^{-1}_{B,A}}{B}.
\end{aligned}$$

Now the question is, what happens if λ/κ is inseparable? Unfortunately, we don't have an elementary proof at hand...

Well, the answer is

$$\chi_B(\Omega^1_{B,A}) = \chi_B(\mathcal{D}^{-1}_{B,A}/B).$$

Try to figure this out?

Moving on to higher ramification groups. We've got A a complete DVR, $K = \mathrm{Frac}(A)$, L a finite Galois extension with group G. And as usual, $B \subseteq L$, etc. Define subgroups $G_i \subseteq G$ by

$$G_i = \{\sigma \in G : \sigma|_{(B/\mathfrak{P}^{i+1})} = \mathrm{id}\}.$$

Here, $\mathrm{Z} \ni i \geq -1$; $G_{-1} = G$. And

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "e"'] & (1) \arrow[d, dash] \\
K^{\mathrm{unr}} \arrow[r, dash] \arrow[d, dash, "f"'] & G_0 \arrow[d, dash] \\
K \arrow[r, dash] & G
\end{tikzcd}$$

[16]The standard number theory setup.

So $\#G_0 = e$. It should be clear that these areally are subgroups. If $B = A[x]$, then we know that $\sigma \in G_i \iff \sigma(x) \equiv x \bmod \mathfrak{P}^{i+1}$.

Now define $i_G(\sigma) \in \mathbb{Z}$ by $i_G(\sigma) \geq i+1 \iff \sigma \in G_i$. In other words, σ operates trivially on $B/\mathfrak{P}^i$, but not on $B/\mathfrak{P}^{i-1}$.

So we see that $i_G(\sigma) = v_L(\sigma(x) - x)$. So $i_G(\sigma) = \min_{y \in B} v_L(\sigma(y) - y)$.

There's another thing in the literature called $j_G(\sigma)$. We set $j_G(\sigma) = i_G(\sigma) - 1$. This is useful because $j_G(\sigma) \geq i \iff \sigma \in G_i$.

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash] & (1) \arrow[d, dash] \\
K_1 \arrow[d, dash] & G_1 \arrow[d, dash] \\
K^{\mathrm{unr}} \arrow[r, dash] \arrow[d, dash, "f"'] & G_0 \arrow[d, dash] \\
K \arrow[r, dash] & G
\end{tikzcd}$$

Clearly, G_0 is the inertia group $I_{L,K}$. We've got a filtration

$$G \supseteq G_0 \supseteq G_1 \supseteq \cdots$$

We'll se that G_0 and G_1 give the tame ramification. For now, simply note that if we take a uniformizer π, and $\sigma \in G_0$, then $\sigma(\pi)$ is, well, all we know is that it's a uniformizer. Try to get a handle on $\frac{\sigma(\pi)}{\pi}$. It's a unit. So consider

$$\sigma \mapsto \frac{\sigma(\pi)}{\pi} \bmod \mathfrak{P} \in \lambda = \frac{B}{\mathfrak{P}}.$$

Check that this is a well-defined map $G_0 \to B/\mathfrak{P}$, that is, it's independent of the choice of π. The kernel of this map, θ_0, is G_1.

For today, A a complete DVR, $K = \mathrm{Frac}(A)$, L a finite Galois extension, $G = \mathrm{Gal}(L, K)$, $B \subset L$ the integers. We defined a filtration

$$G = G_{-1} \supseteq G_0 \supseteq \cdots \supseteq G_N = \{1\}$$

where

$$G_i = \{\sigma \in G : \sigma|_{B/\mathfrak{P}^{i+1}} = \mathrm{id}\}.$$

We had a numerical measure $i_G(\sigma) = j_G(\sigma) + 1$, given by $\sigma \in G_i \iff j_G(\sigma) \geq i$.

At the end of last time we were thinking about G_0 the inertia group. And there's a map $G_0/G_1 \to \lambda$. How? Well, we choose a uniformizer π, and send $\sigma \mapsto \frac{\sigma(\pi)}{\pi} \bmod \pi$. If $u \in B^\times$, we should show that using $u\pi$ is the same. Well, we get $\frac{\sigma(u)\sigma(\pi)}{u\pi}$. But $\sigma(u) \equiv u \bmod \pi$. So the thing is well-defined. Moreover, $\frac{\sigma(\pi)}{\pi} \equiv 1 \bmod \pi, \iff \sigma(\pi) \equiv \pi \bmod \pi^2. \Rightarrow \sigma(u\pi) \equiv u\pi \bmod \pi^2$ for all $u \in B$. [That's because $\sigma(u) \equiv u \bmod \pi$.] This shows that $G_0/G_1 \hookrightarrow \lambda^\times$. We can thus conclude that G_0/G_1 is cyclic, and of order prime to p.[17] So G_0 over G_1 is the tame part of the extension. And shortly, we'll see that this really is the maximal tame extension.

We have the following picture:

$$G_{-1} \overset{\text{unram}}{\supseteq} G_0 \overset{\text{tame}}{\supseteq} G_2 \supseteq \cdots \supset G_N = \{1\}.$$

Claim that the last part, G_1/G_N, is a p-group. Consider $G_i/G_{i+1} \to ?$. Well, choose a uniformizer π. For $\sigma \in G_i$, send it to $\frac{\sigma(\pi)}{\pi}$. We know that $\sigma(\pi) \equiv \pi \bmod \pi^{i+1}$. So $\frac{\sigma(\pi)}{\pi} \equiv 1 \bmod \pi^i$. So the map is $\sigma \mapsto \frac{\sigma(\pi)}{\pi} \in (1 + \pi^i B)/(1 + \pi^{i+1} B)$. Gotta check that we could use $u\pi$ instead of π. But $\frac{\sigma(u\pi)}{u\pi} = \frac{\sigma(u)}{u} \frac{\sigma(\pi)}{\pi}$. But $u \in B^\times$, and $\sigma(u) \equiv u \bmod \pi^{i+1}$. So $\frac{\sigma(u)}{u} \equiv 1 \bmod 1 + \pi^{i+1} B$.

Again, if $\frac{\sigma(\pi)}{\pi} \equiv 1 \bmod \pi^{i+1}$, then $\frac{\sigma(u\pi)}{u\pi} \equiv 1 \bmod \pi^{i+1}$ for all $u \in B$, that is, $\sigma(u\pi) \equiv u\pi \bmod \pi^{i+2}$; and thus $\sigma \in G_{i+1}$.

Let's look at the target of the embedding. We're looking at the $(1 + \pi^i B)$ as multiplicative groups. And

$$\frac{(1 + \pi^i B)^\times}{(1 + \pi^{i+1} B)^\times} \overset{\cong}{\to} \frac{\mathfrak{P}^i}{\mathfrak{P}^{i+1}}.$$

[17] Since the Frobenius map is injective over in $\lambda^\times$.

The backwards map is $x \mapsto 1 + x$. The map

$$\theta_i : \frac{G_i}{G_{i+1}} \hookrightarrow \frac{(1+\pi^i B)^\times}{(1+\pi^{i+1}B)^\times}$$

is Galois invariant. On the left, it's conjugation; on the right, it's the natural action. So this map is a G-map.

Now, $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ has the additional structure of a 1-dimensional vector space over λ. So we get a Galois representation; it's a λ-vector space and an action of $\kappa[G]$. So $\mathfrak{p}^i/\mathfrak{P}^{i+1} \cong \lambda^{\otimes i}$.[18] Anyways, we have a natural embedding $G_i/G_{i+1} \hookrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1}$.

From this we can deduce several things. Among others, we note that G_i/G_{i+1} is a p-group; and it's actually an abelian p-group, $\cong (\mathrm{Z}/p)^{\oplus m}$. [If the characteristic is $p = 0$, then $G_i = \{1\}$ for all i; the extension is automatically tame.]

Lemma For every $i, j \geq 1$, $s \in G_i$, $t \in G_j$, look a the commutator; $sts^{-1}t^{-1} \in G_{i+j}$. For the filtration, we'll se that $\mathrm{gr}_{\mathrm{Fil}}(G_\bullet) = \oplus_{i\geq 0} G_i/G_{i+1} \overset{\theta}{\hookrightarrow} \oplus_{i\geq 0}\mathfrak{P}^i/\mathfrak{P}^{i+1}$. This gives a "Lie bracket" on $\oplus_{i\geq 1} G_i/G_{i+1}$. Anyways,

$$\theta(sts^{-1}t^{-1}) = (j-i)\theta_i(s)\theta_j(t).$$

Proof Pray that it's a straight computation.

$$\begin{array}{rcl}
s(\pi) &=& \pi(1+a)\ a \in \mathfrak{P}^i \\
t(\pi) &=& \pi(1+b) b \in \mathfrak{P}^j \\
sts^{-1}t^{-1}(ts\pi) &=& st(\pi) \\
&=& s(\pi)(1+s(b)) \\
&=& \pi(1+a)(1+s(b)) \\
ts\pi &=& t(\pi)(1+t(a)) \\
&=& \pi(1=b)(1+t(a)) \\
\theta(sts^{-1}t^{-1}) &\equiv& \dfrac{1+a)(1+s(b))}{(1+b)(1+t(a))} \\
a &=& \pi^i u \\
b &=& \pi^j v
\end{array}$$

[18] Somehow. Twisted tensor product?

$$\begin{aligned} s(b) &= s(\pi)^j s(v) \\ &= \pi^j (1+a)^j s(v) \\ &= \pi^j (1+ja) \pmod{\pi^{i+j+1}} \\ t(a) &= \pi^i (1+\pi b) \pmod{\pi^{i+j+1}}. \end{aligned}$$

Then multiply and hope it all works out.◇

Proposition $i, j \geq 1$, $G_i \supsetneq G_{i+1}$, $G_j \supsetneq G_{j+1}$. Then $i \equiv j \bmod p$.

Proof Let $G_{i_0} \supsetneq G_{i_0+1} = \{1\}$, the last break. Want to show that $i, j \equiv i_0 \bmod p$. Let's work with i; clearly, it doesn't matter which we pick. Look at the result from the lemma, and jump up and down.◇

Proposition If $i, j \geq 1$, $(s,t) = sts^{-1}t^{-1} \in G_{i+j+1}$; so the usual Lie bracket structure on the associated graded structure is actually zero.

Proof Look at the same formula in the lemma. If $\theta_i(s)$ or $\theta_j(t)$ is zero, we're done. So assume that they're nonzero; then i an j are both breaks; i and j are $\equiv 0 \bmod p$. So their image is $(j-i) \cdot \text{blah}$, and $j - i \equiv 0 \bmod p$; so the answer is zero, and the result actually lives in G_{i+j+1}.

So if the first break is at G_a, the next one can't be until G_{a+p+1}.

We're still thinking about higher ramification groups. The assumptions are the usual. Specifically, A a complete DVR, $K = \mathrm{Frac}(A)$, L a finite Galois extension, B the integral closure of A in L. We've got the filtration

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq G_N = \{1\}.$$

We think of these indices i as being in Γ, the value group of L. Recall that the value group is $\Gamma = \Gamma_L = K^\times/A^\times \cong \mathrm{Z}$; the isomorphism is given by the valuation. We have

$$\Gamma_L \subseteq \Gamma_L \otimes \mathrm{R}.$$

We're going to define another sort of filtration, the upper-numbering filtration. It looks like this:

$$G^{-1} \supseteq G^0 \supseteq \cdots \supseteq G^u$$

where the u are, in general, rational numbers [not necessarily integral]. We think of them as $u \in \Gamma_K \otimes \mathrm{Q} \subseteq \Gamma_K \otimes \mathrm{R}$. Define a function

$$\begin{aligned} \phi_{L,K} : \mathrm{R} &\to \mathrm{R} \\ u &\mapsto \int_0^u \frac{dt}{[G_0 : G_t]}. \end{aligned}$$

This is basically extending the lower-numbering filtration. $\{G_t\}_{t \in \mathrm{R}}$ is a decreasing filtration, continuous on the left; $G_{t^-} = G_t$. Here, if $i - 1 < t \leq i$, we let $G_t = G_i$.

This is a step function whose values are groups. So $\phi_{L,K}$ is a piecewise linear function, strictly increasing. But we think of $\phi_{L,K}$ as really being

$$\phi_{L,K} : \Gamma_L \otimes \mathrm{R} \to \Gamma_K \otimes \mathrm{R}.$$

Let $\psi_{L,K} = \phi_{L,K}^{-1}$. Then set

$$G^w \stackrel{\mathrm{def}}{=} G_{\psi_{L,K}(w)}$$

so that $G^{\phi(u)} = G_u$. There's a formula for ψ, namely,

$$\psi_{L,K}(w) = \int_0^w [G^0 : G^s] ds$$

by the implicit function theorem; for if $w = \phi(u)$, then

$$\begin{aligned} \psi'_{L,K}(w) &= \phi'(u)^{-1} \\ &= \phi'_{L,K}(\psi(w)). \end{aligned}$$

From now on, we assume that λ/κ is separable.[19]

Proposition Let $L \supset M \supset K$ be a tower of Galois extensions corresponding to $1 \subset H \subset G$;

$$\begin{array}{ccc} L & B & 1 \\ | & & | \\ M & C & H \\ | & & | \\ K & A & G \end{array}$$

H is normal in G. For all $\sigma \in \mathrm{Gal}(L, M)$,

$$\begin{aligned} i_{G,H}(\sigma) &= \frac{1}{e(L,M)} \sum_{s \mapsto \sigma} i_G(s) \\ &= \frac{1}{e(L,M)} \sum_{G_0 \ni s \mapsto \sigma} i_G(s) \\ &= \frac{1}{e(L,M)} \sum_{G \ni s \mapsto \sigma} j_G(s) \end{aligned}$$

[since $\#H_0 = \#(G_0 \cap H) = \#e(L, M)$.]

[19]Nobody knows exactly what happens if this isn't true; but it certainly ain't pretty!

Proof We'll use the proof of Tate. Take x and y with $A[x]=B$, $A[y]=C$. We know that $i_{G,H}(\sigma)=v_M(\sigma y-y)$. So the assertion is equivalent to

$$\sigma y - y \equiv \prod_{s\mapsto\sigma}(sx-x) \bmod {}^{\times}B^{\times}.$$

Let $f(T)\in C[T]$ be the minimal polynomial of x over M. So $f(T)=\prod_{\tau\in H}(T-\tau(x))$. If we hit f with any $s_0\mapsto\sigma$, then $f^{s_0}(T)=\prod_{s\mapsto\sigma}(T-s(x))$.

$$\begin{aligned} f(T) &= \prod_{\tau\in H}(T-\tau(x)) \\ f^{\sigma}(T) &= \prod_{s\mapsto\sigma}(T-s(x)) \\ f^{\sigma}-fx &= (f^{\sigma}(T)-f(T))(x) \end{aligned}$$

The coefficients of the thing on the right are all divisible by $\sigma(y)-y$; for the coefficients are all polynomials in y. From this, we conclude that the right-hand side divides the left-hand side. Thus, $\sigma(y)-y$ divides $\prod_{s\mapsto\sigma}(s(x)-x)$.

So there's a $g(T)\in A[T]$ so that $g(x)=y$; as y generates B over A. Then $g(T)-y\in C[T]$, and thus $f(T)|g(T)-y$. And so $f^{\sigma}(T)|g^{\sigma}(T)-\sigma(y)$. But $g^{\sigma}(T)=g(T)$. So

$$\begin{aligned} f^{\sigma}(x) &\mid g(x)-\sigma(y) \\ &= y-\sigma(y). \end{aligned}$$

◇

Lemma

$$\begin{aligned} \phi_{L,K}(u) &= \left(\frac{1}{[G_0:1]}\sum_{s\in G}\inf(i_G(s),u+1)\right)-1 \\ &= \frac{1}{[G_0:1]}\sum_{s\in G_0}\inf(i_G(s),u+1))-1 \\ &= \frac{1}{[G_0:1]}\sum_{s\in G_0}\inf(j_G(s),u). \end{aligned}$$

Proof Think about their derivatives. They have the same derivative, and the same value at zero. [Details left as exercise.][20]

Proposition For all $\sigma \in G/H$, let $\widetilde{i}(\sigma) = \sup\{i_G(s)\}_{s\mapsto\sigma}$, $\widetilde{j}(\sigma) = \widetilde{i}(\sigma) - 1$. Then

$$j_{G/H}(\sigma) = \phi_{L,K}(\widetilde{j}(\sigma)).$$

Proof

$$\begin{aligned}
j_{G/H}(\sigma) &= \frac{1}{\#H_0}\sum_{H_0\ni s\mapsto\sigma} j_G(s)\\
\widetilde{i}(\sigma) &= i_G(s_0) \text{ for some } s_0 \mapsto \sigma\\
j_{G/H}(\sigma) &= \frac{1}{\#H_0}\sum_{t\in H_0} j_G(s_0 t)\\
&= \frac{1}{\#H_0}\sum_{t\in H_0} \inf(j_G(t), j_G(s_0))\\
&= \phi_{L,M}(j_G(s_0))\\
&= \widetilde{j}(\sigma).
\end{aligned}$$

[20] Recall that $i_G(s) = \sum_{i\geq 0}\delta_{G_i}(s)$. $i_G(s) = i \iff s \in G_0, \cdots, G_{i-1}$ but $s \notin G_i$.

Recall that L/K a finite Galois extension with separable residue fields, $G = \mathrm{Gal}(L, K)$, $B \subseteq L$ and $A \subseteq K$. We've got the filtration

$$G = G_{-1} = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_N = \{1\}.$$

The function ϕ converts the lower numbering filtration into the upper numbering filtration. We think of $\phi_{L,K} : \Gamma_L \otimes \mathrm{R} \to \Gamma_K \otimes \mathrm{R}$. The definition is

$$\phi_{L,K}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}.$$

And $\sigma \in G_t \iff j_G(\sigma) \geq t$. By computing derivatives, we verified that

$$\begin{aligned} \phi_{L,K}(u) &= \frac{1}{\#G_0} \int_0^u \sum_{s \in G_t} \sum_{s \in G} \delta_{G_t}(s) dt \\ &= \frac{1}{\#G_0} \sum_{s \in G} \int_0^u \delta_{G_t}(s) dt. \end{aligned}$$

Now, if $j_G(s) = i$, then $s \in G_i$ but $s \notin G_{i+1}$. Then $0 \leq t \leq i \Rightarrow \delta_{G_t}(s) = 1$; and if $i < t$, then it's zero. So keep working; get

$$\int_0^u \delta_{G_t}(s) dt = \begin{cases} u & i \geq u \\ i & i \leq u \end{cases}.$$

So,

$$\phi_{L,K}(u) = \frac{1}{\#G_0} \sum_{s \in G} \inf(u, j_G(s)).$$

We can compute the value of the different. Suppose $B = A[x]$, $F(T)$ the irreducible polynomial of x with respect to K. So

$$\begin{aligned} v(\mathcal{D}_{L,K}) &= v_L(\prod_{1 \neq s \in G} (x - s(x))) \\ &= \sum_{1 \neq s \in G} i_G(s) \\ &= \sum_{1 \neq s \in G} \sum_{i \geq 0} \delta_{G_i}(s) \\ &= \sum_{i \geq 0} (\#G_i - 1). \end{aligned}$$

Last time, we proved that in the situation of last time – $L \supset M \supset K$ with tower of groups $1 \subset H \subset G$ with H normal. $H = \mathrm{Gal}(L, M)$, $G/H = \mathrm{Gal}(M, K)$. We found out that

$$\begin{aligned} j_{G,H} &= \phi_{L,M}(\tilde{j}_G(\sigma)) \\ \tilde{j}_G(\sigma) &= \sup_{s \mapsto \sigma} j_G(s). \end{aligned}$$

Of course, we already know that how to relate $j_{G,H}$ to the ramification index:

$$j_{G,H}(\sigma)e(L, M) = \sum_{G_0 \ni s \mapsto \sigma} j_G(s).$$

Let's lean on this.

$$G_u H/H = (G/H)_{\phi_{L,M}(u)}.$$

How do you remember this? Think about it like this. We've said before that the lower index filtration is indexed by the valuation upstairs. So think of the u in G_u as something in the value group of L. But here, when we index (G/H)'s filtration, we're using the value group of M. And if you believe the structure, then the way to convert from one to the other is via ϕ; and in this case, obviously the right one to use is $\phi_{L,M}$. That's how you convert value groups.

So let's see what this means. Suppose $\sigma \in G_u H/H$. Then $\exists s \mapsto \sigma$ so that $j_G(s) \geq u$. If $\sigma \in (G/H)_{\phi_{L,M}(u)}$, then $j_{G,H}(\sigma) \geq \phi_{L,M}(u)$. Now use the $\tilde{j}_G(\sigma)$ thing to see that these two conditions are equivalent.

Proposition $\phi_{M,K} \circ \phi_{L,M} = \phi_{L,K}$. Inversely, $\psi_{L,M} \circ \psi_{M,K} = \psi_{L,K}$.

Proof Gotta check that $\phi'_{M,K}(\phi_{L,M}(u))\phi'_{L,M}(u) \stackrel{?}{=} \phi'_{L,K}(u)$. But

$$\begin{aligned} \phi'_{L,K}(u) &= \frac{1}{[G_0 : G_u]} \\ \phi'_{M,K}(\phi_{L,M}(u))\phi'_{L,M}(u) &= \frac{1}{[(G/H)_0 : (G/H)_{\phi_{L,M}(u)}]} \frac{1}{[H_0 : H_u]} \\ [H_0 : H_u][(G/H)_0 : (G/H)_{\phi_{L,M}(u)}] &= [H_0 : H_u][G_0 H/H : G_u H/H] \\ &= [H_0 : H_u][G_0/H_0 : G_u/H_u]. \end{aligned}$$

◇

Proposition $G^w H/H = (G/H)^w$.

Conclusion: We don't have to think only about finite Galois extensions. Look at K^{sep}; assume κ perfect. We've got a decreasing filtration of $G = \mathrm{Gal}(K^{\mathrm{sep}}, K)$; call it (G^w). Of course

$$G = \lim_{\substack{\leftarrow \\ L\text{finite galois extension}}} \mathrm{Gal}(L, K).$$

In general, we don't understand much about this [huge!] Galois group. But we've calibrated it by (G^w), some decreasing sequence of subgroups. Their intersection is zero, and so it's a genuine calibration. We think of w as being in $\Gamma_K \otimes \mathrm{R}$.

In general, the w's are positive rational numbers; not necessarily integral. We can make an integrality statement that, when you measure the ramification of certain finite dimensional representations, then because of the multiplicity you actually get integers.[?]

Fact [Hasse-Arf] If L/K abelian, then if $G^w \supsetneq G^{w+\epsilon}$, then $w \in \mathrm{Z}$. So the breaks only occur at integers.

Combine this with Brauer's theorem that any finite-dimensional representation is induced from an abelian extension[?].

When we do class field theory we'll come back to these ramification groups. Once you have local class field theory, there's another way to calibrate this group.

We'll now begin to do the global part of algebraic number theory. We're gonna do it adelically.

Let K be either an algebraic number field or a function field of a [smooth] geometrically connected algebraic curve over F_q. The second case means that K is a finite separable extension of $\mathrm{F}_p[T]$.[21] Either way, K is called a global field.

You've got K, and a number of places v. If $K \supseteq \mathrm{Q}$, then we think about all possible discrete valuations v. Suppose we have a set of nonequivalent discrete valuations or archimedean places $\|\cdot\|_\infty$. This gives you a collection of local fields K_v. We have a normalized absolute value on each local field K_v, $\|\cdot\|_v$. We normalize so that for any $x \in K^\times$,

$$\prod_v \|x\|_v = 1.$$

If π is a uniformizer at v, then $\|\pi_v\|_v = \#\mathrm{F}_v$ for v non-archimedean.

The adèles are $\mathrm{A}_K = \prod_v' K_v = \{(x_v) : x_v \in K_v \text{ and } x_v \in O_v \text{ for almost all } v\}$.

[21] "The dumbest polynomial ring with positive characteristic."

Adeles and Ideles K is a global field. The adeles are a restricted product

$$\mathbb{A}_K = \prod_v{}' (K_v, O_v).$$

An element looks like $(x_v) \in \prod_v K_v$ so that $x_v \in O_v$ for almost all v.

The ideles are the invertible elements $\mathbb{A}_K^\times \subseteq \mathbb{A}_K$. One can also write $\mathbb{G}_m(\mathbb{A}_K)$.

We put a topology on it; but the product topology actually turns out to be too fine. Define it by writing down a fundamental system of neighborhoods of 0 in $\mathbb{A}_K$. For some finite set S containing all the infinite places ($S \supseteq S_\infty$), take

$$(\prod_{v \notin S} O_v) \times \prod_{v \in S} W_v$$

where W_v is an open neighborhood of 0 in K_v. We might also insist that $\overline{W_v}$ is compact.

This makes $\mathbb{A}_K$ a locally compact topological ring. One verifies that this structure is compatible with multiplication and addition. Open sets are pretty big.

If you think about it, we have $\mathbb{A}_K^\times \to \mathbb{A}_K \times \mathbb{A}_K$ $x \mapsto (x, x^{-1})$ a closed embedding. We can then give the ideles the induced topology. Explicitly, a fundamental system of neighborhoods of 1 in $\mathbb{A}_K^\times$ is

$$(\prod_{v \notin S} O_v^\times) \times (\prod_v W_v')$$

where W_v' is an open neighborhood of 1 in $K_v^\times$. *Do not use the topology given by* $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K$.

Now, K is embedded in $\mathbb{A}_K$ diagonally. So $K \hookrightarrow \mathbb{A}_K \rightharpoonup \mathbb{A}_K/K$; and similarly $K^\times \hookrightarrow \mathbb{A}_K^\times \rightharpoonup \mathbb{A}_K^\times/K^\times$. This last thing is called the idele class group for K. Oh, yeah. For an idele x, we set $\|x\| = \prod_v \|x_v\|_v$.

Theorem $K \hookrightarrow \mathbb{A}_K$ is discrete and cocompact, that is, the quotient is compact.

Theorem $K^\times \hookrightarrow \mathbb{A}_{K,1}^\times \subseteq \mathbb{A}_K^\times$, where $\mathbb{A}_{K,1}^\times$ is the elements of norm 1. There's no way this can be cocompact in the whole thing, but $K^\times \hookrightarrow \mathbb{A}_{K,1}^\times$ is discrete and cocompact.

This will imply, for instance, finiteness of class number and the Dirichlet unit theorem. This is the adelic remix of those classical finiteness theorems.

We can define the volume of a fundamental domain, following Minkowski.

Haar measures And Fourier inversion, Poisson summation, etc. Really, this'll just be some elementary harmonic analysis.

Recall that if G is a locally compact [Hausdorff] group, then you get Haar measures. There are two of them, μ^l_G and μ^r_G, the left and right invariant Haar measures. Each up them is unique up to $\mathrm{R}^\times_{>0}$.[22]

Then there's Weil's formula for manifolds. If you have a fibration $F \subset X$ over B, you can integrate over the fibers and then over the base in order to integrate over X. So the formula looks like this. If $H \trianglelefteq G$ is a closed, normal subgroup, then [23]

$$\int_{G/H} d\mu_{G/H}(\overline{x}) \int_H f(x\xi) d\mu_H(\xi) = \int_G f(x) d\mu_G(x).$$

So we can just write

$$d\mu_G = d\mu_{G/H} d\mu_H.$$

Check out Weil's *Integration on locally compact groups*. And there's a Bourbaki course on it, too.

On to normalization of measures.

1. If G is compact, set $\mu_G(G) = 1$.
2. If G is discrete, set $\mu_G(\{P\}) = 1$.

Suppose we have

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_N = \{1\}$$

where each H_i/H_{i+1} is either compact or discrete. [Assume everthing is abelian.] Then we normalize $d\mu_G$ by this sequence.

Unfortunately, normalizing with respect to different filtrations can give you different measures.

[22] Actually, we'll probably be dealing just with abelian groups for some time to come.
[23] Assume everything in sight is nice and integrable, measurable, whatever.

Lemma $G \supseteq H \supseteq \{1\}$, $G \supseteq H' \supseteq \{1\}$ corresponding to μ and μ'. Then

1. If H, H' compact, G/H, G/H' discrete, then $\mu'_G = [H : H']\mu G$. [Since $HH' \supset H$ and $H \supset H \cap H'$ are discrete and compact, the index is finite. We set $[H : H'] = \frac{[H:H\cap H']}{H':H\cap H']}$.
2. H, H' discrete and G/H, G/H' compact, then $\mu'_G = [H : H']^{-1}\mu_G$.
3. H, G/H' compact; then the others are discrete, and $\mu'_G = \frac{[H\cap H':1]}{[G:HH']^{-1}}\mu_G$.

For instance, to prove the first we'd write

$$\begin{aligned}
\mu'_G(H) &= [H : H \cap H'] \cdot \mu'_G(H \cap H') \\
\mu'_G(H \cap H') &= [H' : H \cap H']^{-1}\mu'_G(H') \\
\mu'_G(H) &= [H : H'].
\end{aligned}$$

The others are left as exercises, but they're pretty much the same.

Fourier inversion [For locally compact abelian groups.] We've got a group G and a dual group $\widehat{G}$ of continuous homomorphisms $G \to \mathbb{C}_1^\times$. Suppose there's a map $e^{\langle x,\widehat{x}\rangle} : G\times\widehat{G} \to \mathbb{C}_1^\times$. So if $f \in L^1(G)$, then we can take its Fourier transform

$$\widehat{f}(x) = \int f(x)e^{-2\pi i\langle x,\widehat{x}\rangle}d\mu_G(x).$$

We can invert the Fourier transform via

$$f(x) = \int_{\widehat{G}} \widehat{f}(\widehat{x})e^{2\pi i\langle x,\widehat{x}\rangle}d\mu_{\widehat{G}}(\widehat{x}).$$

We're working with the Poisson summation formula. Let G be locally compact (Hausdorff) abelian group, and $H \subseteq G$ a closed subgroup. Define the dual as the set of [unitary] characters $\widehat{G} = \mathrm{Hom}_{\mathrm{cont}}(G, \mathrm{C}_1^\times)$; then there's an isomorphism $G \stackrel{\cong}{\to} \widehat{\widehat{G}}$. Pontryagin duality gives $G \times \widehat{G} \to \mathrm{C}_1^\times$. The inclusion $H \hookrightarrow G$ induces a map of characters $\widehat{G} \to \widehat{H}$.[24] What is $\ker \widehat{G} \to \widehat{H}$? It's just $H^\perp$. And the duality statement says that

$$\widehat{G}/H^\perp \stackrel{\cong}{\to} \widehat{H}.$$

Here, $H^\perp$ is the unitary characters trivial on H. And we can induce to the quotient;

$$H^\perp \stackrel{\cong}{\to} \widehat{G/H}.$$

G compact $\iff$ $\widehat{G}$ discrete. How do you see that? For instance, if G is discrete, what's the topology of $\widehat{G}$? Need to know the natural topology on the homomorphisms. It's the compact-open; an open subset of one consists of all those unitary characters mapping a fixed neighborhood into a fixed open neighborhood of $\mathrm{C}_1^\times$. More precisely, if $U \subseteq G$, a neighborhood of 1 would be $\{\chi : |\chi(U) - 1| < \epsilon\}$.

By duality, G discrete $\iff$ $\widehat{G}$ is compact. Of course, $\widehat{G} \hookrightarrow \prod_{g \in G}\{z : |z| = 1\}$; and by Tychonoff's theorem, it's compact.

This isn't a completely self-contained exposition; the curious student is invited to look at Weil, *Integration on locally compact abelian groups.*

Hmm. Correction of statement made last time. $\mathrm{A}_K^\times \hookrightarrow \mathrm{A}_K \times \mathrm{A}_K$ is closed. If you look at the first projection onto A_K, you get an immersion $\mathrm{A}_K^\times \hookrightarrow \mathrm{A}_K$ which is neither closed nor open. But the induced topology on $\mathrm{A}_K^\times$ is still the right one. When you want to look at topological properties of the ideles, it's still better to use this closed immersion; don't bother projecting back down.

We define a Fourier transform

$$\widehat{f}(\widehat{x}) = \int_G f(x)\langle x, \widehat{x}\rangle dx.$$

A function on G becomes a function on $\widehat{G}$. Classically, you have a duality $\mathrm{R} \times \mathrm{R} \to \mathrm{C}_1^\times$, $(x, y) \mapsto e^{-2\pi i x y}$.

Duality tells us that $\widehat{\mathrm{R}^n} = \mathrm{R}^n$, $\widehat{\mathrm{Z}^n} = (\mathrm{R}/\mathrm{Z})^n$.

[24] There's a little bit of confusion in notation. We'll say our characters are unitary; continuous maps $G \to \mathrm{C}_1^\times$. We'll reserve the term quasicharacters for $G \to \mathrm{C}^\times$.

Let's ponder the classical Poisson summation formula. It says that if $f \in \mathcal{S}(\mathrm{R})$, a Schwarz[25] function on R, then

$$\sum_{a\in\mathbb{Z}} f(a) = \sum_{a\in\mathbb{Z}} \widehat{f}(a).$$

How do we generalize this? We've got Z a subgroup of R. The copy of Z on the left is just coincidentally the same thing; think of it as a subgroup of $\widehat{\mathrm{R}}$. So the Poisson summation formula, properly generalized, is

$$\int_H f(\xi)d\mu_H(\xi) = \int_{H^\perp} \widehat{f}(\widehat{\eta})d\mu_{H^\perp}(\widehat{\eta}).$$

This makes sense if $f \in L^1(G) \cap C(G)$ a continuous integrable function; and we want $\widehat{f} \in L^1(\widehat{G}) \cap C(\widehat{G})$. We also want $f|_H \in L^1(H)$, and $\widehat{f}|_{H^\perp} \in L^1(H^\perp)$.

In proving classical case, you lean on $\sum_{a\in\mathbb{Z}} f(x+a)$. So here, the right thing to do is $F(\overline{x}) = \int_H f(x\xi)d\mu_H(\xi)$, $F \in L^1(G/H) \cap C(G?H)$. We apply harmonic analysis, or whatever. So then [remember $\widehat{\eta} \in H^\perp$]

$$\begin{aligned}
\widehat{F}(\widehat{\eta}) &= \int_{G/H} F(\overline{x})\langle \overline{x}, \widehat{\eta}\rangle d\mu_{G/H}(\overline{x}) \\
&= \int_{G/H} d\mu_{G/H}(\overline{x}) \int_H f(x\xi)\langle \overline{x}, \widehat{\eta}\rangle d\mu_H(\xi) \text{ Fubini!} \\
&= \int_G f(x)\langle x, \widehat{\eta}\rangle d\mu_G(x). \\
&= \widehat{f}(\widehat{\eta}).
\end{aligned}$$

Normalize so that $d\mu_G = d\mu_{G/H} d\mu_H$.

Fourier inverison for G/H works like this. Want $d\mu_{H^\perp} \overset{\text{dual}}{\leftrightarrow} d\mu_{G/H}$. In the situation above, we know that

$$\widehat{\widehat{F}}(\overline{x}) = F(\overline{x}^{-1}).$$

Actually, just need $\widehat{\widehat{F}}(1) = F(1)$, and that's the Poisson summation formula.

[25] Nice!

Normalize; $d\mu_{\widehat{G}} = d\mu_{\widehat{G}/H^\perp} d\mu_{H^\perp}$. But $\widehat{G}/H^\perp = \widehat{H}$; and so pick $d\mu_{\widehat{G}/H^\perp} \overset{\text{dual}}{!} d\mu_H$.

With this normalization we can run the Poisson summation formula backwards; and get

$$\int_{H^\perp} \widehat{f}(\widehat{\eta}) d\mu_{H^\perp}(\widehat{\eta}) = \int_H \widehat{\widehat{f}}(\xi) d\mu_H(\xi) \int_G f(x) d\mu_G(x).$$

Conclusion: if $d\mu_{H^\perp}$ is dual to $d\mu_{G/H}$, and $d\mu_H$ is dual to $d\mu_{\widehat{G}/H^\perp}$, then $d\mu_{G/H} d\mu_H$ is dual to $d\mu_{\widehat{G}/H^\perp} d\mu_{H^\perp}$; and these are $d\mu_G$ and $d\mu_{\widehat{G}}$, respectively.

We'll apply this sort of thing to the following situation. There's a diagonal embedding $K \hookrightarrow \mathbb{A}_K$. Let these be H and G, respectively, and apply Poisson summation. Then it'll turn out that the dual of K is [canonically] K, and you get a Poisson summation formula. You get some function on the adelic space, take its Fourier transform, and if you sum over K values of f, that's the same as $\sum_{a \in K} \widehat{f}(a)$. That's a crucial part of Tate's thesis.

Incidentally, our goal in all of this is to understand Tate's method for ζ and L-functions, and functional equations. The idea is to analyze everything locally. He defines local zeta functions, and local functional equation. That'll be pretty elementary analysis. No surprises. But we do it in such a way as to extract local L-factors and local ϵ-factors. [Some people would call the ϵ-factor the local root number.] And then the global functional equation follows. Possibly nobody completely understands the global equation; it's magic. In some sense, the key is the Poisson summation formula. This is sort of like the Riemann-Roch theorem for number fields.

What is automorphicity? It means that it comes from, well, anything automorphic will be fine. This comes from some motive, in this case abelian motive, and that's why it satisfies it. But we don't really understand why the functional equation holds.

Enough philosophy. Let's do some math.

Normalization of measures This should be in quotes, I guess, since technically it's not absolutely necessary. But it's sort of nice to have around. We have K a local field. Assume it's a finite extension of $\mathbb{Q}_p$. There are two possibilities; it's archimedean or it ain't, depending on whether p is finite or ∞. . We'll define a pairing $\Lambda : K \times K \to \mathbb{C}_1^\times$ so that K is identified with its Pontryagin dual. It's given by

$$\pm \exp(\pm 2\pi\sqrt{-1}\,\mathrm{tr}_{K,\mathbb{Q}_p}) \qquad \begin{cases} + & p \text{ finite} \\ - & p = \infty \end{cases} .$$

If K is archimedean, then it's $\mathbb{R}$ or $\mathbb{C}$, and we're not doing anything. Then $\Lambda(x) = -x$ if $K \cong \mathbb{R}$, and $\Lambda(z) = -(z + \overline{z})$ if $K = \mathbb{C}$.

$$\begin{tikzcd} K \times K \arrow[r] \arrow[dr, "\Lambda"'] & \mathbb{R}/\mathbb{Z} \arrow[d, "\exp(2\pi\sqrt{-1}\cdot)"] \\ & \mathbb{C}_1^\times \end{tikzcd}$$

If K is nonarchimedean, then we have $\mathrm{tr}_{K,\mathbb{Q}_p}(x) \in \mathbb{Q}_p$; and we can write it as $x_1 + x_2$ with $x_1 \in \mathbb{Z}[\frac{1}{p}]$, and $x_2 \in \mathbb{Z}_p$. This is a sort of partial fraction decomposition; the fractional part and the integral part. This is nonunique; both are determined up to rational integers. So anyways, the trace is $\exp(2\pi\sqrt{-1}x_1)$; the indeterminacy is in $\mathbb{Z}$.

Oops. We've been writing Λ as a function of just one thing. Well, the pairing is $K \times K \to K \to \mathbb{C}_1^\times$ via $(a, b) \mapsto ab \mapsto \Lambda(ab)$.

Why do we bother with this + and − nonsense? Well, you want to use the local formula to define a global formula; and this is the only way it will work. For this gives you a pairing $\mathbb{A}_K \times \mathbb{A}_K \to \mathbb{C}_1^\times$. If $x = (x_p)$, then we set $\Lambda(x) = \prod_p \Lambda(x_p)$.[26] So why the $\pm$ stuff? Well, for all $x \in K$, $\Lambda(x) = 1$.

$$\begin{aligned}\Lambda(x) &= \prod_{p \text{ finite}} \exp(2\pi\sqrt{-1}\,\mathrm{tr}_{K,\mathbb{Q}}(x))^{[K:\mathbb{Q}} \cdot \prod_{p=\infty} \exp(-2\pi\sqrt{-1}\,\mathrm{tr}_{K,\mathbb{Q}}(x))^{[K:\mathbb{Q}} \\ &= 1.\end{aligned}$$

Well, $\mathrm{tr}_{K,\mathbb{Q}}(x)_p$ is a rational number. Write $r = \sum r_p + n$ for some integer n and $r_p \in \mathbb{Z}[\frac{1}{p}]$. When all's said and done, you get $\exp(2\pi\sqrt{-1}r)$.

Uh-oh. Notes are going to be a bit garbled for today; sorry.

We're using

$$\sum_{v|p} \mathrm{tr}_{K_v,\mathbb{Q}_p}(x) = \mathrm{tr}_{K,\mathbb{Q}}(x).$$

So then we can compute

$$\Lambda_K(x) = \prod_v \Lambda_K(x_v).$$

So $\Lambda(x) = 1$, since $\Lambda_K(x) = \Lambda_{\mathbb{Q}}(\mathrm{tr}_{K,\mathbb{Q}}(x))$.

Moving right along...

$$\begin{aligned}\mathbb{A}_K \times \mathbb{A}_K &\to \mathbb{C}_1^\times \\ (x,y) &\mapsto \Lambda(xy).\end{aligned}$$

Now, if x is a global element, and y is another one, then $(x,y) \mapsto 1$. So we know that $K^\perp \supseteq K$. We'll see that equality holds.

Now consider $K/\mathbb{Q}_p$, p finite. We've got $\mathcal{O} \subseteq K$. $\mathcal{O}$ is compact, and $K/\mathcal{O}$ is discrete. We know a way to put a Haar measure on it; μ'_K, with $\mu'_K(\mathcal{O}) = 1$. We know that

[26] Can do this, since $\Lambda(x_p) = 1$ except for finitely many of them.

$$\begin{aligned}\mathcal{O}^\perp &= \{x \in K : \Lambda(xy) = 1 \forall y \in \mathcal{O}\}\\ &= \{x \in K : \mathrm{tr}_{K,\mathbb{Q}_p}(xy) \in \mathbb{Z}_p \forall y \in \mathcal{O}_K\}\\ &= \mathcal{D}^{-1}_{K,\mathbb{Q}_p}.\end{aligned}$$

What is the dual measure of μ'_K? It has the property that $\mu_K^{\mathrm{dual}}(\mathcal{D}^{-1}_{K,\mathbb{Q}_p}) = 1$. Well, we know that

$$\mu'_K(\mathcal{D}^{-1}_{K,\mathbb{Q}_p}) = \mathrm{N}\mathcal{D}_{K,\mathbb{Q}_p}$$

In a finite residue field situation, we say that $\mathrm{N}(\mathfrak{P}) = \#(\mathcal{O}/\mathfrak{P})$. Anyways, we're not yet self dual; gotta normalize. Set

$$\mu_K = (\mathrm{N}\mathcal{D}_{K,\mathbb{Q}_p})^{-\frac{1}{2}} \cdot \mu'_K.$$

And this is indeed self-dual with respect to Λ. And very often people prefer to use this measure. We know that the naive measure is self-dual $\iff$ K is unramified over $\mathbb{Q}_p$.

Theorem $\mathbb{A}_K/K$ is compact.

Proof $\mathbb{A}_K = \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} K$. That's since $K \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{v|p} K_v$; simply pick a $\mathbb{Q}$-basis $x_1, \cdots, x_n$ for K. This condition holds locally; want to see if it holds globally.

Now, $\mathcal{O}_K \otimes \mathbb{Z}_p = \prod_{v|p} O_{K_v}$ for p finite. Pick a $\mathbb{Q}$ basis $x_1, \cdots, x_n$ of K. Then for $x = (x_p) \in \mathbb{A}_{\mathbb{Q}}$, we see that $x \otimes x_i \in \mathbb{A}_K$. But this should be clear from our discussion; for all but finitely many v's, all these global elements are in $\mathcal{O}_{K_v}$.

Similarly for the other inclusion. We now know that $\mathbb{A}_K = \mathbb{A}_{\mathbb{Q}} \otimes K$.

So now we look at $\mathbb{A}_K/K$. Well, $K = \mathbb{Q} \otimes K$.[27] So

$$\mathbb{A}_K/K \cong (\mathbb{A}_{\mathbb{Q}}/\mathbb{Q})^{[K:\mathbb{Q}]}$$

since $\otimes$ is right exact. As commutative locally compact groups, these two are isomorphic. Therefore, it suffices to prove that $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact.

[27] All tensors are over $\mathbb{Q}$.

Theorem K a numberfield $\Rightarrow \mathbb{A}_K/K$ is compact.

Proof We've reduced to $K = \mathbb{Q}$, since $\mathbb{A}_K/K$ is homeomorphic to $(\mathbb{A}_\mathbb{Q}/\mathbb{Q})^{\oplus[K:\mathbb{Q}}$ as topological groups. We know that there's a surjection $\mathbb{A}_\mathbb{Q} \rightharpoonup \mathbb{A}_\mathbb{Q}/\mathbb{Q}$. We write down a compact subset $V \subseteq \mathbb{A}_\mathbb{Q}$ which surjects onto $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$. Set

$$V = \{(x_p) : 0 \le x_\infty \le 1, x_p \in \mathbb{Z}_p\}.$$

This is certainly compact. Now, for any $x = (x_p) \in \mathbb{A}_\mathbb{Q}$, we want to show that we can translate by an element of $\mathbb{Q}$ so that the thing winds up in V. For (x_p), there's a finite set S so that for every $p \notin S$, $x_p \in \mathbb{Z}_p$. We may assume $\infty \in S$. Let $S = \{p_1, \cdots, p_n = \infty\}$. We want an element $y \in \mathbb{Q}$ so that $\|x_{p_i} - y\| \le 1$, and $y \in \mathbb{Z}_p$ for all $p \notin S$. But this is no problem. Each x_{p_i} has a partial fraction decomposition. Write $x_{p_i} = u_i + v_i$, with $v_i \in \mathbb{Z}_p$ and $u_i \in \mathbb{Z}[\frac{1}{p}]$. First, let's try $y_1 = \sum_{i=1}^{n-1} u_i$. Then $x_p - y_1 \in \mathbb{Z}_p$ for every $p \neq \infty$. So $x - y_1 \in (\prod_p \mathbb{Z}_p) \times \mathbb{R}$. There's an integer $m \in \mathbb{Z}$ so that $0 < x_\infty - y_1 - m < 1$. So take $y = y_1 + m$; this works.$\diamond$

Remark We've shown that $V = \{x = (x_p) : 0 \le x_\infty < 1, \|x_p\| \le 1\}$ is in fact a fundamental domain for $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$. [We've seen that $V + \mathbb{Q} = \mathbb{A}_\mathbb{Q}$. And $V \cap \mathbb{Q} = \{0\}$.]

Exercises

1. Prove that $\mathbb{A}_K/K$ is compact if K is a global function field.
2. As before, we define μ_v the self-dual Haar measure on K_v with respect to the trace $\mathrm{tr}_{K_v,\mathbb{Q}_p}$. If v is finite, then $\mu_v(\mathcal{O}_v) = (\mathrm{N}\mathcal{D}_v)^{-\frac{1}{2}}$. If $\infty | v$, then $\mu_v = \begin{cases} dx \\ |dz \wedge d\bar{z}| = 2dxdy \end{cases}$. Take $\mu = \prod_v \mu_v$. This gives you a Haar measure on $\mathbb{A}_K$. The exercise is, compute $\mu(\mathbb{A}_K/K)$, the volume of the fundamental domain.
3. Do (2) for global function field. What you're actually computing here is, essentially, the genus.

Recall that $\mathbb{A}_{K,1}^\times$ is the ideles of norm 1; and $\mathbb{A}_{K,1}^\times \supseteq K^\times$, by the product formula.

Theorem $\mathbb{A}_{K,1}^\times/K^\times$ is compact.

Corollary *Finiteness of class number.*

Proof [cor] Look at $I_K = \oplus_{v \text{ finite}} \mathbb{Z}$, the group of invertible ideals of O_K. Look at $I_K/(\text{principal ideals})$; this is finite. That's what we want to show. Well, look at

$$\begin{aligned} \alpha : \mathbb{A}_K^\times &\to I_K \\ x = (x_v) &\mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}(x_{\mathfrak{p}})}. \end{aligned}$$

This is clearly surjective. What's the kernel? It's the product of the local kernels; so it's $(\prod_{\mathfrak{p}} \mathcal{O}_v^\times) \times \prod_{v|\infty} K_v^\times$. Thus, $I_K/(\text{principal ideals})$, or the ideal class group of K, is isomorphic to $\mathbb{A}_K^\times/(\ker(\alpha) \cdot K^\times)$. The top sequence is exact in

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & K^\times \arrow[r] \arrow[d, "\cong"'] & \mathbb{A}_{K,1}^\times \arrow[r] \arrow[d] & \mathbb{A}_{K,1}^\times/K^\times \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & K^\times \arrow[r] & \mathbb{A}_K^\times \arrow[r] \arrow[d, "\|\cdot\|"'] & \mathbb{A}_K^\times/K^\times \arrow[r] \arrow[d, "\|\cdot\|"'] & 1 \\
 & & \mathbb{R}_{>0}^\times \arrow[r, "="] \arrow[d] & \mathbb{R}_{>0}^\times \arrow[d] & \\
 & & 1 & 1 &
\end{tikzcd}$$

So we actually get

$$\frac{\mathbb{A}_{K,1}^\times}{K^\times((\prod_{v|\infty} K_v^\times)_1 \times \prod_v \mathcal{O}_v^\times)} \overset{\cong}{\to} \frac{\mathbb{A}_K^\times}{K^\times \cdot \prod_{v|\infty} K_v^\times \prod_v \mathcal{O}_v^\times}.$$

Now,

$$(\prod_{v|\infty} K_v^\times)_1 \times \prod_{v \text{ finite}} \mathcal{O}_v^\times \subseteq \mathbb{A}_{K,1}^\times$$

is actually an open subgroup. $\ker\alpha$ is open. So α is continuous, if you regard the target as a disrete group. Now, the thing just written above is that open subgroup intersected with the unit ideles. The thing on the right, two lines above, is the ideal class group. And we've realized this as the quotient of the unit idele class group by some open subgroup of it. But what do we know about this? We know that the unit idele class group is compact. So it's a compact group mod an open subgroup. So the result is a discrete group. So it's finite, and this proves the finitude of the class number.

Next time, we'll prove the theorem and deduce the Dirichlet unit theorem.

We'll also do local functional equations. That'll require a little bit of analysis, some of which we hint at here.

Let $K = K_v$, a completion of a number field. Let f be a nice function. We'll integrate it against a quasicharacter of K, $f(x)\chi(x)$. A quasicharacter is a map $\chi : K^\times \to \mathbb{C}^\times$. We think of them as variables; they correspond to a complex variable s. For we can think of it as a real, live unitary charcter $\chi_1(x) \cdot \|\cdot\|^s$; as you vary s, you get a family of quasicharacters, and that's your variable. We'll look at

$$\int_{K^\times} f(x)\chi(x)d^\times x.$$

We'll take a Fourier transform and relate it so something else, dividing by local L-factors

$$\frac{\int_{K^\times} \widehat{f}_\psi(x)(\|\cdot\|\,\chi)^{-1}(x)d^\times x}{L(\|\cdot\|\,\chi^{-1})} = \epsilon(\chi, \psi, dx)\frac{\int_{K^\times} f(x)\chi(x)d^\times x}{L(\chi)}.$$

Here, $\psi : (K, +) \to \mathbb{C}_1^\times$, and

$$L(\chi) = \begin{cases} v \text{ nonarchimedean} & \begin{cases} (1-\chi(\pi))^{-1} & \chi \text{ unramified} \\ 1 & \chi \text{ ramified} \end{cases} \\ v \text{ archimedean} & \Gamma_{\mathbb{R}}(\chi) \text{ or } \Gamma_{\mathbb{C}}(\chi) \end{cases}.$$

Theorem $\mathbb{A}_{K,1}^\times/K^\times$ is compact.

Remember that we have $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$.

Lemma [Minkowski] $V_1 \stackrel{\text{def}}{=} \{x = (x_v) \in \mathbb{A}_K : \|x_v\| \le 1\}$.[28] Let μ be a Haar measure on $\mathbb{A}_K$, say, the normalized one. There's a constant $c > 0$ so that for all $x \in \mathbb{A}_K^\times$ with $\|x\| \ge c$, theres an $a \in K^\times \cap xV_1$.

Proof Let $y = (y_v)$ be such that

$$y_v = \begin{cases} 1 & v \text{ finite} \\ \frac{1}{2} & v|\infty \end{cases}.$$

Think about yV_1. Ask whether $yxV_1 + a$, $a \in K$, are disjoint. If so, then $\mu(yxV_1) < \mu(\mathbb{A}_K/K)$; the volume is less than that of the fundamental domain. So if $\|x\| \cdot 2^{-[K:\mathbb{Q}]}\mu(V_1) \ge \mu(\mathbb{A}_K/K)$, then you can find $a_1, a_2 \in K$ so that $(yxV_1 + a_1) \cap (yxV_1 + a_2) \ne \emptyset$. So $yxV_1 - yxV_1 \cap K^\times \ne \emptyset$. But $yxV_1 - yxV_1 \subseteq xV_1$. So take $c = 2^{[K:\mathbb{Q}]}\frac{\mu(\mathbb{A}_K/K)}{\mu(V_1)}$.$\diamond$

This is the crucial result about finding global elements.

Proof [of theorem] We want to find a compact set $X \subseteq \mathbb{A}_{K,1}^\times$ so that $\iota : X \hookrightarrow \mathbb{A}_{K,1}^\times/K^\times$ is surjective. Well, what does it mean to say that X is compact? Well, we know that $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$ via $x \mapsto (x, x^{-1})$. So we have to show that X is in a compact set of $\mathbb{A}_K$, and if you invert every element it is again contained in a compact set.

Start with any $x \in \mathbb{A}_{K,1}^\times$. Fix an element $z_0 \in \mathbb{A}_K^\times$ whose norm is large; $\|z_0\| > c$, where the c is the constant from the lemma. Then there's an $a \in K^\times \cap z_0xV_1$. There's also a $b \in K^\times \cap z_0x^{-1}V_1$.[29] So we know that $ab \in z_0^2V_1$.[30] So a and b^{-1} really aren't very far away from each other. Actually, $ab \in z_0^2V_1 \cap K$, the intersection of a compact set with a discrete one. So $z_0^2V_1 \cap K = \{c_1, \cdots, c_n\}$.

We know that $ax^{-1} \in z_0V_1$. And $(ax^{-1})^{-1} = a^{-1}x$. We'll translate x by a^{-1}; want to show that $a^{-1}x$ and its inverse both lie in some fixed compact set. If we can do that then we'll win. Well, $a^{-1}x = (ab)^{-1}bx \in \cup_{i=1}^n c_i^{-1}z_0V_1$.

So now we've shown that for all $x \in \mathbb{A}_{K,1}^\times$, there's an $a \in K^\times$ so that $a^{-1}x \in \iota^{-1}((\cup_{i=1}^n c_i^{-1}z_0V_1) \times (z_0V_1)) = X$ *compact.*

[28] Clearly this is compact, as the product of compact sets.
[29] z_0x takes the role of x in the lemma's notation.
[30] Using the fact that the product of a pair of elements in V_1 is in V_1.

Corollary Let S be a finite set of primes containing all infinite places. Let $\mathbb{A}_{K,S}^\times = \{x = (x_v) \in \mathbb{A}_K^\times : \|x_v\| = 1 \forall v \notin S\}$. The S-units are $\mathcal{O}_{K,S}^\times = K^\times \cap \mathbb{A}_{K,S}^\times$.[31] This is a finitely generated abelian group of rank $\#S - 1$. When $S = S_\infty$, this is the classical Dirichlet unit theorem.

Proof

$$\begin{tikzcd}[arrows=dash]
 & & \mathbb{A}_{K,1}^\times \cap K^\times \mathbb{A}_{K,1} \arrow[dl] \arrow[dr] & \\
 & K^\times \mathbb{A}_{K,\emptyset}^\times \arrow[dl] \arrow[dr] & & \mathbb{A}_{K,1}^\times \cap \mathbb{A}_{K,S}^\times \arrow[dl] \\
K^\times \arrow[dr] & & \mathcal{O}_{K,S}^\times \mathbb{A}_{K,\emptyset}^\times \arrow[dl] \arrow[dr] & \\
 & \mathcal{O}_{K,S}^\times \arrow[dr] & & \mathbb{A}_{K,\emptyset}^\times \arrow[dl] \\
 & & \mu_K. &
\end{tikzcd}$$

Let r_1 be the number of real embeddings, r_2 the number of complex embeddings, $r = r_1 + r_2 = \#S_\infty$. Note that $\mathbb{A}_{K,S}^\times / \mathbb{A}_{K,\emptyset} = {\mathbb{R}_{>0}^\times}^{r_1+r_2} \mathbb{Z}^{s-r_1-r_2}$.

Similarly, $\frac{\mathbb{A}_{K,1}^\times \cap \mathbb{A}_{K,S}^\times}{\mathbb{A}_{K,\emptyset}} = {\mathbb{R}_{>0}^\times}^{r_1+r_2-1} \mathbb{Z}^{s-r_1-r_2}$.

So $\mathcal{O}_{K,S}^\times / \mu_K \cong$ a cocompact discrete subgroup in that thing. And we know its rank; it's isomorphic to $\mathbb{Z}^{s-1}$; it has to take out the discrete part, and give you a discrete cocompact subgroup of ${\mathbb{R}_{>0}^\times}^{r_1+r_2-1}$.

[31] $\mathcal{O}_{K,S} = \{x = (x_v) \in \mathbb{A}_K : \|x_v\| \le 1 \forall v \notin S\}$.

Tate's thesis We start by defining local L-factors. $K = K_v$ a finite extension of $\mathbb{Q}_p$.[32]

For every quasicharacter $\chi : K^\times \to \mathbb{C}^\times$, well, there's a special one $\omega_s : K^s \to \mathbb{C}^\times$ by $x \mapsto \|x\|^s$. We can break the characters into equivalence classes, translates by ω_s.[33] Define $L(\chi)$ in the following way.

1. $x : K \overset{\cong}{\to} \mathbb{R}$. Every quasicharacter can be written as $x^{-N}\omega_s$ for $N \in \{0, 1\}$. Set

$$\begin{aligned} L(x^{-N}\omega_s) &= \Gamma_{\mathbb{R}}(s) \\ &\overset{\text{def}}{=} \pi^{\frac{s}{2}}\Gamma(\frac{s}{2}). \end{aligned}$$

[34]

[32] Ongoing exercise; verify everything we do for function fields as well.

[33] χ_1 and χ_2 are equivalent if there's an $s \in \mathbb{C}$ so that $\chi_1 = \chi_2 \cdot \omega_s$; $\{\chi_0\omega_s\}$ is one equivalence clas.

[34] Quick review of Gamma functions. Well,

$$\begin{aligned} \Gamma(s) &= \int_0^\infty e^{-t}t^{s-1}dt \\ &= \int_{\mathbb{R}^\times_{>0}} e^{-t}t^s d^\times t \end{aligned}$$

Absolutely convergent for $\Re(s) > 0$. Otherwise, you analytically continue with the functional equation. Some basic properties:

$$\begin{aligned} \Gamma(s+1) &= s\Gamma(s) && (1) \\ \Gamma(s)\Gamma(1-s) &= \frac{s}{\sin \pi s} && (2) \\ 2^{2s-1}\Gamma(s)\Gamma(s+\frac{1}{2}) &= \sqrt{\pi}\Gamma(2s) && (3) \\ & && (4) \end{aligned}$$

There are some variants of it:

$$\begin{aligned} \Gamma_{\mathbb{R}}(s) &= \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2}) \\ \Gamma_{\mathbb{C}}(s) &= 2(2\pi)^{-s}\Gamma(s) \\ &\overset{(3)}{=} \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1). \end{aligned}$$

2. $K \cong \mathbb{C}$. We have $z : K \hookrightarrow \mathbb{C}$ canonical mod $\mathbb{R}$. Then we write $\chi = z^{-N}\omega_s$ with $N \geq 0$. Then set

$$L(\chi) = L(z^{-N}\omega_s) = \Gamma_{\mathbb{C}}(s).$$

   Note that $L(z^{-N}\omega_s) = L(\overline{z}^{-N}\omega_s)$, so it doesn't matter which embedding we pick.

3. K nonarchimedean. A character's unramified if it's trivial on units. Then set

$$L(\chi) = \begin{cases} (1-\chi(\pi))^{-1} & \chi \text{ unramified} \\ 1 & \chi \text{ ramified} \end{cases}.$$

   The ramified 1 is since we have a 1-dimensional abelian thing. $(1-\chi(s))^{-1}$ is essentially $(1-\mathrm{N}\mathfrak{p}^{-s})^{-1}$.

Let dx be a Haar measure on $(K,+)$. Then set $d^\times x$ to be a Haar measure on $K^\times$, e.g., $\frac{dx}{\|x\|}$. Suppose we have $\psi : (K,+) \to \mathbb{C}_1^\times$ a nontrivial additive character. Then we can identify K with its Pontryagin dual; there's an isomorphism $K \to \mathrm{Hom}(K, \mathbb{C}_1^\times)$. We have a Fourier transform running around,

$$\widehat{f}_{\psi,dx}(y) \stackrel{\text{def}}{=} \int f(x)\psi(xy)dx.$$

Proposition f, g functions on K, satisfying some nice properties. Like maybe they have compact support or something. Let χ be a quasi-character, and think of $\widehat{\chi} = \omega\chi^{-1}$, where $\omega = \omega_1$.

$$\int_{K^\times} f(x)\chi(x)d^\times x \int_{K^\times} \widehat{g}(x)\widehat{\chi}(x)d^\times x = \int_{K^\times} \widehat{f}(x)\widehat{\chi}(x)d^\times x \int_{K^\times} g(x)\chi(x)d^\times x.$$

Here, all the Fourier transforms are respect to some ψ and Haar measure dx. Doesn't matter what they are, but you better keep 'em the same all the way.

Typically, we define

$$\zeta(f,\chi) = \int_{K^\times} f(x)\chi(x)d^\times x.$$

Then the proposition says that

$$\zeta(f,\chi)\zeta(\widehat{g},\widehat{\chi}) = \zeta(\widehat{f},\widehat{\chi})\zeta(g,\chi).$$

Remember that χ is, so to speak, a variable; that's why it's a zeta function.

Proof

$$\begin{aligned}
\int_{K^\times} f(x)\chi(x)d^\times x \cdot \int_{K^\times} \widehat{g}(y)\,\|y\| \cdot \chi(y)^{-1}d^\times y &= Blah. \\
\widehat{g}(y) &= \int_K g(z)\psi(zy)dz \\
\int_{K^\times} f(x)\chi(x)d^\times x \cdot \int_{K^\times} \widehat{g}(y)\,\|y\| \cdot \chi(y)^{-1}d^\times y &= \int_K \int_{K^\times \times K^\times} \int \psi(zy)f(x)g(z)\,\|y\|\,\chi(x)\chi(y^{-1})d^\times x d^\times y dz \\
zy &= w \\
dw &= \|y\|\,dz \\
Blah &= \int_K \psi(w)dw \int\int_{K^\times \times K^\times} f(x)g(wy^{-1})\chi(x)\chi(y^{-1})d^\times x d^\times y \\
u &= wy^{-1} \\
Blah &= \int_K \psi(w)\chi(w)^{-1}dw \int\int_{K^\times \times^\times} f(x)g(u)\chi(x)\chi(u)d^\times x d^\times u
\end{aligned}$$

And this might prove it; and it's certainly as much as any of us feels like doing right now.

Anyways, this equality for local zeta functions holds whenever it makes sense, i.e., things are integrable, etc. It tells us that $\zeta(f,\chi)/\zeta(\widehat{f},\widehat{\chi})$ depends only on χ. Anyways, we[?] now know that

$$\frac{\zeta(\widehat{f}_\psi,\widehat{\chi})}{L(\widehat{\chi})} = \epsilon(\chi,\psi,dx)\frac{\zeta(f,\chi)}{L(\chi)}$$

the local functional equation.

Local functional equation We have dx a Haar measure on $(K,+)$; $\psi : (K,+) \to \mathbb{C}_1^\times$ a nontrivial character. We also have $d^\times x$ a Haar measure on $K^\times$.[35] We compute Fourier transforms with this character and measure, and get

$$\frac{\int_{K^\times} \widehat{f}_\psi \cdot \omega\chi^{-1}(x) d^\times x}{L(\omega\chi^{-1})} = \epsilon(\chi, \psi, dx) \frac{\int_{K^\times} f(x)\chi(x) d^\times x}{L(\chi)}.$$

Here, the ϵ is a sort of harmless constant. And experience tells us[36] that the definition of the L-factors is crucial.

There are some formal proprties of $\epsilon(\chi, \psi, dx)$:

1. For $a > 0$, $\epsilon(\chi, \psi, a dx) = a\epsilon(\chi, \psi, dx)$.
2. ψ is what we use to identify K with its dual. Note that $x \mapsto \psi(c \cdot x)$ is another character; and actually, every character must have that form. So

$$\epsilon(\chi, \psi(c\cdot)) = \chi(c) \|c\|^{-1} \epsilon(\chi, \psi, dx).$$

   To prove this, just look at the only place where ψ enters the computation; compute

$$\begin{aligned}
\widehat{f}_{\psi(c\cdot)}(x) &= \int_K f(y)\psi(cxy) dy \\
&= \widehat{f}_\psi(cx) \\
\int_{K^\times} \widehat{f}_\psi(cx)(\omega\chi^{-1})(x) d^\times x &= \int_{K^\times} \widehat{f}_\psi(z)(\omega\chi^{-1})(c^{-1}z) d^\times z \\
(\omega\chi^{-1})(c^{-1}z) &= \chi(c) \|c\|^{-1} \cdot \omega\chi^{-1}(z).
\end{aligned}$$

Computation of $\epsilon(\chi, \psi, dx)$ There are three cases to worry about.

1. $K \cong \mathbb{R}$. Then $\psi(x) = e^{2\pi\sqrt{-1}x}$. $\chi(x) = x^{-N} \|x\|_s$ with $N = 0$ or 1. For the Haar measure, let dx be the Lebesgue measure on $\mathbb{R}$. Then $L(\chi) = \Gamma_{\mathbb{R}}(s)$.

   If $N = 0$, then $\chi^{-1} = \omega_{-s}$; $\omega\chi^{-1} = \omega_{1-s}$. Then $L(\widehat{\chi}) = \Gamma_{\mathbb{R}}(1-s)$.[37]

[35] It looks like K is a local field.
[36] Well, Ching-Li, anyway
[37] Recall that $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$.

$$\begin{aligned}
f(x) &= e^{-\pi x^2}\\
\widehat{f}(x) &= \int_{\mathbb{R}} e^{-\pi y^2} e^{2\pi\sqrt{-1}yx} dy\\
&= \int_{\mathbb{R}} e^{-\pi(y-\sqrt{-1}x)^2} e^{-\pi x^2} dy\\
&= e^{-\pi x^2}\int_{\mathbb{R}} e^{-\pi y^2} dy \text{ by Cauchy's formula.}\\
(\int_{\mathbb{R}} e^{-\pi y^2} dy)^2 &= \int\int_{\mathbb{R}} e^{-\pi(x^2+y^2)} dxdy\\
&= \int\int e^{-\pi r^2} r dr d\theta\\
&= 2\pi(2\pi)^{-1}\int_0^\infty e^{-\pi r^2} d(\pi r^2)\\
&= 1.\\
\widehat{f}(x) &= e^{-\pi x^2}\\
&= f(x).
\end{aligned}$$

We have to compute two more serious integrals;

$$\begin{aligned}
\int_{\mathbb{R}^\times} e^{-\pi x^2} |x|^s d^\times x &= 2\int_0^\infty e^{-\pi x^2} x^{s-1} dx\\
\text{Choose } d^\times x &= \frac{dx}{|x|}\\
\text{Set } t &= x^2\\
2\int_0^\infty e^{-\pi x^2} x^{s-1} dx &= \int_0^\infty e^{-\pi t} t^{\frac{s}{2}-1} dt \text{ set } \pi t = u\\
&= \int_0^\infty e^{-u} (\pi^{-\frac{s}{2}} u^{\frac{s}{2}-1} du\\
&= \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\\
&= \Gamma_{\mathbb{R}}(s).
\end{aligned}$$

So much for that. We now lean on

$$\begin{aligned}
\int_{\mathbb{R}^\times} \widehat{f}(x)\widehat{\chi}(x) d^\times x &= \int_{\mathbb{R}^\times} e^{-\pi x^2}\omega_{1-s}(x) d^\times x\\
&= \Gamma_{\mathbb{R}}(1-s).
\end{aligned}$$

So in this case, with $N=0$, we conclude that $\epsilon(\chi,\psi,dx)=1$.

What about when $N=1$? Need to integrate against an odd Schwarz function. A natural choice is $g(x)=xe^{-\pi x^2}$. Can compute the Fourier transform with a trick, based on what we know about f.

$$\begin{aligned}
\frac{\partial}{\partial x}\widehat{f}(x) &= 2\pi\sqrt{-1}\int_{\mathbf{R}} ye^{-\pi y^2}e^{2\pi\sqrt{-1}yx}dy \\
\widehat{g}(x) &= \frac{1}{2\pi\sqrt{-1}} - 2\pi xe^{-\pi x^2} \\
&= \sqrt{-1}g(x).
\end{aligned}$$

Also,

$$\begin{aligned}
\int_{\mathbf{R}^\times} xe^{-\pi x^2}x^{-1}\left|x\right|^s d^\times x &= \int_{\mathbf{R}^\times} e^{-\pi x^2}\left|x\right|^s d^\times x \\
&= \Gamma_{\mathbf{R}}(s) \\
\widehat{\chi} &= \omega\chi^{-1}(x) \\
&= x\left|x\right|^{1-s} \\
&= x^{-1}\left|x\right|^{3-s} \\
L(\widehat{\chi}) &= \Gamma_{\mathbf{R}}(3-s) \\
\int_{\mathbf{R}^\times}\sqrt{-1}g(x) &= \int_{\mathbf{R}^\times}\sqrt{-1}xe^{-\pi x^2}x^{-1}\left|x\right|^{3-s}d^\times x \\
&= \sqrt{-1}\Gamma_{\mathbf{R}}(3-s).
\end{aligned}$$

The conclusion is that, for $N=1$, $\epsilon(\chi,\psi,dx)=\sqrt{-1}$. Note that this i came in when we computed the Fourier transform; so it comes from the $\sqrt{-1}$ in $e^{2\pi\sqrt{-1}x}$.

2. $z: K\hookrightarrow \mathbf{C}$. We fix an embedding $z: K\hookrightarrow\mathbf{C}$. Set $\psi(z)=e^{2\pi\sqrt{-1}\cdot 2\Re(z)}$. Then $\chi(z)=z^{-N}\omega_s$ for some $N\geq 0$. For $n\in\mathbf{N}$ define $f_n(z)=z^n e^{-2\pi(z\overline{z})}$. Choose as the Haar measure $\mu=|dz\wedge d\overline{z}|=2dxdy$. So compute the Fourier transform

$$\widehat{f_0}(z) = \int\int_{\mathbf{C}} e^{-2\pi(w\overline{w})}e^{2\pi\sqrt{-1}(zw+\overline{zw})}\left|dw\wedge d\overline{w}\right|.$$

Left as exercise; it's a horrible mess. Gotta separate into real and imaginary parts, and just chunk it out. The answer is

$$\widehat{f}_0(z) \quad = \quad f_0(z).$$

To compute the Fourier transform of f_n, use the standard trick, that is, take partial derivatives. So apply $\frac{\partial}{\partial z}$ to get

$$\begin{aligned} -2\pi\overline{z}e^{-2\pi(z\overline{z})} &= 2\pi\sqrt{-1}\widehat{f}_1(zz) \\ \widehat{f}_1(z) &= \sqrt{-1}\overline{z}f_0(z). \end{aligned}$$

We have the local functional equation

$$\frac{\int_{K^\times} \widehat{f}_\psi(x)\omega\chi^{-1}(x)d^\times x}{L(\omega\chi^{-1})} = \epsilon(\chi,\psi,dx)\frac{\int_{K^\times} f(x)\chi(x)d^\times x}{L(\chi)}.$$

Last time we were trying to compute when $K = \mathbb{C}$. We have $\chi = z^{-N}\omega_s$ for some $N \geq 0$. Then $\omega\chi^{-1} = z^N\omega_{1-s} = \overline{z}^{-N}\omega_{1+N-s}$. So the L factors are

$$\begin{aligned} L(\chi) &= \Gamma_{\mathbb{C}}(s) \\ L(\omega\chi^{-1}) &= \Gamma_{\mathbb{C}}(1+N-s). \end{aligned}$$

Here, as always,

$$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1).$$

Beware; some earlier papers won't have that factor of 2.

We have a definition, possibly modified from last time:

$$\begin{aligned} f_0(z) &= e^{-2\pi z\overline{z}} \\ f_n(z) &= z^n e^{-2\pi z\overline{z}} \text{ for } n \geq 0 \\ f_{-n}(z) &= \overline{z}^n e^{-2\pi z\overline{z}}. \end{aligned}$$

Recall that

$$\begin{aligned} \psi &= e^{2\pi\sqrt{1}\circ\mathrm{tr}_{\mathbb{C}\mathbb{R}}} \\ dx &= |dz \wedge d\overline{z}| \\ d^\times x &= \frac{|dz \wedge d\overline{z}|}{z\overline{z}} \\ \widehat{f}_0(z) &= f_0(z) \\ &= \int f_0(w)e^{2\pi\sqrt{-1}(w+\overline{w})}\,|dw \wedge d\overline{w}|\,. \end{aligned}$$

Apply $\frac{1}{2\pi}\frac{\partial}{\partial z}$ to get

$$\begin{aligned} -\overline{z} f_0(z) &= \sqrt{-1}\widehat{f}_1 \\ \widehat{f}_1 &= -\sqrt{-1} f_{-1} \\ &\vdots \\ \widehat{f}_n &= (\sqrt{-1})^n f_{-n}. \end{aligned}$$

If instead we apply $\frac{1}{2\pi}\frac{\partial}{\partial \overline{z}}$, we get

$$\begin{aligned} -z f_0(z) &= \sqrt{-1}\widehat{f}_{-1}(z) \\ &\vdots \\ \widehat{f}_{-n}(z) &= (\sqrt{-1})^n f_n(z). \end{aligned}$$

Let's try and compute the damned integrals, using f_N.

$$\begin{aligned} \int_{\mathbb{C}^\times} f_N(z)\chi(z)\frac{|dz \wedge d\overline{z}|}{z\overline{z}} &= \int_{\mathbb{C}} f_0(z)(z\overline{z})^{s-1}\,|dz \wedge d\overline{z}| \\ &\overset{z=re^{i\theta}}{=} \int\int_{0<r<\infty, 0\le\theta\le 2\pi} e^{-2\pi r^2} r^{2(s-1)} 2r\,dr\,d\theta \\ &= 2\pi \int\int e^{-2\pi r^2}\left(\frac{2\pi r^2}{2\pi}\right)^{2(s-1)}\frac{d(2\pi r^2)}{2\pi} \\ &= (2\pi)^{-(s-1)}\Gamma(s) \\ &= \frac{1}{\pi}\Gamma_{\mathbb{C}}(s). \end{aligned}$$

Also,

$$\begin{aligned} \widehat{f}_\psi &= (\sqrt{-1})^N \int f_{-N}(z)\overline{z}^{-N}(z\overline{z})^{1+N-s}\frac{|dz \wedge d\overline{z}|}{z\overline{z}} \\ &= (\sqrt{-1})^N \int_{\mathbb{C}} f_0(z)(z\overline{z})^{1+N-s}\frac{|dz \wedge d\overline{z}|}{z\overline{z}} \\ &= (\sqrt{-1})^N \pi^{-1}\Gamma_{\mathbb{C}}(1+N-s). \end{aligned}$$

Now just compare, and find out that

$$\epsilon(\chi,\psi,dx) = (\sqrt{-1})^N.$$

Everything is stable under a choice of embedding. And this $\sqrt{-1}$ is the same $\sqrt{-1}$ we used to define $\psi = e^{2\pi\sqrt{-1}\circ \mathrm{tr}_{\mathbf{C}}\mathbf{R}}$. So any choice of $\sqrt{-1}$ will work.

Now we work with K nonarchimedean. There's really no particularly good way to enumerate all good characters χ, the way we did for R and C. In the more general case we don't really understand them. Let $\psi : (K,+) \to \mathbf{C}_1^\times$ an additive character, and $\chi : K^\times \to \mathbf{C}^\times$. Choose a Haar measure dx on $(K,+)$. There are two invariants. The first is the conductor of χ, $a(\chi)$. Well, χ is a quasicharacter. $\mathbf{C}^\times$ is a Lie group, and as such doesn't have small subgroups. By continuity, χ is trivial on some pretty small open subgroup. It's measured by this integer, the conductor. We set

$$a(\chi) = \begin{cases} 0 & \chi(\mathcal{O}^\times) = 1 (\iff \chi \text{ unramified}) \\ \min n \text{ st } \chi(1+\mathfrak{p}^n) = 1 & \chi \text{ ramified} \end{cases}.$$

We also have a conductor for ψ, $n(\psi)$, which is the integer n so that $\psi(\mathfrak{p}^{-n}) = 1$ and $\psi(\mathfrak{p}^{-n-1}) \neq 1$. Results are as follows.

1. If χ is unramified, then

$$\epsilon(\chi,\psi,dx) = \frac{\chi(\pi^{n(\psi)})}{\|\pi\|^{n(\psi)}}\int_{\mathcal{O}} dx = \chi\omega^{-1}(\pi^{-n(\psi)})\int_{\mathcal{O}} dx.$$

2. If χ is ramified, then

$$\epsilon(\chi,\psi,dx) = \int_{K^\times} \chi^{-1}(x)\psi(x)dx,$$

   whatever that is. In representation theory, this is usually called a Gaussian integral. Superficially, this looks divergent. It's the infinite analogue of a Gaussian sum.

   In the classical case, we have an abelian group – say, $\mathbf{F}_q$. Let $\psi : \mathbf{F}_q \to \mathbf{C}_1^\times$ be a character, say, $e^{2\pi\sqrt{-1}\,\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}}$. There's a multiplicative character $\chi : \mathbf{F}_q^\times \to \mathbf{C}_1^\times$. From these two you cook up a Gaussian sum, $\sum_{x\neq 0}\chi(x)\psi(x)$.

Two more minutes to go. What are we going to do? Define characteristic functions

$$g_m(x) = \begin{cases} 1 & x \equiv 1 \bmod \mathfrak{p}^m \\ 0 & \text{otherwise} \end{cases} .$$

Then we take the Fourier transform, and hopefully find out that, essentially, $\widehat{g}_m(x)$ is essentially another characteristic function.

BTW, interpret that Gaussian integral as $\sum_{\pi^n \mathcal{O}^\times}$ of that integral; and find that the integrals are zero for all but on of the n; so the integral vanishes unless $n = -a(\chi) - n(\psi)$.

The goal today is to show that you can compute ϵ factors without peeking. Recall that we had

$$L(\widehat{\chi})^{-1}\int_{K^\times}\widehat{f}_\psi(x)\widehat{\chi}(x)d^\times x=\epsilon(\chi,\psi,dx)L(\chi)^{-1}\int_{K^\times}f(x)\chi(x)d^\times x.$$

We have K non-archimedean, $\chi : K^\times \to \mathrm{C}^\times$, $\psi : (K,+) \to \mathrm{C}_1^\times$ nontrivial, and $a(\chi)$ and $n(\psi)$ are the conductors of these [quasi]characters. Let g_m be the characteristic function of $1+\mathfrak{p}^m$. F'rintance, g_0 is the characteristic function of $\mathcal{O}$. Let's compute

$$\begin{aligned}
\widehat{g}_m(x) &= \int_K g_m(y)\psi(xy)dy\\
(*) &= \int_{1+\mathfrak{p}^m} g_m(y)\psi(xy)dy\\
\text{Let } y &= 1+z\\
(*) &= \psi(x)\int_{\mathfrak{p}^m}\psi(xz)dz.
\end{aligned}$$

Now, if $v(x)+m\geq -n(\psi)$, then $\psi(xz)\equiv 1$ for $z\in\mathfrak{p}^m$. But if $v(z)+m<-n(\psi)$, then $\psi(x)$ is not identically 1 on $z\in\mathfrak{p}^m$, and we get that the integral is either $\psi(x)\,\|\pi\|^m\int_{\mathcal{O}}dx$ if it's trivial there, and zero otherwise. So

$$\widehat{g}_m=\|\pi\|^m\int_{\mathcal{O}}dx\cdot\psi\cdot(\text{char fcn of }\mathfrak{p}^{-m-n(\psi)}).$$

Now we'll try and compute the ϵ factor. And to do that, we'll have to do some integrals. Suppose χ is unramified. Then

$$\begin{aligned}
\int_{K^\times} g_0(x)\chi(x)d^\times x &= \int_{\mathcal{O}}\chi(x)\frac{dx}{\|x\|}\\
&= \sum_{n\gg 0}\chi(\pi^n)\int_{\mathfrak{p}^n\mathcal{O}^\times}\frac{dx}{\|x\|}\\
&= \sum_{n\geq 0}\chi(\pi)^n\int_{\mathcal{O}^\times}\frac{dx}{\|x\|}\\
\int_{\mathcal{O}^\times}\frac{dx}{\|x\|} &= \int_{\mathcal{O}}dx\\
&= (1-\|\pi\|)\int_{\mathcal{O}}dx\\
\int_{K^\times} g_0(x)\chi(x)d^\times x &= (1-\|\pi\|)\int_{\mathcal{O}}dx(\frac{1}{1-\chi(\pi)})\\
&= (1-\|\pi\|)\int_{\mathcal{O}}dxL(\chi).
\end{aligned}$$

Also,

$$\begin{aligned}
\widehat{g}_0(x) &= \begin{cases} \int_{\mathcal{O}} dx\psi(x) & x \in \mathfrak{p}^{-n(\psi)} \\ 0 & \text{otherwise} \end{cases} . \\
\int_{K^\times} \widehat{g}_0(x)\omega\chi^{-1}(x)d^\times x &= \int_{\mathfrak{p}^{-n(\psi)}} \omega\chi^{-1}(x)d^\times x \\
\text{Use } x &= \pi^{-n(\psi)}y
\end{aligned}$$

If $x \in \mathfrak{p}^{-n(\psi)}$, then this is

$$(\omega\chi^{-1})(\pi^{-n(\psi)}) \int_{\mathcal{O}} \omega\chi^{-1}(y)d^\times x$$

and otherwise it's

$$(\chi\omega^{-1})(\pi^{n(\psi)})(1 - \|\pi\|) \int_{\mathcal{O}} dx L(\omega\chi^{-1}).$$

The last few things should have been multiplied by $\int_{\mathcal{O}} dx$; ask Seon-in for exactly what. The conclusion is that

$$\epsilon(\chi, \psi, dx) = \frac{\chi(\pi)^{n(\psi)}}{\|\pi\|^{n(\psi)}} \int_{\mathcal{O}} dx.$$

For the ramified case, we first want to do something about Gaussian integrals. We're worrying about things which look like

$$\mathcal{I} : \int_{K^\times} \chi^{-1}(x)\psi(x)dx$$

On the face of it, this may be a divergent integral. We'll think of it as

$$\mathcal{I} = \sum_{n \geq 0} \int_{\pi^n \mathcal{O}^\times} \chi^{-1}(x)\psi(x)dx.$$

So we want to compute $\int_{\pi^n\mathcal{O}^\times} \chi^{-1}(x)\psi(x)dx$. Lok at $\pi^n\mathcal{O}^\times/U_{a(\chi)}$, where $U_{a(\chi)} = \mathcal{O}^\times$ if $a(\chi) = 0$, and is $1\mathfrak{p}^{a(\chi)}$ if χ is ramified, that is, $a(\chi) \geq 1$. Well,

$$\int \pi^n \mathcal{O}^\times \chi^{-1}(x)\psi(x)dx = \sum_{x_i \in \pi^n \mathcal{O}^\times / U_{a(\chi)}} \|\pi\|^n \chi^{-1}(x_i) \int_{U_{(a(\chi))}} \psi(x_i u)du.$$

Assume that $a(\chi) \geq 1$. Then this is

$$\begin{aligned}
\mathcal{I}_n &= \sum \mathit{Blah} \int_{1+\mathfrak{p}^{a(\chi)}} \psi(x_i u)du \\
\int_{1+\mathfrak{p}^{a(\chi)}} \psi(x_i u)du &= \psi(x_i) \int_{\mathfrak{p}^{a(\chi)}} \psi(x_i y)dy \\
&= \psi(x_i) \|\pi\|^{a(\chi)} \int_{\mathcal{O}} dx.
\end{aligned}$$

This is zero, unless, $n + a(\chi) \geq -n(\psi)$. So $\mathcal{I}_n \equiv 0$ if $n < -a(\chi) - n(\psi)$; and if n is strictly greater, it's zero as well. So assume that $n > -a(\chi) - n(\psi)$. Well, we get

$$\begin{aligned}
\mathcal{I}_n &= \sum_{x_i \in \pi^n \mathcal{O}^\times / (1+\mathfrak{p}^{a(\chi)})} \|\pi\|^{n+a(\chi)} \chi^{-1}(x_i)\psi(x_i) \\
&= \|\pi\|^{n+a(\chi)} \sum \psi(x_i) \sum \chi^{-1}(x_i)
\end{aligned}$$

Strategy: there's a proper subgroup in $\mathcal{O}^\times$, probably $(1+\mathfrak{p}^{n+a(\chi)+n(\psi)})$ so that $\psi(x_i) = \psi(x_j)$ if $x_i x_j^{-1} \in$ it. What we're trying to say [although we haven't written it down] is that, if you look at $\sum \chi^{-1}\psi$, this value depends only on something small inside the quotient group $\pi^n \mathcal{O}^\times / \mathit{Blah}$. And those x_i having the same value can be grouped under a coset, a proper subcoset of $\mathcal{O}^\times / \mathit{Blah}$.

We start with a Gaussian integral

$$\mathcal{I} = \int_{K^\times} \chi^{-1}(x)\psi(x)dx.$$

We assume that χ ramified with $a(\chi) \geq 1$; there's also the conductor $n(\psi)$ running around. We saw that this integral is

$$\mathcal{I} = \sum_{n \in \mathbb{Z}} \int_{\pi^n \mathcal{O}^\times} \chi^{-1}(x)\psi(x)dx.$$

And if $n < -a(\chi) - n(\psi)$, then $\int_{\pi^n \mathcal{O}^\times} \chi^{-1}(x)\psi(x)dx = 0$; you wind up with a nontrivial character on a compact group, and when you integrate it dies.

Now, if $n > -a(\chi) - n(\psi)$, we want the integral to die then, as well. Let $x = \pi^n u$ in the following development, where u is a unit. We know that n is big. Look at

$$\mathcal{I}_n = \int_{\pi^n \mathcal{O}^\times} \chi^{-1}(x)\psi(x)dx.$$

We know that $\chi^{-1}(x)$ depends only on u mod ${}^\times 1 + \mathfrak{p}^{a(\chi)}$. And $\psi(x) = \psi(\pi^n u)$ depends only on u mod $1 + \mathfrak{p}^{-n-n(\psi)} < a(\chi)$. Let $H = 1 + \mathfrak{p}^{-n-n(\psi)} \subseteq \mathcal{O}^\times$. Then

$$\mathcal{I}_n = \chi^{-1}(\pi^n)\, \|\pi\|^n \int_{\mathcal{O}^\times} \chi^{-1}(u)\psi(\pi^n u)du$$

Let $\{z_\alpha\}$ be a set of representatives of $\mathcal{O}^\times/H$. Then

$$\mathcal{I}_n = \chi^{-1}(\pi^n)\, \|\pi\|^n \sum_\alpha \int_H \chi^{-1}(z_\alpha)v)\psi(\pi^n z_\alpha v)d^\times v.$$

But $\psi(\pi^n z_\alpha v)$ is constant, and $\chi^{-1}(z_\alpha v)$ isn't, since $\chi^{-1}|_H$ is not trivial. So it's the sum of zeros, and as such is zero.

When all is said and done, we see that

$$\mathcal{I} = \int_{\pi^{-a(\chi)-n(\psi)} \mathcal{O}^\times} \chi^{-1}(x)\psi(x)dx.$$

Let's briefly treat again with the calculation of ϵ factors. We'll try to figure out $\epsilon(\chi, \psi, dx)$ when χ is ramified.

Aside; let A be a finite ring, e.g., $\mathcal{O}/(\pi^n)$ or F_q. Let $\chi : A^\times \to \mathrm{C}_1^\times$, $\psi : (A,+) \to \mathrm{C}_1^\times$, and then compute the Gaussian sum $\sum_{x \in A^\times} \chi(x)\psi(x)$.

Moving on to χ ramified for ϵ factors. What we want to compute is

$$L(\widehat{\chi})^{-1} \int_{K^\times} \widehat{f}_\psi(x)\widehat{\chi}(x) d^\times x = \epsilon(\chi,\psi,dx) L(\chi) \int\int_{K^\times} f(x)\chi(x) d^\times x.$$

We're assuming χ is ramified, so the two L-factors are just 1. Take $f = g_{a(\chi)}$, the characteristic function of $1 + \mathfrak{p}^{a(\chi)}$. Then

$$\begin{aligned}
\int_{K^\times} g_{a(\chi)}\chi(x) d^\times x &= \int_{1+\mathfrak{p}^{a(\chi)}} d^\times x \\
&= \|\pi\|^{a(\chi)} \int_{\mathcal{O}} dx \\
\widehat{g}_{a(\chi)} &= \|\pi\|^{a(\chi)} \int_{\mathcal{O}} dx \cdot \psi \cdot (\text{char fcn of } \mathfrak{p}^{-a(\chi)-n(\psi)}) \\
&= \left(\int_{\mathfrak{p}^{-a(\chi)-n(\psi)}} \|x\|\, \chi^{-1}(x)\psi(x) \frac{dx}{\|x\|} \right) \cdot \int_{\mathcal{O}} dx \cdot \|\pi\|^{a(\chi)} \\
&= \left(\int_{\mathfrak{p}^{-a(\chi)-n(\psi)}} \chi^{-1}(x)\psi(x) dx \right) \cdot \|\pi\|^{a(\chi)} \int_{\mathcal{O}} dx \\
&= \left(\int_{\pi^{-a(\chi)-n(\psi)}} \chi^{-1}(x)\psi(x) dx \right) \|\pi\|^{a(\chi)} \int_{\mathcal{O}} dx \\
&= \left(\int_{K^\times} \chi^{-1}(x)\psi(x) dx \right) \|\pi\|^{a(\chi)} \int_{\mathcal{O}} dx.
\end{aligned}$$

The conclusion is that, for χ ramified,

$$\epsilon(\chi,\psi,dx) = \int_{K^\times} \chi^{-1}(x)\psi(x) dx.$$

Let's write down the local functional equation once more:

$$\frac{\int_{K^\times} \widehat{f}_\psi(x)\widehat{\chi}(x) d^\times x}{L(\widehat{\chi})} = \epsilon(\chi,\psi,dx) \frac{\int_{K^\times} f(x)\chi(x) d^\times x}{L(\chi)}.$$

How do we get something global out of this. Let $\chi : \mathrm{A}_K^\times / K^\times \to \mathrm{C}^\times$ a global quasicharacter, sometimes called a Hecke character or idele class [quasi]character. For every local place, we have the local functional equation. Remember that, in the L-function, we think of χ as being a variable. Define

$$L(\chi) = \prod_{v \text{ finite}} L(\chi_v).$$

If

$$\chi : \begin{matrix} K_v^\times \\ \mathbb{A}_K^\times / K^\times \end{matrix} \to \mathbb{C}^\times$$

and we restrict, $|\chi|\,|_{\mathcal{O}_v^\times}$, well, we know that $|\chi|\,(\mathcal{O}_v^\times)$ is a compact subgroup of $\mathbb{R}_{>0}^\times$, and as such must be $\{1\}$.

In the local case $K = K_v^\times$, we know that $|\chi| = \omega_s$ for some s. Can define a real part via $\Re(\chi) = \Re(s)$. Can also think of χ as a unitary character times some ω_s; then set $\Re(\chi) = \Re(s)$.

Anyways, if $\Re(\chi) > 1$, then the global L-function is absolutely convergent and thus well-defined. The simplest example is when χ is trivial, in which case you get nothing but the classical ζ function, which converges when $s > 1$. It's useful to complete this infinite product with some Γ factors; then the resulting thing is invariant under $s \mapsto 1 - s$. So set

$$\Lambda(\chi) = L(\chi) \prod_{v|\infty} L(\chi_v).$$

Take f to be some nice global function, say a Schwartz function $f \in \mathcal{S}(\mathbb{A}_K)$.[38] Take $f = \prod_v f_v$ where f_v is a local Schwartz function. That works fine. And for almost all v, we let f_v be the characteristic function of $\mathcal{O}_v^\times$.

Let $\psi : \mathbb{A}_K/K \to \mathbb{C}_1^\times$ be a global character. And we've got a Haar measure dx. Choose dx to be self-dual for the Fourier transform defined by ψ. Then we can think about

$$\frac{\int_{\mathbb{A}_K^\times} \widehat{f}_\psi(x)\widehat{\chi}(x)d^\times x}{\Lambda(\widehat{\chi})} \quad = \quad \epsilon(\chi, \psi, dx)\frac{\int_{\mathbb{A}_K^\times} f(x)\chi(x)d^\times x}{\Lambda(\chi)}.$$

And the global ϵ factor is just the product of the local ones, and as such is a finite product.

There's a main theorem of Tate which says that these two integrals are equal; it's a consequence of the Poisson summation formula. So we get

$$\Lambda(\chi) = \epsilon(\chi)\Lambda(\widehat{\chi}).$$

And that's the functional equation.

[38]Schwartz functions decrease rapidly at ∞ and are very smooth. Over nonarchimdedean fields, it's a locally constant function with compact support.

As usual, we're fighting with

$$\int_{K^\times} \chi^{-1}(x)\psi(x)d^\times x$$

If χ is ramified with $a(\chi) \geq 1$, we defined this as $\int_{\pi^{(-a(\chi)-n(\psi))}} \chi^{-1}(x)\psi(x)d^\times x$. This is like a Gaussian sum. Let $n = a(\chi) + n(\psi)$. Then we have the integral $\mathcal{I}$ is

$$\begin{aligned}
\mathcal{I} &= \int_{O^\times} \chi^{-1}(\pi^{-n}u)\psi(\pi^{-n}u)d^\times u \\
&= \chi(\pi^n) \int_{\mathcal{O}^\times} \chi^{-1}(u)\psi(\pi^{-n}u)d^\times u \\
&= \chi(\pi^n) \sum_{(\mathcal{O}/\pi^{a(\chi)}\mathcal{O})^\times \ni \overline{u}} \chi^{-1}(\overline{u}).
\end{aligned}$$

Now, we can get an additive character $\psi(\pi^{-n}\cdot ?) : \mathcal{O}/\pi^n\mathcal{O} \to \mathbb{C}_1^\times$. Hmm. Not sure what he's doing, but he's *saying* that this defines some character $\overline{\psi}$, and it'll be of the form $e^{2\pi\sqrt{-1}\,\mathrm{tr}(b?)}$. Hmm. We've got $\psi : (K, +) \to \mathbb{C}_1^\times$. We know that $\exists! c \in K$ so that $\psi(x) = e^{2\pi\sqrt{-1}\,\mathrm{tr}(cx)}$. The conductor of this is, well, what could it be? If $c = 1$, then we look at all those u so that, umm, hold on. We define

$$\mathfrak{p}^{-n(\psi)} = \{x \in K : e^{2\pi\sqrt{-1}\,\mathrm{tr}(cx\cdot u)} = 1 \forall u \in \mathcal{O}\}.$$

And this holds $\iff$ $cx \in \mathcal{D}^{-1}$. So $x \in c^{-1}\mathcal{D}^{-1}$. So the valuation $-n(\psi) = -v(c) - v(\mathcal{D})$, or $n(\psi) = v(c) + v(\mathcal{D})$. Once we know this, we see that $\psi(\pi^{-n}x) = e^{2\pi\sqrt{-1}\,\mathrm{tr}(\pi^{-n}c\cdot x)}$, where $\pi^{-n}\cdot c \in$, well, $\pi^{-n}c = \pi^{-a(\chi)-n(\psi)}c$ with $c \in \mathfrak{p}^{n(\psi)}\mathcal{D}_v^{-1}$. So the thing is in $\pi^{-a(\chi)}\mathcal{D}_v^{-1}$. So then $b = \pi^{-n}c$, if we return to that b? above. So we write

$$\mathcal{I} = \chi(\pi^n) \sum_{\overline{u} \in (\mathcal{O}/\pi^{a(\chi)}\mathcal{O})^\times} \chi^{-1}(\overline{u})e^{2\pi\sqrt{-1}(\overline{b}\overline{u})}.$$

We know that $\overline{b} \in (\mathcal{O}/\pi^{a(\chi)}\mathcal{O})^\times$. Note that this expression for $\mathcal{I}$ really does make sense for every $\overline{b} \in \mathcal{O}/\pi^{a(\chi)}\mathcal{O}$.[39] And if it's zero, then $\overline{b} \in \mathfrak{p}/\mathfrak{p}^{a(\chi)}$.

We can look at that sum as a classical Gaussian sum; extend χ to the nonunits by setting it to zero there. Call this sum $\tau(\chi^{-1}, \overline{b})$. So we write this thing as

[39] To some people.

$$\begin{aligned} \tau(\chi^{-1}, \overline{b}) &= \sum_{\overline{u} \in (\mathcal{O}/\pi^{a(\chi)}\mathcal{O})^\times} \chi(\overline{b})\chi^{-1}(\overline{b}\overline{u}) e^{2\pi\sqrt{-1}(\overline{b}\overline{u})} \\ &= \chi(\overline{b})\tau(\chi^{-1}, 1). \end{aligned}$$

This is some nice, simple algebraic integer sitting inside a cyclotomic field.

Gotta make sure that this is nonzero.[40]

Kate says he's saying that the ϵ factors don't depend on ψ.

Oh.

Anyways, we've got

$$\tau(\chi^{-1}, \overline{b}) \cdot \overline{\tau(\chi^{-1}, \overline{b})} = \tau(\chi^{-1}, 1) \cdot \overline{\tau(\chi^{-1}, 1)}$$

Sum over $\overline{c} \in (\mathcal{O}/\mathfrak{p}^{a(\chi)})^\times$, and get[41]

$$\begin{aligned} \#(\mathcal{O}/\mathfrak{p}^{a(\chi)})^\times \left|\tau(\chi^{-1}, \overline{b})\right|^2 &= \sum \chi(u^{-1}) e^{2\pi\sqrt{-1}(bu - bv)} \\ &= \end{aligned}$$

I locally give up.

We're trying to sum over all additive characters ψ.

Let $x \in (\mathcal{O}/\mathfrak{p}^{a\chi)})^\times$. Look at $\sum_x e^{2\pi\sqrt{-1}b(u-v)}$. This is zero if $u \neq v$, and is $\mathrm{N}(\mathfrak{p})^{a(\chi)}$. The only thing which contributes is when $u = v$. How many are there? That's $\#(\mathcal{O}/\mathfrak{p}a(\chi)$. So the whole answer is

$$\#((\mathcal{O}/\mathfrak{p}^{a(\chi)})^\times)\mathrm{N}(\mathfrak{p}^{a(\chi)}.$$

So when all is said and done, $\left|\tau(\chi^{-1}, \overline{b})\right| = \mathrm{N}\mathfrak{p}^{\frac{a(\chi)}{2}}$.

[40] If it's zero, the functional equation would utterly go down and flames.

[41] Provided we keep in mind $\overline{\tau(\chi^{-1}, \overline{b})} = \sum \chi(v) e^{-2\pi\sqrt{-1}(\overline{b}v)} = \sum \chi(v) e^{-2\pi\sqrt{-1}(bv)}$.

Tate's main theorem [42] Look at $\mathbb{A}_K^\times$. On the other hand, we have the group of adeles $\mathbb{A}_K$. We want to take a nice $f \in \mathcal{S}(\mathbb{A}_K)$, Schwartz functions on $\mathbb{A}_K$. For us, such a beast is a linear combination of functions of the sort $(\prod_{v|\infty} f_v) \cdot (\prod_{v \in S} f_v) \cdot (\prod_{v \notin S} f_{v,0})$ with $f_v \in \mathcal{S}(K_v)$ and S a finite set of primes, and f_{v_0} is the characteristic function of $\mathcal{O}_v$.

If $f \in \mathcal{S}(\mathbb{A}_K)$ we'll build a zeta function. Let $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$. Choose a nontrivial additive character $\psi : \mathbb{A}_K / K \to \mathbb{C}_1^\times$. Then we define

$$\zeta(f, \chi) = \int_{\mathbb{A}_K} f(x)\chi(x) d^\times x$$

where $d^\times x$ is a Haar measure on $\mathbb{A}_K^\times$. Before we go on further, let's clarify a couple of points. There are certain subtleties.

The point is the following. Naively you'd think that, f being a product, the integral should be $\zeta(f, \chi) = \prod \zeta(f_v, \chi_v)$. This is true, but not for the reason you're thinking of. For f, although it's a product, is a Schwartz function with respect to the additive structure. So if you integrated over $\mathbb{A}_K$, you'd be cool. But we're working over the ideles $\mathbb{A}_K^\times$; and the product there is different. Recall that an idele is not, well,

$$\mathbb{A}_K^\times \neq \prod K_v^\times.$$

$\mathbb{A}_K^\times$ is really an inductive [direct] limit.

[42]This'll work out to be the Poisson summation formula.

The goal today is to prove Tate's theorem. The most important part of Tate's theorem is that if $f \in \mathcal{S}(\mathbb{A}_K)$, and we choose $\chi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$, $\psi : \mathbb{A}_K/K \to \mathbb{C}_1^\times$, then in analogy to the local case we have two quantities:

$$\int_{\mathbb{A}_K^\times} \widehat{f}_\psi \widehat{\chi} d^\times x = \int_{\mathbb{A}_K^\times} f(x)\chi(x) d^\times x.$$

These make sense in the sense that we can analytically continue both sides as holomorphic functions of s, where χ is ω_s, more or less, I think. We'll also see how to holomorphically continue these functions; and when and where each side can have a pole. Furthermore, each pole is simple, and we'll compute the residue.

Recall that if $f \in \mathcal{S}(\mathbb{A}_K)$ the Schwartz functions, then, remember that as a space, $\mathbb{A}_K^\times$ is quite different from $\mathbb{A}_K$. We can write

$$\mathbb{A}_K^\times = \lim_{\vec{S}} \mathbb{A}_{K,S}^\times$$

where

$$\mathbb{A}_{K,S}^\times = \prod_{v \notin S} \mathcal{O}_v^\times \times \prod_{v \in S} K_v^\times.$$

Let's figure out the meaning of the integral $\int_{\mathbb{A}_K^\times} f(x)\chi(x)d^\times x$. This converges absolutely if $\Re(\chi) > 1$. Let $f = f_1^{S_0} f_{0,S_0}$ where f_{0,S_0} is the characteristic function of $\prod_{v \notin S_0} \mathcal{O}_v$, and $f_1^{S_0}$ is a Schwartz function on $\prod_{v \notin S_0} K_v$. First, notice that the Haar measure may be taken as $d^\times x = \prod' d^\times x_v$, the restricted product. For all but a finite number of places, this has the property that $\int_{\mathcal{O}_v^\times} d^\times x_v = 1$ for $v \notin S_1$.

Let's think about

$$\int_{\mathbb{A}_K^\times} f(x)\chi(x)d^\times x = \lim_{\vec{S}} \int_{\prod_{v\in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times} f(x)\chi(x) d^\times x.$$

For S sufficiently large, we can assume that $S \supseteq S_0$, and χ is unramified outside S. For $v \in S - S_0$, $\int_{\mathcal{O}_v^\times} d^\times xv = 1$. Then $\int_{\mathcal{O}_v^\times} f(x)\chi(x)d^\times x = \int 1 \cdot 1 \cdots d^\times xx = 1$. Then

$$\begin{aligned}
\int_{\mathbb{A}_K^\times} f(x)\chi(x)d^\times x &= \lim_{\vec{S}} \int_{\prod_{v\in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times} f(x)\chi(x)d^\times x \\
&= \lim_{\vec{S}} \int_{\prod_{v \in S_0} K_v^\times} f(x)\chi(x)(\prod_{v\in S_0} d^\times x_v) \cdot \prod_{v \in S - S_0} \int_{O_v} \chi(x) d^\times x
\end{aligned}$$

We may assume that χ is unramified outside for $v \notin S_0$. In that case,

$$\begin{aligned}
\prod_{v \in S-S_0} \int_{\mathcal{O}_v} \chi(x) d^\times x &= \prod_{v \in S-S_0} (\int_{\mathcal{O}_v} dx)(1-\chi(\pi))^{-1} \\
\text{May assume} \int_{\mathcal{O}_v} dx_v = 1 \quad &\text{and} \quad d^\times x_v = \frac{dx_v}{\|x_v\|} \; \forall v \notin S_0, \Re(\chi) > 0
\end{aligned}$$

So at this point, the question is when does $\prod_{v \notin S_0}(1-\chi(\pi))^{-1}$ converge?

If $\Re(\chi) = \sigma$, then

$$\prod_{v \notin S_0} (1-\chi(\pi))^{-1} \sim \prod_{v \notin S_0} (1 - \mathrm{N}\mathfrak{p}_v^{-\sigma})^{-1}.$$

But this is bounded by 1 and $\prod_{p \geq p_0}(1-p^{-\sigma})^{-n}$ where $n = [K : \mathrm{Q}]$.

So it turns out that the original integral is the product of the local integrals. This is what you'd naïvely guess, but it takes some work to show that it's true over *ideles*, not *adeles*.

So much for that. There are now a couple of things we'd like to do. First, holomorphic continuation. Second, $\Lambda(\chi) = \epsilon(\chi)\Lambda(\omega\chi^{-1})$, where $\Lambda(\chi) = \prod_v L(\chi_v)$. Usually, we write $L(\chi) = \prod_{v \text{ finite}} L(\chi_v)$; and $\epsilon(\chi) = \prod_v \epsilon(\chi_v, d\psi_v, dx_v)$.

Let's get on with the business of the proof. It's essentially an application of Poisson summation formula.

$$\begin{aligned}
\zeta(f,\chi) &\stackrel{\text{def}}{=} \int_{\mathrm{A}_K^\times} f(x)\chi(x) d^\times x \\
&= \int_{\mathrm{R}_{>0}^\times} \frac{dt}{t} \int_{\mathrm{A}_{K,1}^\times} f(tu)\chi(tu) d^\times u \\
\text{where } d^\times x &= d^\times u \frac{dt}{t} \\
\text{measures on } & \quad \mathrm{A}_{K,1}^\times \;\; \mathrm{A}_K/\mathrm{A}_{K,1} \\
\zeta(f,\chi) &= \int_{\mathrm{R}_{>0}^\times} \frac{dt}{t} \zeta_t(f,\chi) \text{ by Fubini}
\end{aligned}$$

Now we want to apply the Poisson summation formula. The point is that we have the unitary ideles $\mathrm{A}_{K,1} \supseteq K^\times$ a discrete subgroup; and the quotient is compact. On the other hand, we have K not differing very much from $K^\times$, and $\mathbb{A}_K \supseteq K$; again, the quotient is compact. We know a Poisson summation formula for the latter pair, that is, well, $K \hookrightarrow \mathbb{A}_k$. We have $\psi : (\mathbb{A}_K, +) \to \mathbb{C}_1^\times$ coming from [or inducing] $(k_v, +) \to \mathbb{C}_1^\times$; and we multiply all the local ones together to get a global character. We can identify the dual of $\mathbb{A}_K$ with itself via $\psi : \mathbb{A}_K \overset{\cong}{\to} \widehat{\mathbb{A}_K}$, although this isn't canonical. Under this duality we can take K sitting inside $\mathbb{A}_K$. What do we know about $K^\perp$? $\psi|_K$ is trivial. Since the quotient is cocompact, K is of finite index inside $K^\perp$. But $K^\perp$ is a K-vector space, and.... a miracle occurs and $K = K^\perp$. Poisson summation says that

$$\begin{aligned} \sum_{x\in K} f(x) &= \sum_{x\in K} \hat{f}(x) \\ \zeta_t(f,\chi) &= \int_{\mathbb{A}^\times_{K,1}/K^\times} \Big(\sum_{a\in K^\times} f(tua)\chi(tua)\Big) d^\times u \end{aligned}$$

But $\chi(tua) = \chi(tu)$, since χ is an idele class character. So

$$\zeta_t(f,\chi) = \int_{\mathbb{A}^\times_{K,1}/K^\times} \chi(tu)\Big(\sum_{a\in K^\times} f(tau)\Big) d^\times u.$$

Still working with Tate's theorem. We have

$$\begin{aligned}
\zeta(f,\chi) &= \int_{\mathbb{A}_K^\times} f(x)\chi(x)d^\times x \\
&= \int_{\mathbb{R}_{>0}^\times} \frac{dt}{t}\int_{\mathbb{A}_{K,1}^\times} f(tu)\chi(tu)d^\times u \\
&= \int_{\mathbb{R}_{>0}^\times} \zeta_t(f,\chi)\frac{dt}{t} \\
\zeta_t(f,\chi) &= \int_{\mathbb{A}_{K,1}^\times} f(tu)\chi(tu)d^\times u \\
&= \int_{\overline{u}\in\mathbb{A}_{K,1}^\times/K^\times} (\sum_{\xi\in K^\times} f(\xi tu))\chi(tu)d^\times\overline{u} \\
&= \int_E \chi(tu)(\sum_{\xi\in K^\times} f(\xi tu))fd^\times u.
\end{aligned}$$

Here, E is a fundamental domain for $\mathbb{A}_{K,1}^\times/K^\times$. On $\mathbb{A}_K$, choose ψ via $\mathrm{tr}_{K,\mathbb{Q}}$, and dx a self-dual Haar measure with respect to this global trace. Then for every Schwartz function $g\in\mathcal{S}(\mathbb{A}_K)$, we have

$$\sum_{\xi\in K} g(\xi) = \sum_{\xi\in K}\widehat{g}(\xi)$$

Apply this to $g=f(\xi tu)$. Let $g(x)=f(tux)$. Then

$$\begin{aligned}
\widehat{g}(y) &= \int_{\mathbb{A}_K} f(tux)\psi(xy)dx \\
&= \frac{1}{\|tu\|}\int f(z)\psi(\frac{z}{tu}y)dz \\
&= \frac{1}{\|tu\|}\widehat{f}(\frac{y}{tu}).
\end{aligned}$$

Apply this result to the thing above. We had $\sum_{\xi\in K^\times} f(\xi tu)$. We can add in the missing term $\xi=0$ so that the sum is over all $\xi\in K$. The result is

$$\sum_{\xi\in K^\times} f(\xi tu) = -f(0)+\frac{1}{\|tu\|}\widehat{f}(0)\sum_{\xi\in K^\times}\frac{1}{\|tu\|}\widehat{f}(\frac{\xi}{tu})$$

$$\begin{aligned}
\zeta_t(f,\chi) &= \int_E \chi tu)\frac{1}{\|tu\|}\sum_{\xi\in K^\times}\widehat{f}(\frac{\xi}{tu})d^\times u - \\
&\quad f(0)\int_E \chi(tu)d^\times u + \widehat{f}(0)\int_E \chi\omega^{-1}(tu)d^\times u \\
\zeta(f,\chi) &= \int_1^\infty \zeta_t(f,\chi)\frac{dt}{t} + \int_0^1 \zeta_t(f,\chi)\frac{dt}{t} \\
&= \int_1^\infty \zeta_t(f,\chi)\frac{dt}{t} + \\
&\quad \int_0^1 \frac{dt}{t}\int_E \chi\omega^{-1}(tu)(\sum_{\xi\in K^\times}\widehat{f}(\xi tu))d^\times \\
&\quad -f(0)\kappa\int_0^1 \frac{dt}{t}t^s + \widehat{f}(0)\kappa\int_0^1 t^{s-1}\frac{dt}{t} \\
\text{Use } t,u &\mapsto t^{-1},u^{-1} \\
\zeta(f,\chi) &= \int_1^\infty \zeta_t(f,\chi)\frac{dt}{t} + \\
&\quad \int_1^\infty \frac{dt}{t}\int_{\mathbb{A}_{K,1}^\times/K^\times}\widehat{\chi}(tu)(\sum_{\xi\in K^\times}\widehat{f}(tu\xi))d^\times u + \widehat{f}(0)\kappa\frac{1}{s-1} - \kappa f(0)\frac{1}{s}
\end{aligned}$$

$$\text{Note that } \int_{\mathbb{A}_{K,1}^\times/K^\times}\widehat{\chi}(tu)(\sum_{\xi\in K^\times}\widehat{f}(tu\xi))d^\times u = \zeta_t(\widehat{f},\widehat{\chi})$$

[43]

So the possible poles are at $\chi=\omega$ or χ trivial. Otherwise, it's holomorphic.

The grand conclusion is that

$$\zeta(f,\chi)=\zeta(\widehat{f},\widehat{\chi})$$

[43]Remember that $E=\mathbb{A}_{K,1}^\times/K^\times$. And $\chi:\mathbb{A}_K^\times/K^\times\to\mathbb{C}^\times$; and χ is nontrivial unless its just a power of ω; so we get $\mathbb{A}_K^\times/\mathbb{A}_{K,1}^\times \overset{\omega\cong}{\to} \mathbb{R}_{>0}^\times$. So the integral over E dies unless $\chi=\omega_s$. And in the case that $\chi=\omega_s$, $\int_{\mathbb{A}_{K,1}^\times/K^\times}\chi(tu)d^\times u = t^s\,\mathrm{vol}(E)$. And

$$\int_{\mathbb{A}_{K,1}^\times/K^\times}\chi\omega^{-1}(tu)d^\times u = \begin{cases} 0 & \chi\neq\omega_s \\ \mathrm{vol}(\mathbb{A}_K^\times/K^\times)t^{s-1} & \chi=\omega_s \end{cases}.$$

Define

$$\kappa = \begin{cases} 0 & \chi\neq\omega_s\forall s \\ \int_{\mathbb{A}_{K,1}^\times/K^\times} d^\times u & \chi=\omega_s \end{cases}.$$

by symmetry. And we see that $\int_1^\infty \zeta_t(f,\chi)\frac{dt}{t}$ is holomorphic in χ; $\zeta_t(\widehat{f},\widehat{\chi})$ is holomorphic in χ, as well.

That's a great big theorem. This essentially tells us everything we know about abelian L-functions. From this, we'll deduce all sorts of functional equations for abelian L- and ζ functions.

Exercise When $d^\times x_v$ is normalized so that $\int_{\mathcal{O}_v^\times} d^\times x_v = 1$, and at the archimedean places $d^\times x_v = \begin{cases} \frac{dx}{|x|} & K_v \cong \mathrm{R} \\ \frac{|dz\wedge d\bar{z}|}{z\bar{z}} & K_v \cong \mathrm{C} \end{cases}$, this gives us a multiplicative Haar measure on the restricted product $\mathrm{A}_K^\times$. Then the fundamental domain has volume

$$\int_{\mathrm{A}_{K,1}^\times/K^\times} d^\times x = 2^{r_1}(2\pi)^{r_2} hR/(\#\mu(K)).$$

The denominator is w, the number of roots of unity; $\mu(K)$ is the torsion subgroup of the units. The regulator R is a certain determinant, defined as follows. We know that the units of K are finitely generated as an abelian group; $\mathcal{O}_K^\times \cong \mu(K)\times \mathrm{Z}^{r_1+r_2-1}$. Let the free part have generators $\epsilon_1,\cdots,\epsilon^{r_1+r_2-1}$. For such an ϵ_i we can look at[44] $\|\epsilon_i\|_{v_1},\cdots,\|\epsilon_i\|_{v_{r_1}},\|\epsilon_i\|_{v_{r_1+1}},\cdots,\|\epsilon\|_{r_1+r_2}$. Actually, take logs of these norms. This gives us an $(r_1+r_2-1)\times(r_1+r_2)$ matrix. This will have a relation in it. So take the absolute value of the determinant of any maximal minor of this matrix. By the product formula, this is well-defined. In general, this is a pretty transcendental number, and we don't know very much about it.

Whenever you want to prove anything like this, in fact what you have to find is some sort of explicit fundamental domain. In this case, because of the roots of unity, it's tough to write it down. But you can find some domain so that every point is represented exactly w times.[45] So we've got this w-fold fundamental domain. The class number comes in because it's natural to consider the product of all units; and then you want to take away or mod out by $K^\times$, where $K^\times$ corresponds to principal ideals. Elements in the product of the units correspond to the trivial ideal. So basically, you know that $\mathrm{A}_K^\times/(\prod_{v|\infty} K_v^\times\cdot K^\times\cdot\prod_v \mathcal{O}_v^\times)$ is the class group. The $K^\times$ doesn't do anything, and we know what to do with the nonarchimedean places. So you compute the unit part of the denominator divided by $K^\times$. And that, pretty much, is the class number. When you compute this you'll see that the units naturally come in. So find a fundamental domain for $(\prod_{v|\infty} K_v^\times\cdot K^\times\cdot\prod_v \mathcal{O}_v^\times)_1/K^\times$.

[44] Let the v_j be the archimedean places.

[45] Otherwise you have to take something smaller which isn't easy to write down.

Today we'll play with zeta functions. As usual, we define

$$\begin{aligned}\zeta_K &= \sum_{\mathfrak{a}\subset\mathcal{O}_K}\frac{1}{(\mathrm{N}\mathfrak{a})^s}\\ &= \prod_{\mathfrak{p}}\frac{1}{1-N\mathfrak{p}^{-s}}.\end{aligned}$$

When $K=\mathbb{Q}$, then $\zeta\mathbb{Q}(s)$ is the Riemann zeta function. This is the prototype of all these zeta and L-functions. $L(\chi\omega_s)=L(\chi,s)$. We saw that for every quasicharacter χ you have an L function, and $L(\chi,s)$ will be holomorphic on the whole complex numbers, with possible poles only when χ is a power of ω. If χ isn't a power of ω, then this is entire; holomorphic on the coplex plane. When χ is a power of s, you pick up the poles exactly when $\chi\omega_s$ is the trivial character of χ itself.

Today, we're going to write down what this implies for the classical zeta function of a number field. These functions are analytic gadgets. From experience, everybody knows that the zeta function of a global field encodes everything about it; if you really understand the zeta function, you understand everything about the number field. In ways we don't fully understand, it encodes all the information you'd want.

We'll see that the classical thing has a simple pole at $s=1$, and there's a functional equation. The residue at $s=1$ gives the class number.

The way to get started is to identify this zeta function as a special case of the $L(\chi\omega_s)$ things we did before, since if you take χ the trivial quasicharacter, then that's the zeta function. $\zeta_K(s)=L(\omega_s)$. Immediately we know it has a functional equation. We know that $\Lambda(\omega_s)=\epsilon(\omega_s)\Lambda(\omega_{1-s})$. Here, $\epsilon(\omega_s)$ is what? It's a product of local factors;

$$\epsilon(\omega_s)=\prod_v \epsilon(\omega_s,\psi_v,dx_v).$$

Choose $\psi_v=e^{-2\pi\sqrt{-1}\,\mathrm{tr}}$ if $v|\infty$, and $e^{2\pi\sqrt{-1}\,\mathrm{tr}}$ if v is finite. Let dx_v be the self-dual measure with respect to ψ. We know that it's $|dz\wedge d\overline{z}|$ for v complex; dx if x is real; and $\int_{\mathcal{O}_v}dx_v=(N\mathcal{D}_v)^{-\frac{1}{2}}$. Immediately we know that if v is unramified over $\mathbb{Q}$ then it's one. So if v is infinite, then $\epsilon(\omega_s,\psi_v,dx_v)=1$. If v is finite and unramified, then $\epsilon(\omega_s,\psi_v,dx_v)=1$ again. Finally, what about $\mathcal{D}_v$ nontrivial, that is, v is ramified, while χ trivial. Then we see that $\epsilon(\omega_s,\psi_v,dx_v)=\frac{\omega_s(\pi_v^{d_v})}{\|\pi_v\|^{d_v}}\int_{\mathcal{O}_v}dx_v=\|\pi_v\|^{sd_v-d_v+\frac{d_v}{2}}=\|\pi_v\|^{sd_v-\frac{d_v}{2}}$.[46] Putting it all together, we have

[46]We're thinking of $\mathcal{D}_{K,}\mathbb{Q}=\prod\mathfrak{p}_v^{d_v}$.

$$\begin{aligned}
\epsilon(\omega_s) &= \prod_v \epsilon(\omega_s, \psi_v, dx_v) \\
&= \mathrm{N}\mathcal{D}_K^{-s+\frac{1}{2}} \\
\Lambda(\omega_s) &= (\mathrm{disc}_K)^{\frac{1}{2}-s}\Lambda(\omega_{1-s}).
\end{aligned}$$

We can write this in terms of gamma factors.

$$\zeta_K(s)\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2} = (\mathrm{disc}_K)^{\frac{1}{2}-s}\Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\zeta_K(1-s).$$

As an exercise, take a Dirichlet character, a character of $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times$. You can write this as an idele class character for $\mathbb{Q}$. Then the Dirichlet L-function becomes one of our $L(\chi)$'s. You can get a functional equation. See if this corresponds to the functional equation in any number theory book.

Let's go for the analytic class number formula. The way we want to do this is the following. In general, from this product formula [for L-series], you can do some Hecke theory, but it doesn't tell you anything about the zeros or poles. In order to do tis, you'll need to do a global calculation. The information we have about the residues comes from a global calculation, and that occurs in the proof of Tate's theorem. So, if we can identify either $\zeta_K(s)$ or the $\Lambda(\omega_s)$ as a global zeta function in the sense of Tate, then we win.

But we're almost there, for if you remember, when we computed the local epsilon factors, we actually computed a lot of the local zeta functions, by which we mean $\int_{K_v^\times} f(x)\chi(x)d^\times x$. Recall that if $K_v \cong \mathbb{R}$, then $\int_{\mathbb{R}^\times} e^{-\pi x^2}\omega_s d^\times x = \Gamma_{\mathbb{R}}(s)$.; if $K_v \cong \mathbb{C}$, then $\int_{\mathbb{C}^\times} e^{-2\pi z\overline{z}}\omega_s d^\times x_v = \pi\Gamma_{\mathbb{C}}(s)$.

If v is nonarchimedean, let f_0 be the characteristic function of $\mathcal{O}_v$. Then

$$\begin{aligned}
\int_{\mathcal{O}_v} f_0(x)\omega_s(x)d^\times x &= \sum_{n\geq 0}\int_{\pi^n\mathcal{O}_v^\times} \|\pi\|^{ns}\, d^\times x_v \\
&= \frac{1}{1-N\mathfrak{p}_v^{-s}}\cdot\int_{\mathcal{O}_v^\times} d^\times x_v \\
\text{Take } d^\times x_v \text{ so that } \int_{\mathcal{O}_v^\times} d^\times x_v &= (\mathrm{N}\mathcal{D}_v)^{-\frac{1}{2}}. \\
&= (\mathrm{N}\mathcal{D}_v)^{-\frac{1}{2}}\frac{1}{1-N\mathfrak{p}_v^{-s}}.
\end{aligned}$$

Now take $f_0 = \prod_v f_{0,v}$. Then use the Euler product. Then

$$\zeta(f_0, \omega_s) = (\mathrm{N}\mathcal{D})^{-\frac{1}{2}} \pi^{r_2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \zeta_K(s).$$

But the left-hand side has a simple pole at $\omega_s = \omega$ or ω_s is trivial, i.e., at $s = 0$ and $s = 1$. Furthermore, at $s = 1$, the residue is $f_0(0) \int_{\mathbb{A}_K^\times / K^\times} d^\times x$; some constant times the volume of the fundamental domain. This is everything.

Now, we have to remember that last time we had a formula for the volume of the fundamental domain. But now the normalization of the Haar measure is different from that one. Cause the other one is normalized in such a way that $\int_{\mathcal{O}_v^\times}$ is always one. If we use the formula, we get that at $s = 1$ the residue is

$$f_0(0) 2^{r_1} (2\pi)^{r_2} hR/W.$$

But this measure differs by a factor of the discriminant. So actually the residue [using this measure] is

$$f_0(0) \frac{2^{r_1} (2\pi)^{r_2} hR}{|\mathrm{disc}_K|^{\frac{1}{2}}\, W}.$$

But $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

The final answer is that

$$\mathrm{res}_{s=1}\, \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} hR}{|\mathrm{disc}_K|^{\frac{1}{2}}\, w}.$$

This is the analytic class formula. Now, there are cases when this is easy to use. For example, if K is a cyclotomic field, then we know that the zeta function is related to the Riemann zeta function by a product formula. Let $K = \mathbb{Q}(\sqrt[n]{1})$. We'll see shortly that $\zeta_K(s) = \zeta_{\mathbb{Q}}(s) \prod_{\chi \neq 1} L(\chi, s)$, where $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$.

We want to find fundamental domains for

- $\mathbb{A}_K/K$ for function fields.
- $\mathbb{A}_K^\times/K^\times$ for number fields and function fields.

Find their measures with respect to the self-dual Haar measure, for the adelic case. And for ideles, define

$$x_v = \begin{cases} \int_{\mathcal{O}_v^\times} d^\times x_v = 1 & v \text{ finite} \\ \frac{|dz\wedge d\bar{z}|}{z} & K_v \cong \mathbb{C} \\ \frac{dx}{|x|} & K_v \cong \mathbb{R} \end{cases}.$$

There's another problem, namely, K a function field. We had the Poisson summation formula for $K \subseteq \mathbb{A}_K$; and that, essentially, gave Tate's theorem. For the function field case, the question is to show that this exactly corresponds to Riemann-Roch[47] and Serre duality.

Today's lecture is about Artin L-functions. We saw before that we have one kind of L function. Namely, given an idele class quasicharacter $\chi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$, we have an L function $L(\chi, s)$. And if we add the Γ factors at ∞, we get $\Lambda(\chi, s)$. Recall that

$$L(\chi, s) = \prod_{v \text{ finite}} L(\chi_v \omega_s)$$

and

$$\Lambda(\chi, s) = \prod_v L(\chi_v \omega_s).$$

Note that these correspond to 1-dimensional [abelian] representations. Automorphic L functions come from $\mathbb{G}_m/K$. This is sort of like abelian harmonic analysis. And we saw that it has an analytic continuation and satisfies functional equations, etc. We know it has [possibly] simple poles for certain χ's, specifically, exactly those of the form ω_s for certain s. And we even know what the s's are, and how to compute the residues at those poles.

Artin L-functions arise as follows. Take a finite Galois extension L over K, with group G. Take a finite dimensional complex representation of G; call this $\rho : G \to \mathrm{Aut}(V)$ with V a $\mathbb{C}$ vector space. Then we can define an Artin L-function as follows.

[47]For a smooth curve over a finite field.

$$L(\rho, s) \stackrel{\text{def}}{=} \prod_{v \text{ finite}} L(\rho_v, s).$$

Okay, fine. Gotta define the local factors. They are given by

$$L(\rho_v, s) = \det(\operatorname{id} - \rho(\mathrm{Fr}_v) q_v^{-s} | V^{\rho(I_v)})^{-1}.$$

You take the inertia group at V. It's a subgroup of G, defined up to conjugation; fix a place upstairs, and look at its inertia group. If w is a place over v, then $D_w \supseteq I_w$, and $D_w/I_w \cong \mathrm{Gal}(\kappa_w, \kappa_v)$. So there's a frobenius element, and we can use it. And $q_v = \#\kappa_v$.

Let's think about $\operatorname{id} - \rho(\mathrm{Fr}_v) q_v^{-s}|_{V^{\rho(I_v)}}$.

Aside; $\rho(\mathrm{Fr}_v)$ operates on the inertia invariants $V^{(\rho(I_v))}$. So it has eigenvalues $\lambda_1, \cdots, \lambda_{m_v}$. And here, we're taking $\prod_{i=1}^{m_v}(1 - \lambda_i q_v^{-s})^{-1}$. For example, if ρ is the trivial representation, well, everything is inertia invariant, and so we get $\prod_v (1 - q_v^{-s})^{-1} = \zeta_K(s)$.

As another example, let L be the cyclotomic field $\mathbb{Q}(\zeta_n)$, and $K = \mathbb{Q}$. Then $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is a 1-dimensional character of the Galois group. Then $L(\chi, s)$ is the classical Dirichlet L-function attached to χ.

Artin sez, when ρ is a 1-dimensional representation, then (ρ, s) should come be $L(\chi, s)$ for some $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}$ an idele class [quasi]character. And therefore, this Artin L-function is identified with an automorphic L-function. In this way, well, the true reason of course is that there's a map $\mathbb{A}_K^\times / K^\times \to G$, where $G = \mathrm{Gal}(L, K)$ for some L; and there's a $\rho : G \to \mathbb{C}^\times$ which, when composed with that map, gives χ. And that map to G is the Artin reciprocity law.

Let's try to understand this operator $\rho(\mathrm{Fr}_v)|_{V^{\rho(I_v)}}$ as a linear operator. You have a finite dimensional representation of a finite group. How do you get the invariants? Representation theory tells us the answer.

Recall that, for G a compact group and $\rho : G \to \mathrm{Aut}(V)$ V a $\mathbb{C}$-vector space how do you get the invariants? Well, you compute $\int_G \rho(g) dg \in \mathrm{End}_{\mathbb{C}}(V)$. This is a projection onto the invariants V^G.

Apply this to our situation. We know that

$$\frac{1}{\# I_v} \sum_{g \in I_v} \rho(g)$$

is a projection operator onto V. Then

$$\det((\mathrm{id}_v - \rho(\mathrm{Fr}_v)T)\frac{1}{\#I_v}\sum_{g\in I_v}\rho(g))^{-1} = \det(\mathrm{id} - \rho(\mathrm{Fr}_v)T|_{V^{\rho(I_v)}})^{-1}$$

and set $T = q_v^{-s}$. Take logarithms of everything in sight. Let $\chi = \chi_\rho$, i.e., $\chi(g) = \mathrm{tr}(\rho(g))$.

$$\begin{aligned} \log(1 - aT)^{-1} &= \sum_{m\geq 1}\frac{a^m T^m}{m} \\ \text{In general } \log\det(\mathrm{id}_W - A\cdot T)^{-1} &= \sum_{m\geq 1}\frac{\mathrm{tr}(A^m)}{m}T^m \end{aligned}$$

[Here, we assumed A is diagonal, and then $\sum_i a_i^m = \mathrm{tr}(A^m)$.]

And that determinant above is

$$\det(\mathrm{id}_V - T\rho(\mathrm{Fr}_v)(\frac{1}{\#I_v}\sum_{g\in I_v}\rho(g)))^{-1}$$

since this thing operates as the identity on $V/V^{\rho(I_g)}$. For this is really id_v - something times some projection operator. So we can compute $0 \to V^{I_v} \to V \to V/V^{I_v} \to 0$. And therefore the determinant of any automorhpism is the product of the determinant induced on the invariants and the quotient thing. Both sides [in the determinant equation] are the same on the invariants and the quotient space, so they're the same. That sum operates as zero on the quotient.

Then

$$\begin{aligned} \log\det(\mathrm{id}_V - T\rho(\mathrm{Fr}_v)(\frac{1}{\#I_v}\sum_{g\in I_v}\rho(g)))^{-1} &= \sum_{m\geq 1}\frac{\chi_\rho(\mathrm{Fr}_v^m(\frac{1}{\#I_v}\sum_{g\in I_v}\rho(g)))T^m}{m} \\ \log L(\rho, s) &= \sum_{m\geq 1}\frac{\chi(\mathrm{Fr}_v^m\ \frac{1}{\#I_v}\sum_{g\in I_v}\rho(g))}{m}q_v^{-ms} \end{aligned}$$

One usually writes this as $\sum\frac{\chi(\mathrm{Fr}_v^m)}{m}q_v^{-ms}$.

Facts of life:

- $L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s)L(\rho_2, s)$.

- If $L \supset M \supset K$, everything Galois, $H = \mathrm{Gal}(L, M)$, $G/H = \mathrm{Gal}(M, K)$, and ρ a representation of G/H, then $L(\rho_{G/H}, s) = L(\rho_G, s)$.
- [48] Assume $H \subseteq G$ is just any old subgroup of G, not necessarily normal. Assume $\rho : H \to \mathrm{Aut}(V)$. Then we can induce, and $L(\mathrm{Ind}_H^G(\rho), s) = L(\rho, s)$. In other words, the Artin L-function is inductive.

[48] The only nonobvious property

Working on Artin L-functions.

If there's a finite Galois extension L/K of global fields, $G = \mathrm{Gal}(L, K)$, we suppose a finite representation $\rho : G \to GL(V)$ with V a $\mathbb{C}$-vector space. Then we define the Artin L-function

$$L(\rho, s) = \prod_{v \text{ finite}} \det(\mathrm{id} - \mathrm{Fr}_v\, q_v^{-s}|_{V^{I_v}})^{-1}.$$

Fact If ρ is abelian, then $L(\rho, s)$ has a meromorphic continuation. This isn't obvious at all; all we can tell for sure is that it's absolutely convergent for $\Re(s) > 1$. Additionally, when ρ is abelian, there's a functional equation relating $L(\rho, s)$ and $L(\check{\rho}, 1 - s)$. Equality holds when you add in the Gamma factors properly. This fact, in essence, is class field theory *in toto.*

This tells us that, in general, $L(\rho, s)$ has a meromorphic contintation to $\mathbb{C}$ and a functional equation. This is an easy consequence of a theorem of Brauer, say, for any finite dimensional representation ρ of a group G, we can find subgroups $H_i \subset G$, one-dimensional representations τ_i of H_i, and $n_i \in \mathbb{Z}$ so that $\chi_\rho = \sum_i n_i \mathrm{Ind}_{H_i}^G(\chi_{\tau_i})$.

Brief review of induced representations. Suppose $H \subset G$, and $\tau : H \to GL(V)$ a finite dimensional representation. Then you can define an induced representation $\mathrm{Ind}_H^G(\tau) : G \to GL(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V)$. Recall that $\chi_\rho(g) = \mathrm{tr}(\rho(g))$.

Anyways,

$$L(\mathrm{Ind}_H^G(\tau), s) = L(\tau, s).$$

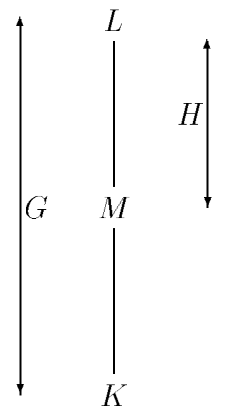
Then $L(\rho, s) = \prod_i L(\tau_i, s)^{n_i}$.

But there's a problem. In general, we know that if we take a 1-dimensional representation, then it's automatically irreducible. Assume it's nontrivial. From Tate's theorem, a nontrivial 1-dimensional representation then the Artin L-function corresponding to it is entire in s.[49] In particular, if χ is nontrivial, $\dim \chi = 1$, then $L(\chi, s)$ is entire.

There's a conjecture of Artin: ρ nontrivial irreducible. Then $L(\rho, s)$ is entire. Thus far, the only known results are that it's known if ρ is 2-dimensional. The method is base change of automorphic representations to get down to the abelian case; there are only finitely many finite subgroups of $SL_2(\mathbb{C})$. Good reference is Michael Artin's textbook in algebra.

We're now going to prove that the Artin L-function is inductive. The situation is this:

[49]Linguistic note: a grössen characer is an idele class character.



Claim is that $L(L/M, \rho, s) = L(L/K, \mathrm{Ind}_H^G(\rho), s)$. This is a local question; we'll prove place by place that the Euler factors coincide.[50]

So assume that L, M, K are local fields. Just go to work and pray that everything works out. So, look at $\mathrm{Ind}_H^G(V)$. Let v be a place of K, $v' \in M$, v'' in L all lying over/under each other. Well, maybe we'll just call them all v. We have to look at the inertia invariants. What's $\mathrm{Ind}_H^G(V)^{I_v}$?

$$\begin{aligned}
\mathrm{Ind}_H^G(V)^{I_v} &= \mathrm{Hom}_{I_v}(\mathbf{1}_{I_v}, \mathrm{Ind}_H^G V|_{I_v}) \\
&= \mathrm{Mor}_G(G/I_v, \mathrm{Ind}_H^G(V)) \\
&= \mathrm{Mor}_H(H/(I_v \cap H), V) \\
&= \mathrm{Ind}_{\mathrm{Gal}(l,m)}^{\mathrm{Gal}(l,k)} V^{I_{v'}}.
\end{aligned}$$

Hmm. We're using the diagram

$$\begin{tikzcd}
1 \arrow[r] & I_v \arrow[r] & G \arrow[r] & \mathrm{Gal}(l,\kappa) \arrow[r] & 1 \\
1 \arrow[r] & I_{v'} \arrow[r] \arrow[u, hook] & H \arrow[r] \arrow[u, hook] & \mathrm{Gal}(l,m) \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

and Frobenius reciprocity, which says that

[50]Why? That's an exercise. The reason, essentially, is $M \otimes_K K_v = \prod_{w|v} M_w$.

$$\mathrm{Hom}_G(W, \mathrm{Ind}_H^G V) = \mathrm{Hom}_H(W, V).$$

Anyways, it's alleged that the identity

$$\mathrm{Ind}_H^G(V)^{I_v} = \mathrm{Ind}_{\mathrm{Gal}(l,m)}^{\mathrm{Gal}(l,k)} V^{I_{v'}}.$$

Let's go compute the local Euler factor.

$$\det(\mathrm{id} - \mathrm{Fr}_v\, q^{-s}|_{\mathrm{Ind}_{\mathrm{Gal}(l,m)}^{\mathrm{Gal}(l,k)} V^{I_{v'}}})^{-1}$$

We're in a simple linear algebra situation. Let W be the induced Galois thing; and T acts on W, it's Gal of something. There's an exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_1 = \mathrm{Z} & \stackrel{n}{\hookrightarrow} & G_2 = \mathrm{Z} & \longrightarrow & \mathrm{Z}/n\mathrm{Z} & \longrightarrow & 1 \\ & & T^n & \longmapsto & T & & & & \end{array}$$

And T operates on W; it's $\mathrm{Ind}_{G_1}^{G_2} W$. Then what we really have is

$$\det(\mathrm{id} - T \cdot X|_{\mathrm{Ind}_{G_1}^{G_2} W}) \;=\; \det(\mathrm{id} - T^n X^n|_W).$$

Example time today, hurray!

Start with quadratic fields. $K = \mathbb{Q}(\sqrt{d})$ with d square free. The ring of integers is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \bmod 4 \end{cases}.$$

[51]

So in the first case, the matrix is $\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}$, whence $d_K = \mathrm{disc}_K = 4d$, and d otherwise. So we typically write

$$\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{d_K} + \sqrt{d_K}}{2}].$$

We know p ramified $\iff p|d_K$. For p unramified, there are two cases. Either the rational prime p stays prime; the inert case; and otherwise it splits into two primes, which is called split. For $p \not| d_K$, if $p \neq 2$, then $\left(\frac{d_K}{p}\right) = 1 \iff p$ splits. What about $p = 2$? In that case ou have to do the same thing. Or, if 2 is unramified, then $d \equiv 1 \mathrm{mod}$, and $d_K = d$. So look at $\mathbb{Z}[\frac{d_K+\sqrt{d_K}}{2}]$. For $\alpha = \frac{d_K+\sqrt{d_K}}{2}$, what is its minimal polynomial? It's $x^2 - \mathrm{tr}(\alpha)x - \mathrm{N}$, i.e., $x^2 - d_K X + \frac{d_K(d_K-1)}{4}$. This splits mod 2 $\iff$ the constant term is zero mod 2. The condition is precisely that $d_K \equiv 1 \bmod 8$.

Now let's talk about units $\mathcal{O}_K^\times$.

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1\} \times \mathbb{Z} & K \text{ real} \\ \{\pm 1\}, \mu_4, \mu_6 & K \text{ imaginary} \end{cases}.$$

If you have an n^{th} root of unity, then the degree of the whole extension is at least $\phi(n)$. That constrains what sort of units you can get.

Now, if K is real, we can try to get a generator for the free part of $\mathcal{O}_K^\times$. For all $\eta \in \mathcal{O}_K^\times$, $\eta \neq \pm 1$, we can get four other units pretty much like it; $\eta, \eta^{-1}, -\eta, -\eta^{-1}$. If $\eta \neq \pm 1$, then these four numbers each lie in a unique interval out of $(0,1)$, $(1,\infty)$, $(-1,0), (-\infty,-1)$. In other words, for a fixed embedding $K \hookrightarrow \mathbb{R}$, and we look at a fixed unit η under that embedding, the four values move around these four intervals. Fix some embedding ι. Then we say η is a normalized fundamental unit with respect to this embedding if $\iota\eta > 1$ and η is a fundamental unit.

[51] Can compute these by writing down the norm and trace, and finding necessary and sufficient conditions for them to be [rational] integers.

Remark: $\eta\eta^\tau = \pm 1$; it's the norm of a unit, and thus must be a unit in Q. So the conjugate of η is one of the four numbers.

And now, an easy characterization of normalized fundamental units. Let's go slow; and at the end we'll answer the original question. Suppose v is a normalized fundamental unit with respect to a fixed embedding ι. We know that, for every unit η with $\iota\eta > 1$, η has the form v^n for some $n \geq 1$. Write $v = x + y\sqrt{d}$; suppose ι is such that $\iota(\sqrt{d}) > 0$. Anyways, $v = x + y\sqrt{d}$ with $x, y \in \mathbb{Q}_{>0}$.

For $n \geq 1$, write $v^n = x_n + y_n\sqrt{d}$. Then

$$\begin{aligned} (x_n + y_n\sqrt{d})(x + y\sqrt{d}) &= xx_n + yy_n d + (xy_n + x_n y)\sqrt{d} \\ x_{n+1} &= xx_n + yy_n d \\ y_{n+1} &= xy_n + x_n y. \end{aligned}$$

Observe that the x_n are either integers of half integers. And if $d \equiv 2, 3 \bmod 4$, then $x_n \geq 1$ since everything's integers. Then $x_{n+1} > x_n$. If $d \equiv 1 \bmod 4$, if $x \geq 1$, then $x_{n+1} > x_n$. So the only hangup is if $x = \frac{1}{2}$. Well, v is a unit. So $N_{K,\mathbb{Q}}(v) = \frac{1}{4} - y^2 d$. Take absolute values; $\left|\frac{1}{4} - y^2 d\right| = 1$. Then $y^2 d = \frac{5}{4}$ or $-\frac{3}{4}$. The second is impossible, since we have a real quadratic extension. Then $y^2 d = \frac{5}{4}$, and $d = 5$; $y = \frac{1}{2}$. And $x_{n+1} = \frac{x_n}{2} + \frac{5}{2}y$. Hold on a minute. $v = \frac{1}{2} + \frac{\sqrt{5}}{2}$. Then every $x_n > \frac{1}{2}$ is $n \geq 2$.

The conclusion is that v is a fundamental unit normalized with respect to $\iota \iff \iota(v)$ and $x < x'$ for every unit $\eta = x' + y'\sqrt{d}$ such that $\iota(\eta) > 1$.

You get uniqueness from this, too.

For example, $\mathbb{Q}(\sqrt{2})$. The smallest possible thing would be $1 + \sqrt{2}$; and this is a unit, so we're done.

Try $\mathbb{Q}(\sqrt{3})$, it's $2 + \sqrt{3}$. $\mathbb{Q}(\sqrt{5})$, get $\frac{1+\sqrt{5}}{2}$.

For real quadratic fields with small discriminant, this is pretty convenient. In general, there's an efficient algorithm which looks at the continued fraction expansion of $\sqrt{d}$. The problem is to find some unit at all; and that comes from Pell's equation, thus named in spite of its irrelevance to Pell and vice-versa.

Move on. Let u be a fundamental unit; we know the other four. Then $N_{K,\mathbb{Q}}(u) = \pm 1$. It's interesting to know which one it is. There are easy criteria to detect when it's one, namely: if the discriminant d_K has a divisor $p \equiv -1 \bmod 4$, then $N_{K,\mathbb{Q}}(\mathcal{O}_K^\times) = 1$. Well, compute

$$N_{K,\mathbb{Q}}\left(a + b\frac{d_K + \sqrt{d_K}}{2}\right) = a^2 + abd_K + \frac{1}{4}b^2 d_K^2 - \frac{1}{4}b^2 d_K$$

$$= \quad a^2 + d_K(ab + b^2(\frac{d_K - 1)}{4})).$$

Suppose this is -1. Then $a^2 \equiv -1 \bmod d_K$; and if $p|d_K$, then -1 is a quadratic residue mod p, and we're done.

So the only case that leaves any doubt is when all the odd prime divisors of the discriminant are congruent to 1 mod 4.

Talk about Riemann-Roch $\Longleftrightarrow$ Poisson summation.

Let K be a global function field i.e., $\mathrm{F}_q(C)$, where C is a smooth, proper geometrically connected algebraic curve over F_q: F_q is the field of constants. Then Poisson summation is equivalent to Riemman-Roch. Here's why; well, a sketch, anyway.

Think about what Riemann Roch says. It says that, for every divisor D on C, you look at sections $H^0(C, \mathcal{O}(D))$, and the dimension of that over F_q. Actually, take

$$\dim_{\mathrm{F}_q}(H^0(C, \mathcal{O}(D)) - \dim_{\mathrm{F}_q} H^1(C, \mathcal{O}(D)) = 1 - g(C) + \deg D.$$

Here, $\dim_{\mathrm{F}_q} H^1(C, \mathcal{O}(D)) = \dim_{\mathrm{F}_q} H^0(C, \Omega_{C,\mathrm{F}_q}(-D))$. That's by Serre duality.

Well, you have to get a hold of $\dim_{\mathrm{F}_q} H^0(C, \mathcal{O}(D))$. This is in additive notation. We can rewrite it as follows.

$$\#H^0(C, \mathcal{O}(D)) \cdot (\#H^1(C, \mathcal{O}(D)))^{-1} \quad = \quad q^{1-g(C)+\deg D}.$$

Poisson summation says that if f is a Schwartz function on adeles, $f \in \mathcal{S}(\mathrm{A}_K)$, then

$$\sum_{\xi \in K} f(\xi) = (\text{const}) \sum_{\eta \in K} \widehat{f}(\eta).$$

In this case, we have no archimedean places. So a Schwartz function is a locally constant function wihth compact support. So we can choose f to be the characteristic function of $\prod_v \mathfrak{p}_v^{-n_v}$, where $D = \sum n_v v$. This thing is compact, and so f is a Schwartz function. Apply Riemann-Roch. Then the left hand side is

$$\sum_{\xi \in K} f(\xi) \quad = \quad \#H^0(C, \mathcal{O}(D)).$$

How do we choose ψ? Pick some 1-form, and use residues; this gives you a pairing. This gives you a nontrivial global additive character ψ, so you can take transforms. That'll more or less give you the right-hand side of the Poisson summation formula. Ω comes in since you choose a 1-form, and the choice of ψ determines the Fourier transform locally. So basically, the $1 - g(C)$ gives you essentially the volume of the fundamental domain, if you make a good choice. Another way of saying this is that you know, well, why do you se the inverse measure? Remember that if $g(x) = f(ax)$, then $\widehat{g}(y) = \int f(ax)\psi(xy)dx = \int f(x)\psi(a^{-1}xy)\frac{dx}{a} = \|a\|^{-1} \widehat{f}(a^{-1}y)$. The inverse inside there is the same as the $-D$ in $\Omega^1_{C,\mathrm{F}_q}(-D)$.

Quadratic Fields Let $K = \mathbb{Q}(\sqrt{d})$ with d square free. Assume for the moment that K is real. If u is a fundamental unit, then $N_{K,\mathbb{Q}}(u) = \pm 1$. But which? Can relate this to ideal class groups versus strict ideal class groups. This'll be essentially Galois cohomological, but we'll pretty much blow that off for now.

Now, the class group is a quotient, so we can write down an exact sequence.

$$0 \to P_K \to I_K \to C_K \to 0.$$

We also define the strict ideal class group C_K^+ as the quotient of principal ideals generated by totally positive elements.

$$\begin{tikzcd}
0 \arrow[r] & P_{K,+} \arrow[r] \arrow[d, hook] & I_K \arrow[r] \arrow[d] & C_K^+ \arrow[r] \arrow[d, two heads, "\pi"'] & 0 \\
0 \arrow[r] & P_K \arrow[r] & I_K \arrow[r] & C_K \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{K,+}^\times \arrow[r] \arrow[d, hook] & K_+^\times \arrow[r] \arrow[d] & P_{K,+} \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathcal{O}_K^\times \arrow[r] & K^\times & P_K \arrow[r] & 0
\end{tikzcd}$$

By diagram chasing or the snake lemma or whatever, we get a long exact sequence. So

$$\ker(C_K^+ \to C_K) \xrightarrow{\cong} \operatorname{coker} = \frac{P_K}{P_{K,+}}$$

$$0 \longrightarrow \mathcal{O}_K^\times / \mathcal{O}_{K,+}^\times \longrightarrow K^\times / K_+^\times \longrightarrow (P_K / P_{K,+}) \longrightarrow 0$$

But we understand the bottom thing. By weak aproximation, there's a surjection $K^\times / K_+^\times \overset{\cong}{\twoheadrightarrow} (\mathbb{Z}/2\mathbb{Z})^2$. Now, $\mathcal{O}_{K,+}^\times \subseteq \mathcal{O}_{K,+}^\times \times \{\pm 1\} \subseteq \mathcal{O}_K^\times$. The index of the first thing is 2, and the second in the last is either 1 or 2. It's one $\iff$ all units have norm 1; and if it's two, then some units have norm -1. Thus, $N_{K,\mathbb{Q}}(u)$ of a fundamental unit u is 1 $\iff$ $\# P_K / P_{K,+} \cong \mathbb{Z}/2\mathbb{Z}$ $\iff$ $\ker(C_K^+ \to C_K) \cong \mathbb{Z}/2\mathbb{Z}$. And $N_{K,\mathbb{Q}}(u) = -1 \iff C_K^+ \overset{\cong}{\twoheadrightarrow} C_K$.

Move on. Consider K over Q. We'll try to understand the 2-torsion subgroup of the strict ideal class group. In other words, the subgroup of the ideal class group killed by 2. Denote this $C_K^+[2]$. We'll figure out a convenient way to undersand this in terms of ramification K/Q. Let R be the subgroup of I_K generated by ramified primes; it's Z^r where r is the number of prime divisors of the discriminant. There's a map $R \to C_K^+$ via $\mathfrak{p} \mapsto [\mathfrak{p}]$. And the square dies, as $\mathfrak{p}^2 = p > 0$. So R/R^2 goes toC_K^+ through the 2-torsion $C_K^+[2]$. Claim that $R/R^2 \to C_K^+$ is actually a surjection. Take $\mathfrak{a}$ a fractional ideal. We're assuming that $\mathfrak{a}^2 = (x)$, $x \in K_+^\times$.

Let $\mathfrak{a} = \prod \mathfrak{p}_v^{n_v}$. Assume that almost all of these are 1; for if there's a 2, well, (p) is one of $\mathfrak{p}_v^2$¡ $\mathfrak{p}_v$, or $\mathfrak{p}_v\mathfrak{p}_{v'}$.

If τ is a nontrivial Galois element, then

$$
\begin{aligned}
\mathfrak{a}\mathfrak{a}^\tau &= N(\mathfrak{a}) = (r) \text{ for some } r \in \mathrm{Q} \\
[\mathfrak{a}] + [\mathfrak{a}\tau] &= 0 \\
[\mathfrak{a}^2] &= [\mathfrak{a}] + [\mathfrak{a}] \\
&= 0 \\
[\mathfrak{a}] &= [\mathfrak{a}\tau] \\
\mathfrak{a}^{1-\tau} &= (y)\ y \in K_+^\times
\end{aligned}
$$

If p splits, then $\mathfrak{a}^{\tau-1} = (y)$ means that, well, we'll see.

We want $z \in K_+^\times$ so that $(\mathfrak{a}z)^\tau = \mathfrak{a}$, ie., $\mathfrak{a}^{1-\tau} = (z^{\tau-1})$. So take $y^{1+\tau}$. Well, $(y)^{1+\tau}$ is the trivial ideal.

Somehow, we're going to get out of this muddle by applying Hilbert's theorem ninety.

Unfortunately, I missed the last class. But we were looking at biquadratic extensions, i.e., K an extension of $\mathbb{Q}$, $G = \mathrm{Gal}(K, \mathbb{Q}) = (\mathbb{Z}/2)^2$.

There are two cases to worry about; K imaginary and K totally real. We saw that

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^r$$

where

$$r = \begin{cases} 1 & \text{imag} \\ 3 & \text{real} \end{cases} .$$

We want a bound for μ_K, which is some cyclic group μ_n. Immediately we find lots of easy bounds; for then we see that $\phi(n) \leq 4$. And since we have ± 1, n must be even. So the only possible primes dividing n are 2, 3 and 5. Consider 5 for a moment. If 5 is there, i.e., $\mu_5 \subseteq \mu_K$, then $\mathbb{Q}(\mu_5) \subseteq K$, and therefore $\mathrm{Gal}(K, \mathbb{Q}) \rightharpoonup \mathrm{Gal}(\mathbb{Q}(\mu_5), \mathbb{Q})$, impossible since one is cyclic order 4 and the other is the Klein 4-group. So 5 is out, and $n = 2^a 3^b$. For such an n, $\phi(n) = 2^a 3^{b-1}$, and it must divide four. Well, $a \leq 3$, and $b \leq 1$. So $n \in \{2, 3, 4, 6, 8, 12\}$. In the last two cases, $\phi(n) = 4$, and so $K = \mathbb{Q}(\mu_8)$ or $\mathbb{Q}(\mu_{12})$. And n must be even, so 3 is out. If $n = 4$, then $K \supseteq \mathbb{Q}(i)$; and if $n = 6$, then $K \supseteq \mathbb{Q}(\mu_3)$.

Go back to the original cases, K imaginary and K totally real. In the first case, well, there's a unique complex conjugation, so there's a real subfield of degree 2; we have $K \overset{\langle\sigma\rangle}{\supset} F \overset{\langle s\rangle}{\supset} \mathbb{Q}$. And in the second case,

$$\begin{tikzcd}
 & K \arrow[dl, dash, "\sigma_1"'] \arrow[d, dash, "\sigma_2"'] \arrow[dr, dash, "\sigma_3"] & \\
k_1 \arrow[dr, dash] & k_2 \arrow[d, dash] & k_3 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

For the various cases, we have

1. $\mathcal{O}_K^\times \supseteq \mu_K \mathcal{O}_F^\times$, and the smaller thing is of finite index.

2. $\mathcal{O}_K^\times \supseteq \mu_K \mathcal{O}_{k_1}^\times \mathcal{O}_{k_2}^\times \mathcal{O}_{k_3}^\times$, again of finite idnex. Sketch; let $v_i \in \mathcal{O}_{k_i}^\times$. And $v_1^{n_1} v_2^{n_2} v_3^{n_3} \in \mu_K$. Consider how the σ_i's act. Then $v_1^{n_1} v_2^{-n_2} v_3^{-n_3} \in \mu_K$ as well, etc; just take conjugates by the σ_i. Ultimately one can conclude that $v_i \in \mu_K$.

From now on we'll concentrate on the first case, an imaginary biquadratic extension. So we have K totally imaginary over F, and K an imaginary biquadratic extension of Q. We want to understand the index of these groups of units. Consider

$$\begin{array}{ccc} \mathcal{O}_K^\times & \to & \mu_K \\ y & \mapsto & y^{1-\sigma} \end{array}$$

[52]

Extend this to $\mathcal{O}_K^\times \to \mu_K/\mu_K^2$. What is the kernel of this map? If $y^{1-\sigma} = \zeta^2$ with $\zeta \in \mu_K$, then $y^{1-\sigma} = \zeta^2 = \zeta^{1-\sigma}$. Thus, $\zeta^{-1}y$ is invariant under σ; $\zeta^{-1}y \in \mathcal{O}_F^\times$. Thus, the kernel is $\mu_K \mathcal{O}_F^\times$. But we know what μ_K/μ_K^2 is; it's isomorphic to $\{\pm 1\}$. So the index $[\mathcal{O}_K^\times : \mu_K \mathcal{O}_F^\times]$ is one or two. Which happens when? If $\mu_K = \{\pm 1\}$, well, hold on.

If $\mu_K \supseteq \mu_6$, then $K = \mathrm{Q}(\zeta_3, \sqrt{d})$ with $d > 0$.

If $\mu_K \supseteq \mu_4$, then $K = \mathrm{Q}(i, \sqrt{d})$, $d > 0$.

If $\mu_K \supseteq \mu_8$ or μ_{12}, then $K = \mathrm{Q}(\mu_8)$ or $\mathrm{Q}(\mu_2)$.

Anyways, assume now that $\mu_K = \{\pm 1\}$ and there exists an odd prime which ramifies in K/F, the imaginary extension. Then the index $[\mathcal{O}_K^\times : \mu_K \mathcal{O}_F^\times] = 1$.

Proof Suppose not; suppose the index is really two. This means that you can find a unit in K whose square is a fundamental unit of F times a root of unity. Symbolically, there's $u \in \mathcal{O}_K^\times$, $\zeta \in \mu_K$ with $u^2 = \zeta v_1 = v_1' = \pm v_1$. And also, $u \notin F$. Then v_1' has a square root in K, and therefore $K = F(\sqrt{v_1'})$. But v_1' is a unit; think about its minimal polynomial, $t^2 - v_1$. So the only possible ramification is at 2, contradicting the assumption.

Now, assume that the norm is $\mathrm{N}_{F,\mathrm{Q}}(v_1) = -1$. If this happens, something very bad will happen. And the index will have to be one; $[\mathcal{O}_K^\times : \mu_K \mathcal{O}_F^\times] = 1$. Let's see why this is the case. If not, then there's a unit $u \in \mathcal{O}_K^\times$ and $\zeta \in \mu_K$ so that $u^2 = \zeta v_1 = v_1'$. Now, $\mathrm{Q}(\sqrt{\zeta})$ is a cyclotomic, and thus abelian, extension of Q. Then so is $K(\sqrt{\zeta})$. In between $K(\sqrt{\zeta})$ and Q we have $\mathrm{Q}(\sqrt{v_1})$. Now, the big extension is abelian, and thus so is the subextension. But there's a problem. We know that v_1's norm is -1; under the two archimedean embeddings, well, under one embedding v_1 is real; and on the other it has an imaginary embedding;

[52]Think about why this lands us in the roots of unity.

$\mathbb{Q}(\sqrt{v_1})$ has both real and imaginary places. Which is sewage, since the extension is abelian; all of its archimedean places are conjugate, and the thing is either totally real or totally imaginary.

Move on to a third case. Suppose we have p_1, p_2 distinct rational primes. Suppose $p_i \equiv -1 \bmod 4$. Consider $K(\mathbb{Q}(\sqrt{-p_1}, \sqrt{-p_2})$. The totally real subextension is $\mathbb{Q}(\sqrt{p_1 p_2}) = F$. We'll see that the index $[\mathcal{O}_K^\times : \mu_K \mathcal{O}_F^\times] = 2$. It's not hard to see that only the p_i ramify in $K/\mathbb{Q}$; but already $\mathbb{Q}(\sqrt{p_1 p_2})$ gives you that ramification. So K/F is unramified. So this gives a piece of the Hilbert class field for F. Given v_1 a fundamental unit of $\mathcal{O}_F^\times$, we know that $\mathrm{N}_{F,\mathbb{Q}}(v_1) = 1$ purely by congruence considerations. Therefore, Hilbert's theorem 90 says that there's a $\rho \in F^\times$ so that $\rho^{1-s} = v_1$.[53]

We may assume that $\rho \in \mathcal{O}_F$, by clearing denominators. Then the ideal (ρ) is equal to $(\rho)^s$. Assume that the divisor (ρ) involves only ramified primes to the first power; $(\rho) | (\sqrt{p_1 p_2})$. There are three cases.

1. $\rho \in \mathcal{O}_F^\times$. That's bad, for then $\mathrm{N}_{F,\mathbb{Q}}(v_1)$ gives us $v_1 = \rho^2$, although v_1 is a fundamental unit.
2. $(\rho) = (\sqrt{p_1 p_2})$. Consider $w = \frac{\rho}{\sqrt{p_1 p_2}}$. Then $w \in \mathcal{O}_F^\times$. So $\rho^{1-s} = (w\sqrt{p_1 p_2})^{1-s} = -w^2 = v_1$, again a contradiction.
3. $(\rho)^2 = (p_1)$. Then $v_1 = \rho^{1-s}$. Write $w = \frac{\rho}{\sqrt{-p_1}} \in \mathcal{O}_K^\times$. Then $v_1 = (w\sqrt{-p_1})^{1-s} \in w^2 \mu_K$. Thus, the index is two.

Exercise Assume $p_1, p_2 > 3$. For then $\mu_K = \{\pm 1\}$. Show that h_K the class number is odd.

[53] Recall that $s = \mathrm{Gal}(F, \mathbb{Q})$, and $\sigma = \mathrm{Gal}(K, F)$.

Cyclotomic fields We saw, as an exercise, that $\mathrm{Q}(\zeta_{p^m})$ is totally ramified over $(p) \subset \mathrm{Q}$, and is unramified outside p. It's an extension of degree $p^{m-1}(p-1) = \varphi(p^m)$. Furthermore, $\mathcal{O}_{\mathrm{Q}(\mu_{p^m})} = \mathrm{Z}[\zeta_{p^m}]$. You first prove the ramification stuff by a calculation of relative differents. To show the integral basis, well, you check it everywhere locally; if true locally it's true. By a different calculation, you know equality holds everywhere outside p. And at p you essentially show that $1-\zeta$ is already a uniformizer. This being totally ramified, you're done. You could also do it with tricks, if you were so inclined.

Now let's try it for general $n = \prod p_i^{m_i}$. Well, you know that $\mathrm{Q}(\zeta_n)$ is the compositum of $\mathrm{Q}(\zeta_{p_i^{m_i}})$. Hence, $\mathrm{Q}(\mu_n)$ over Q is unramified outside the p_i. We also know that its degree is, well, hold on. There's some small problem. The degree certainly divides $\varphi(n)$, i.e., $[\mathrm{Q}(\mu_n) : \mathrm{Q}] | \varphi(n)$. We want to show equality, and ths means that the $\mathrm{Q}(\mu_{p_i^{m_i}})/\mathrm{Q}$ are linearly disjoint over Q. There are many ways to do this. Well, we know that $\mathrm{Gal}(\mathrm{Q}(\mu_{p_i^{m_i}}), \mathrm{Q})$ is $(\mathrm{Z}/p_i^{m_i})^\times$. We know that $\mathrm{Gal}(\mathrm{Q}(\mu_n), \mathrm{Q}) \hookrightarrow (\mathrm{Z}/n\mathrm{Z})^\times$. For the action of a Galois element depends only on its behavior on the roots of unity. Also, $(\mathrm{Z}/n\mathrm{Z})^\times = \prod_i (\mathrm{Z}/p_i^{m_i}\mathrm{Z})^\times$. And the big Galois group surjects on $\mathrm{Gal}(\mathrm{Q}(\mu_{p_i^{m_i}}), \mathrm{Q})$. So we've got a composite surjection

$$\begin{tikzcd}
\mathrm{Gal}(\mathrm{Q}(\mu_n), \mathrm{Q}) \arrow[r, hook] \arrow[d, two heads] & (\mathrm{Z}/n\mathrm{Z})^\times \arrow[d] \\
\mathrm{Gal}(\mathrm{Q}(\mu_{p_i^{m_i}}, \mathrm{Q}) \arrow[r, "="] & (\mathrm{Z}/p_i^{m_i}\mathrm{Z})^\times
\end{tikzcd}$$

Unfortunately, it turns out that this isn't enough. But the linearly disjoint thing comes from the fact that the discriminants are relatively prime to each other.

Let's do it by overkill, using Dirichlet's theorem on primes in arithmetic progressions.[54] If you look at any prime l prime to p, $\mathrm{Gal}(\mathrm{Q}(\zeta_{p^m}), \mathrm{Q})$ is abelian, so there's a unique Frobenius element $\mathrm{Fr}_l \in \mathrm{Gal}$. Claim that, when you send the Galois group to $(\mathrm{Z}/p_i^{m_i})$, $\mathrm{Fr}_l \mapsto l$. This means that the frobenius element applied to any root of unity $\zeta = \zeta_{p_i^{m_i}}$ is just $\mathrm{Fr}_l(\zeta) = \zeta^l$. This has something to do with congruence modulo a prime lying over l. So anyways, now we have a compositum. Take a prime different from all the p_i's. It maps to some element there which is congruent to l mod each $p_i^{m_i}$. Therefore, it's l in $(\mathrm{Z}/n\mathrm{Z})^\times$. But Dirichlet's theorem says that, for any element of $(\mathrm{Z}/n\mathrm{Z})^\times$, you can find some prime which is congruent to it mod n. And that, pretty much, is the proof.

If you want to prove it honestly, use the following lemma.

[54] This has to do with the nonvanishing of L functions at $s = 1$.

Lemma [Exercise] Let L_1 and L_2 be extensions of K, say everything's a number field.[55] Suppose $\mathrm{disc}(L_1, K)$ and $\mathrm{disc}(L_2, K)$ are relatively prime. Then L_1 and L_2 are linearly disjoint.

Linearly disjoint says that $[L_1L_2 : L_1] = [L_2 : K]$, and vice-versa.

Linearly disjoint *does not* mean that their intersection is K. F'rinstance. Consider $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3})$. Each is a cubic field over $\mathbb{Q}$. Their intersection is $\mathbb{Q}$. Their composition is $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. Its degree is six, and not the nine you'd get if they were linearly disjoint.

Suppose L_1 and L_2 are both Galois over K. Does linearly disjoint mean that their interection is K? Well, we've got a tower of groups

$$\begin{tikzcd}[column sep=small]
& \mathrm{Gal}(L_1L_2, K) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathrm{Gal}(L_1L_2, L_1) \arrow[dr, dash] & & \mathrm{Gal}(L_1L_2, L_2) \arrow[dl, dash] \\
& (1) &
\end{tikzcd}$$

Write this as

$$\begin{tikzcd}
& G \arrow[dl, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\
& (1) &
\end{tikzcd}$$

[55] The proof goes through for fraction fields of Dedekind domains, too.

And $H_1 \cap H_2 = (1)$. This is all the information we have. G is the composition of the H_i. This means that, well, $G \hookrightarrow G/H_1 \times G/H_2$. Now, $H_1 H_2$ is the smallest subgroup containing both of them. Well, it seems to me we're basically done; $H_1 \overset{\cong}{\to} G/H_2$.

So we see that if both are Galois then there's no problem. And actually, we only need L_1 and $L_1 L_2/K$ to be Galois.

Back to cyclotomic fields. In the case at hand, you want to say that, suppose we have the compositum of all the factors but one, and that last p_i. We want to show that their intersection is trivial. So you've got $\mathbb{Q}(\zeta_N)$ and $\mathbb{Q}(\zeta_p)$, $(p, n) = 1$. Want to show their intersection is $\mathbb{Q}$. Well, the intersection is contained in $\mathbb{Q}(\zeta_p)$, so only p's may be ramified; and similarly for N. So $\mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_p)$ is unramified over $\mathbb{Q}$. But it sits inside a totally ramified extension. So it must just be $\mathbb{Q}$.

We can formulate a stronger version of the lemma. $\mathcal{O}_{L_1 L_2} = \mathcal{O}_{L_1, K} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2, K}$.

Proof Localize. We may assume that K is a local field. Moreover, L_i may be assumed to both be local, as well. At most one of the L_i is ramified in the local picture. So now we have

$$\begin{tikzcd}
L_1 \arrow[d, dash] & \mathcal{O}L_1 \arrow[l, hook'] \arrow[d, dash] \\
K & \mathcal{O}_K \arrow[l, hook']
\end{tikzcd}$$

Uh-oh. The lemma we wrote down earlier isn't exactly true. Here's why. The problem is that we've ignored the unramified extensions.

Let's try an easy case. Suppose L_1/K totally ramified, L_2/K unramified. And everything's local. Then one can show tha t$\mathcal{O}_{L_1 L_2} = \mathcal{O}_{L_1, K} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2, K}$.

Proof Take L_2/K.

$$\begin{tikzcd}
L_2 \arrow[dr, dash] & & L_1 \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

We know that L_2 is obtained by a separable residue field extension. We can take some monic polynomial $f_2[T]$ so that $f_2[T] \bmod \pi_K$ is separable and irreducible, of degree $[L_2 : K]$.

We also know that L_1 comes from some Eisenstein polynomial. Think of this as an Eisenstein polynomial over L_2. By the same damned criterion, it's irreducible over L_2. And this poly gives the extension $L_1 L_2 / L_2$.

Let's show the stuff about integers. One knows that $\mathcal{O}_{L_1} \otimes \mathcal{O}_{L_2} \subseteq \mathcal{O}_{L_1 L_2}$. But now we have a subring which contains the uniformizer, and which also gives every element in the residue field extension, then it must be the whole works.

Wait. He's writing it down now. In a local field situation you have L/K with rings of integers B and A, respectively. Suppose $B \supseteq C \supseteq A$. Suppose $\pi_B \in C$. Suppose that the composition $C \to B \to B/\pi_B$ is surjective, then $C = B$. That's how you use the completeness; sort of slice it one layer at a time.

So in the lemma at hand, equality holds.

The reason the original lemma fails is that you might have two unramified extensions, and you've got no idea if one is contained in the other.

Now we're trying to redo the lemma we somewhat botched last time. This'll be phrased in terms of number fields, but of course everything works over an arbitrary Dedekind domain.

Proposition Let L_1, L_2 be extensions of K, everything a number field. Suppsoe L_1/K is unramified at primes $\mathfrak{P}_i/\mathfrak{p}$, and L_2/K is totally ramified over $\mathfrak{p}$. Then L_1 and L_2 are linearly disjoint.

Proof It's enough to look at the ramification of some $\mathfrak{P}_i$ in L_1L_2 over L_1. You conclude that it must be totally ramified over each $\mathfrak{P}_i$, and so $[L_1L_2 : L_1] \geq [L_2 : K]$. So they have to be equal, and that's what linearly disjoint means. Remember that we know the ramification index is multiplicative.$\diamond$

This gives us another proof of the fact that, if $n \prod p_i^{m_i}$, p_i's distinct, then $\mathbb{Q}(\mu_{p_i^{m_i}})/\mathbb{Q}$ are linearly disjoint. So we know that $\mathbb{Q}(\mu_n) = \otimes \mathbb{Q}\mathbb{Q}(\mu_{p_i^{m_i}})$. And because of what we proved last time, $\mathcal{O}(\mu_n) = \otimes \mathbb{Z}\mathcal{O}\mathbb{Q}(\mu_{p_i^{m_i}})$.

Now let's talk about units. We know that $\mathbb{Q}(\mu_{p^m})$ is totally ramified at p, and unramified elsewhere; and the degree of the extension is $p^{m-1}(p-1)$. One way to do this is to observe that the cyclotomic polynomial is

$$\begin{aligned} \Phi_{p^m}(X) &= \frac{X^{p^m} - 1}{X^{p^{m-1}} - 1} \\ &= X^{p^{m-1}(p-1)} + X^{p^{m-1}(p-2)} + \cdots + 1 \\ &= \Phi_p(X^{p^{m-1}}). \end{aligned}$$

And $1 - \zeta_{p^m}$ is a uniformizer over p.

For a moment, let's assume $m = 1$ so that $\Phi_p(X) = X^{p-1} + \cdots + X + 1$.

Want to say that $1 - \zeta_{p^m}$ is a uniformizer over p, and a unit elsewhere. We know that $\Phi_p(X^{p^{m-1}}) = \prod_{i \in (\mathbb{Z}/p^m\mathbb{Z})^\times} (X - \zeta_{p^m}^i)$. So

$$p = \prod_{i \in (\mathbb{Z}/p^m\mathbb{Z})^\times} (1 - \zeta_{p^m}^i).$$

And the quotient $\frac{1-\zeta_{p^m}^i}{1-\zeta_{p^m}}$ is a unit. These are the cyclotomic units; and we'll see that they form a subgroup of finite index in the group of all units.

If $n = \prod_{i=1}^{a} p_i^{m_i}$ with $m_i \geq 1$¡ $a \geq 2$. Then we have

$$\begin{aligned}
\frac{X^n - 1}{X - 1} &= \prod_{1 \neq m | n} \Phi_m(X) \\
\Phi_n(X) &= \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^i) \\
\Phi_n(1) &= \prod (1 - \zeta_n^i) \\
\Phi_n(1) &\mid \frac{(X^n - 1)/(X - 1)}{\prod_i \Phi_{p_i^{m_i}}(1) \Phi_{p_i^{m_i - 1}}(1) \cdots \Phi_{p_i}(1)}.
\end{aligned}$$

And from all this, we conclude that $1 - \zeta^n$ is a genuine, honest-to-god unit.

Hmm. We've got the abelian extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$; its Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$. It's abelian and totally imaginary, ramified precisely over primes dividing n. In particular, all the complex conjugations are equal. They're certainly conjugate to each other, but the extension is abelian. Such a situation is called a field with *complex multiplication*

CM fields are central in classfield theory. Any proof of the main theorem uses cyclotomic fields, and sooner or later you run into the following. You define a general reciprocity morphism, and show it has a nice property. You do it like this. You know these properties are satisfied for cyclotomic fields. Then the general theorem is forced to be true as it can't be otherwise.[?]

One thing we know is the following. For every l prime to n, we can talk about the Frobenius element $\mathrm{Fr}_l \in \mathrm{Gal}(\mathbb{Q}(\mu_n, \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where the isomorphism is via the action on the roots of unity. But, in a sense, Fr_l is just l, taken $\bmod n$. For $\mathrm{Fr}_l(\zeta_n) \equiv \zeta_n^l \bmod \mathfrak{l}$, where $\mathfrak{l}$ is over l.. From this characterization of the Frobenii we get the splitting behavior for unramified primes.

F'rinstance, take $\mathfrak{l}$ over l; we want to know the degree of the residue field extension, $f(\mathfrak{l}, l)$. But this is just the order of $l \bmod n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. So l splits completely $\iff$ all the f's have degree one $\iff$ $l \equiv 1 \bmod n$.

We can use this to define the Artin map:

$$\begin{aligned}
\mathrm{rec} : \prod_{(l,n)=1}{}' \mathbb{Q}_l^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times \\
l^i &\mapsto l^i \bmod n
\end{aligned}$$

This is a restricted product, i.e., a subthing of the idele class.

If $a = \frac{b}{c} \in \mathbb{Q}^\times$, $b, c \in \mathbb{Z}$ prime to n, $a \equiv 1 \bmod {}^\times n$[56] then $\mathrm{rec}(a) = 1 \in (\mathbb{Z}/n\mathbb{Z})^\times$.

This is the existence of the conductor for the reciprocity law map.

There's exactly one complex conjugation of $\mathbb{Q}(\mu_n)$; call its fixed field $\mathbb{Q}(\mu_n)^+$. Then $\mathbb{Q}(\mu_n)^+$ is totally real, and $\mathbb{Q}(\mu_n)$ is a CM field. $[\mathbb{Q}(\mu_n)^+ : \mathbb{Q}] = \frac{\varphi(n)}{2}$. What are the Dirichlet ranks of these fields? $\mathbb{Q}(\mu_n)$ has $\frac{\phi(n)}{2} - 1$; but so is $\mathbb{Q}(\mu_n)^+$. So we know that $[\mathcal{O}^\times_{\mathbb{Q}(\mu_n)} : \mu_n : \mathcal{O}^\times_{\mathbb{Q}(\mu_n)^+}] < \infty$, if you assume that $2|n$ so that nothing else happens. Let ι be the complex conjugation. In the case of biquadratic fields, we showed that this index is at most 2. We did this via

$$\begin{array}{rcl} \mathcal{O}^\times_{\mathbb{Q}(\mu_n)} & \to & \mu_n^\times \\ u & \mapsto & u^{1-\iota} \end{array}$$

We want to set the kernel so that we wind up computing the aforementioned index exactly.

$$\begin{array}{rcl} \dfrac{\mathcal{O}^\times_{\mathbb{Q}(\mu_n)}}{\mu_n \mathcal{O}^\times_{\mathbb{Q}(\mu_n)^+}} & \hookrightarrow & \dfrac{\mu_n}{\mu_n^{\times 2}} \\ u & \mapsto & u^{1-\iota} \end{array}$$

And this is injective because if $u^{1-\iota} = \zeta^2$, then $u\zeta \in \mathcal{O}^\times_{\mathbb{Q}(\mu)^+}$.

But the quotient thing on the right is, well, since $2|n$, it's $(\mathbb{Z}/2\mathbb{Z})$. So the index is one or two. Precisely,

$$[\mathcal{O}^\times_{\mathbb{Q}(\mu_n)} : \mu_n : \mathcal{O}^\times_{\mathbb{Q}(\mu_n)^+}] = \begin{cases} 1 & n = p^m \\ 2 & \text{otherwise} \end{cases}.$$

If $n = p^m$, then there's a $u \in \mathcal{O}^\times_{\mathbb{Q}(\mu)}$ so that $u^2 = v\zeta$, where $\zeta \in \mu_n$ and v a fundamental unit of $\mathbb{Q}(\mu_n)^+$. Hmm. Assume $p \neq 2$. Can assume $\zeta = \pm 1$ so that $u^2 = \pm v$, which is absurd. For then $\mathbb{Q}(\mu_{p^m}) = \mathbb{Q}(\mu_{p^m})^+[\sqrt{\pm v}]$. Remember, v is a unit. But the thing is unramified outside 2, and we get a contradiction.

[56] meaning that $b \equiv c \bmod n$.

We have the usual setup for cyclotomic fields. There's $\mathbb{Q}(\mu_n) \supset \mathbb{Q}(\mu_n)^+ \supset \mathbb{Q}$. We saw that there's a map

$$\begin{array}{rcl} \mathcal{O}^{+}_{\mathbb{Q}(\mu_n)} / \mu_{\mathbb{Q}(\mu_n)} \mathcal{O}^{\times}_{\mathbb{Q}(\mu_n)^+} & \hookrightarrow & \mu_{\mathbb{Q}(\mu_n)} / \mu_{\mathbb{Q}(\mu_n)^2} \cong (\mathbb{Z}/2\mathbb{Z}) \\ y & \mapsto & y^{1-\iota} \end{array}$$

where ι is the complex conjugation. We saw that if $n = p^m$, then $\mathcal{O}_{\mathbb{Q}(\mu_n)^+} = \mu_{\mathbb{Q}(\mu_n)} \mathcal{O}^{\times}_{\mathbb{Q}(\mu_n)^+}$. Now, assume that n has ≥ 2 prime divisors. Then we saw that $1 - \zeta_n \in \mathcal{O}^{\times}_{\mathbb{Q}(\mu_n)}$. And it maps to

$$\begin{array}{rcl} 1 - \zeta_n & \mapsto & (1-\zeta_n)^{1-\iota} \\ & = & \dfrac{1-\zeta_n}{1-\zeta_n^{-1}} \\ & = & -\zeta_n^{-1}. \end{array}$$

So we conclude that the map given above is surjective, and thus the index is $[\mathcal{O}^{\times}_{\mathbb{Q}(\mu_n)} : \mu_{\mathbb{Q}(\mu_n)} \mathcal{O}^{\times}_{\mathbb{Q}(\mu_n)^+}] = 2$.

No course on algebraic number theory would be complete without a discussion of quadratic reciprocity.

Let $p > 2$ be prime. Think about $\mathbb{Q}(\mu_p)$. $\mathrm{Gal}(\mathbb{Q}(\mu_p)) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$ even, and so it has a unique quotient of order 2.

$$\begin{array}{c} \mathbb{Q}(\mu_p) \\ \Big| \\ \mathbb{Q}(?) \\ 2\Big| \\ \mathbb{Q} \end{array}$$

So the new field is a quadratic extension, totally ramified over p and unramified outside p. So this says that the discriminant only has p as a divisor. And there's a d so that the thing is

$\sqrt{d}$. Actually, $d = \pm 1$ depending on congruency conditions; $d = \left\{ \begin{array}{ll} -1 & p \equiv -1 \bmod 4 \\ 1 & p \equiv 1 \bmod 4 \end{array} \right\} p$.

So we write this as $\mathrm{Q}(\sqrt{\left(\frac{-1}{p}\right) p})$. we know the spliting behavior from the reciprocity law. For every $l \neq p$ prime, Let $K = \mathrm{Q}(\sqrt{\left(\frac{-1}{p}\right) p})$. Then $\mathrm{Fr}_{l,K/\mathrm{Q}}$ is the restriction of $l \in (\mathrm{Z}/p\mathrm{Z})^\times = \mathrm{Gal}(\mathrm{Q}(\mu_p)/\mathrm{Q})$ to K. How do we recognize if this is the trivial element of $\mathrm{Gal}(k, \mathrm{Q}) = \{\pm 1\}$? It depends exactly on whether l restricted there is trivial or not. But it's the unique quotient of order 2, so it depends precisely on whether l is a square; $\mathrm{Fr}_{l,K/\mathrm{Q}} = \left(\frac{l}{p}\right)$.

So far we haven't used our understanding of K. So on the other hand, l splits in $K \iff \left(\frac{\left(\frac{-1}{p}\right)p}{l}\right) = 1$. So

$$\begin{aligned} \left(\frac{l}{p}\right) &= \left(\frac{\left(\frac{-1}{p}\right) p}{l}\right) \\ &= \left(\frac{p}{l}\right) \left(\frac{\left(\frac{-1}{p}\right)}{l}\right) \\ &= \left(\frac{p}{l}\right) (-1)^{\frac{p-1}{2}\frac{l-1}{2}}. \end{aligned}$$

So much for examples.

Facts about homological algebra *"Homological algebra is something you can mumble about endlessly."*

References: Cartan-Eilenberg. Grothendieck, Sur quelques point de algébra homologique, Tohoku 195?. Verdier, Catégorie Dérivé, Etat 0, SGA $4\frac{1}{2}$.[57]

Here's the idea. The usual idea is this. You've got a functor $F : \mathcal{A} \to \mathcal{B}$ of abelian categories.[58] We usually insist that RF is left exact or right exact. Then you get derived functors measuring the failure of exactness. The derived functors come from resolutions.

There are a couple sort of standard situations.

[57] "Every person should read the classics."

[58] Ad hoc definition of abelian category; it's a subcategory of the category of certain modules in which every map betwen objects has a kernel, cokernel, image and coimage; and the natural map from the coimage to the image is an isomorphism. So just think of it as, say, left-modules over a fixed ring. In algebraic geometry you run into sheaves of modules over some sheaf of rings, possibly over some topos.

1. F is left exact, $\mathcal{A}$ has sufficiently many injectives. In other words, for every $A \in \mathrm{Ob}(\mathcal{A})$, there's $A \to I$ an injection, with I injective.[59] We identify A as a complex concentrated in degree zero; $0 \to A \to 0$. By using the existence of sufficiently many injectives, we imbed $A \hookrightarrow I^0$; and then the quotient into an injective; and keep going. You get a complex

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "\mathrm{quasi-isomorphism}"'] & 0 & & \\ 0 \arrow[r] & I^0 \arrow[r] & I^1 \arrow[r] & I^2 \arrow[r] & \cdot \end{tikzcd}$$

The quasi-isomorphism means that you get an isomorphism of cohomologies. You know you can always find an injective resolution, and thus resolve A by injectives.

We define the derived functor as

$$R^i F(A) \stackrel{\mathrm{def}}{=} H^i(F(I^\bullet)).$$

This is well-defined; it doesn't actually depend in the choice of resolution, since quasi-isomorphism doesn't change homology. It's unique up to chain homotopy.

2. F is right exact. $\mathcal{A}$ has sufficiently any projectives. So for all $A|in\,\mathrm{Ob}(\mathcal{A})$, there's some $A \leftarrow P$ with the map a surjection, P is projective, i.e., $\mathrm{Hom}(P, \cdot)$ is exact.

So all the arrows everywhere are revesed.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & 0 & & \\ 0 & P^0 \arrow[l] \arrow[u, "\mathrm{quasi-isomorphism}"] & P^{-1} \arrow[l] & P^{-2} \arrow[l] & \cdot \arrow[l] \end{tikzcd}$$

[59] Recall that injective means that $\mathrm{Hom}(\cdot, I)$ is exact. So if

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence in $\mathcal{A}$, then

$$0 \to \mathrm{Hom}(M'', I) \to \mathrm{Hom}(M, I) \to \mathrm{Hom}(M', I) \to 0$$

is exact [even on the right!].

The P^i's are projective, and we set $P_i = P^{-i}$. Then define

$$L_i F(A) \stackrel{\text{def}}{=} H_i(F(P_\bullet)).$$

Then everything is still true, provided we reverse the arrows.

Example G a group. $\mathcal{A}$ the category of G-modules. That's he same as the category of $\mathbb{Z}[G]$-modules. Sometimes, you want to fix the coefficient ring, so you could use G-modules over a commutative ring k or whatever. That's an abelian category. Automagically you know a couple of things. First, $\mathcal{A}$ has enough projectives.[60] These projectives are the ones you understand, just the free things. By generality[61], $\mathcal{A}$ has enough injectives. That's a lot harder to prove.[62][63]

[60]That's trivial, sine you have the free obects running around, and any submodule is the image of a free modules; just pick the generator set, and mot out by whatever relations you have running around.

[61]?

[62]Actually, all of this is true for any associate ring R; can look at $R[G]$. And in that context, how do ou construct an embedding intoan injective object? What you do is take lots of direct limits over families indexed by, say, all possible embeddings. The effect of that is that you don'tknow what you're talking about. Can't follow the construction enough to get the information you need. It's a typical existence proof based on the axiom of choice, completely unenlightening.

[63]But if your group isn't too disgusting, you can say a lot more.

We're computing higher derived functors, etc.

Examples Let A be a ring, not necessarily commutative. Let $\mathcal{A}$ be the category of left A-modules. And we'll denote $\mathcal{A}'$ the category of right A-modules. This is the same as the categor of left A^{opp}-modules, where the opposite module is just the thing with the multiplicative action switched. Then we can talk about the extension functors $\operatorname{Ext}^i_A(M, N)$. These are right derived functors of $\operatorname{Hom}_A(\cdot, N)$, which is a left-exact contravariant functor on $\mathcal{A}$ to the category of abelian groups. Or, you can take the right-derived functor $\operatorname{Hom}_A(M, \cdot)$, which is also a functor from $\mathcal{A}$ to the category of abelian groups, except that this time it's covariant. The equivalence of these two things means there's a canonical isomorphism between them.

How do you compute this? Take a projective resolution $P_\bullet \to M$. Then what you want is $H^i(\operatorname{Hom}(P_\bullet, N))$. How do you compute the other thing? Take an injective resolution $N \to I^\bullet$, and then use $H^i(\operatorname{Hom}_A(M, I^\bullet))$. Then show that each of these is equal to the i^{th} cohomology $H^i(\operatorname{Hom}_A(P_\bullet, I^\bullet))$. Everything in sight is canonical.

If M is a right A-module, N a left A-module, then you can form $M \otimes_A N$ an abelian group. Take $\operatorname{Tor}^A_i(M, N)$ is either the i^{th} left-derived functor of $\cdot \otimes_A N$, or the left-derived functor of $M \otimes_A \cdot$.

Let's talk about composition of functors. Suppose you have $\mathcal{A} \xrightarrow{F} \mathcal{B} \xrightarrow{G} \mathcal{C}$. Assume that F and G are both covariant left exact, and both $\mathcal{A}$ and $\mathcal{B}$ have sufficiently many injectives. We make the extra assumption that F(injective) is acyclic with respect to G, i.e., has no higher cohomology. It makes sense to look at $R^\bullet(G \circ F)(A)$. On the other hand, you can take $R^iG(R^jF(A))$. There's a spectral sequence whose $E_2^{i,j}$ term is is this latter thing, whose limit is the former.

Spectral sequence? Wazzat. Look at Serre's paper in *Annals*, his thesis. It's in the collected works, volume I.

We can look at a geometric situation, $f : X \to Y$ a map of topological spaces, $\mathcal{F}$ a sheaf [of coefficients]. Then $\Gamma_Y f_* = \Gamma_X$. From this you get an E_2 spectral sequence with i, j term $E_2^{i,j} = H^i(Y, R^j(f_*(\mathcal{F}))$; and this converges to $H^{i+j}(X, \mathcal{F})$. This is the Leray spectral sequence.

Take a space X and basepoint $*$. Let E be the path space $\{x(t) : x(0) = *, 0 \le t \le 1\}$. There's a natural map $x(t) \mapsto x(1)$. Then a fiber is the loop space with basepoint $*$. Then the $R^if_*(\mathcal{F})$ are essentially the fibers, but the fiber has a monodromy action. When X is an Eilenberg Maclane space, then the fiber F is, too.

Now we can begin some [very simple] group cohomology.

For now, G a group [abstract]. The abelian category we have is $\mathcal{A}$, the set of all left G-modules. So it's left $\mathbb{Z}[G]$-modules. Immediately from what we said, we can specialize our discussion of Tor, etc. First of all, Z with trivial G-action is an object of $\mathcal{A}$. From our discussion, we have $\mathrm{Ext}^i_G(\mathbb{Z}, M) \stackrel{\text{def}}{=} H^i(G, M)$. On the other hand, we can look at $\mathrm{Tor}^i_G(\mathbb{Z}, M) \stackrel{\text{def}}{=} H_i(G, M)$. Of course we have no idea what these are yet. But it's clear that H^0 is just the functor itself, and so $H^0(G, M) = M^G$, the G-invariants of M. Similarly, we can look at cohomology $H_0(G, M) = M_G$, the coinvariants. Concretely, this is $M/\langle \sigma m - m\rangle_{\sigma \in G, m \in M}$. This forces the action to be trivial.

Now, G has an involution $x \mapsto x^{-1}$. This induces a map $\mathbb{Z}[G] \stackrel{\cong}{\to} \mathbb{Z}[G]^{\text{opp}}$. Explicitly, a left G-module M can be made into a right G-module as follows:

If $m \in M$, $g \in G$, then set $mg \stackrel{\text{def}}{=} g^{-1} \cdot m$ where the multiplication on the right hand side is according to the old rule.

So using this construction, M has both a left and right G-action. But you can't expect that these two actions commute, and indeed in general they're not compatible. That is to say that you don't automagically get a $G \times G$ bimodule for free.

Unfortunately, to get this off the ground you need to know something about resolutions. So I guess we're about to construct a resolution. Because in computing group [co]homologies we were talking about Z stuff, our resolution will be of the module Z. If you know anything about algebraic topology, this is called the bar resolution. So if you're so inclined, you can think of things geometrically.

There are two forms of this bar resolution, the inhomogeneous complex and the homogeneous complex. The homogeneous one is the one you'll see when you talk about the bar resolution of some algebra; inhomogeneous is good for explicit formulas. So we'll start with inhomogeneous, as that's how it crops up in Hilbert's theorem 90, with the cocycle condition, etc.

Jam with the inhomogeneous. We want a projective resolution $C_\bullet \to \mathbb{Z}$; usually this is much easier than injective resolutions. That's cause we understand free resolutions [in the category of modules] much better. Anyways, set

$$C_i \stackrel{\text{def}}{=} \mathbb{Z}[G] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[G] = \mathbb{Z}[G]^{\otimes_{\mathbb{Z}} i+1}.$$

The G-action is via the first factor. We want to find differentials among them, arrows $\partial_i : C_i \to C_{i-1}$, and $\epsilon : C_0 \to \mathbb{Z}$ to be acyclic, i.e., exact. So the most convenient thing is to say we have a chain homotopy $h_i : C_i \to C_{i+1}$ so that $\partial_{i+1} h_i - h_{i-1}\partial_i = \mathrm{id}$. We decree that $h_i : C_i \to C_{i+1}$ is given by $\sigma_0 \otimes \cdots \otimes \sigma_i \mapsto 1 \otimes \sigma_0 \otimes \cdots \otimes \sigma - i$. So we've fixed this. How should we define the boundary map? You can inductively define the ∂_i from the h_i's. For the image of the h_i contains a free basis of C_{i+1}, looked upon as a free module over the group ring. And actually, the differential is uniquely determined precisely since $\mathrm{im}\, h_i$ contains a basis.

So this gives an explicit resolution of $\mathbb{Z}$.

Think of $\mathbb{Z} = C_{i-1}$. Then $h_{i-1}(1) = e$, the identity element of $\mathbb{Z}[G]$; so $\epsilon(e) = 1$. Thus, $\epsilon(\sigma) = 1$ for all σ, and that's a unique definition.

We're trying to get a quasi-isomorphism $C_\bullet \to \mathbb{Z}$. Recall that $C_i = \mathbb{Z}[G]^{\otimes_{\mathbb{Z}} i+1}$. And we've got

$$\begin{aligned} h_i : C_i &\to C_{i+1} \\ \sigma_0 \otimes \cdots \otimes \sigma_i &\mapsto e \otimes \sigma_0 \otimes \cdots \otimes \sigma_i. \end{aligned}$$

Want to define the differentials $\partial_i : C_i \to C_{i-1}$ so that $h_{i-1}\partial_i + \partial_{i+1}h_i = \mathrm{id}$.[64] We've decided last time that $\partial_0 = \epsilon$ the augmentation map, $\sigma \mapsto 1$. Let's compute ∂_1. Denote $\sigma_0 \otimes \cdots tensor \sigma_i$ by $\sigma_0[\sigma_1 \otimes \cdots \otimes \sigma_i]$, so that the map h_i is given by $\sigma_0[\sigma_1 \otimes \cdots \otimes \sigma_i] \mapsto [\sigma_0 \otimes \cdots \otimes \sigma_i]$. Anyways, ∂_1 is defined by the condition [remember $i = 0$] $\partial_1(1 \otimes \sigma) + 1 = \sigma$, so that $\partial_1[\sigma] = \sigma - 1$.[65]

Now, set $i = 1$. Then

$$\begin{aligned} \partial_2[\sigma_0, \sigma_1] + h_0\partial_1(\sigma_0[\sigma_1]) &= \sigma_0[\sigma_1] \\ h_0\partial_1(\sigma_0[\sigma_1]) &= h_0(\sigma_0(\sigma_1 - 1)) \\ &= [\sigma_0, \sigma_1] - [\sigma_0] \\ \partial_2[\sigma_0, \sigma_1] &= \sigma_0[\sigma_1] - [\sigma_0, \sigma_1] + [\sigma_0]. \end{aligned}$$

What the hell, let's go for one more and pray we can find the next one – by the pattern, as per Ching-Li's daughter. Set $i = 3$.

$$\begin{aligned} \partial_3[\sigma_0, \sigma_1, \sigma_2] + h_1\partial_2(\sigma_0[\sigma_1, \sigma_2]) &= \sigma_0[\sigma_1, \sigma_2] \\ h_1\partial_1(\sigma_0[\sigma_1, \sigma_2]) &= h_1(\sigma_0\sigma_1[\sigma_2] - \sigma_0[\sigma_1\sigma_2] + \sigma_0[\sigma_1]) \\ \partial_3[\sigma_0, \sigma_1, \sigma_2] &= \sigma_0[\sigma_1, \sigma_2] - [\sigma_0\sigma_1, \sigma_2] + [\sigma_0, \sigma_1\sigma_2] - [\sigma_0, \sigma_1]. \end{aligned}$$

So in general, we have

$$\partial_i[\sigma_1, \sigma_2, \cdots, \sigma_i] = \sigma_1[\sigma_2, \cdots, \sigma_i] + \sum_{j=1}^{i-1} (-1)^j [\sigma_1, \cdots, \sigma_j\sigma_{j+1}, \cdots, \sigma_i] + (-1)^i [\sigma_1, \cdots, \sigma_{i-1}].$$

Using this formula, we've defined a resolution of the trivial G-module, $\mathbb{Z}$.

[64] Changed a sign from last time, but that's no problem. We'll see if this is the right thing to do.
[65] Here, the 1 is the identity element of the group ring, $1 \cdot e$.

Ching-Li is writing ${}^hC$ instead of C^h. We've defined the inhomogeneous complex. One can also define the homogeneous complex $C^h_\bullet \to \mathbb{Z}$, given by $C^h_i = \mathbb{Z}[G]^{\otimes i+1}$. Instead of having G just act on the first term, we'll have it work on all the ocmponents at once with the diagonal G-action. So that

$$\tau(\sigma_0 \otimes \cdots \otimes \sigma_i) \;=\; \tau\sigma_0 \otimes \tau\sigma_1 \otimes \cdots \otimes \tau\sigma_i.$$

Our task now is, well, you've got C_i and C^h_i. Want an isomorphism equivariant under G.

$$\begin{array}{ccc} C_i & \longrightarrow & C_i^h \\ \sigma_0 \otimes \cdots \otimes \sigma_i & \longmapsto & \sigma_0 \otimes \sigma_0\sigma_1 \otimes \sigma_0\sigma_1\sigma_2 \otimes \cdots \otimes \sigma_0\sigma_1\cdots\sigma_i \\ \tau_0 \otimes \tau - 0^{-1}\tau_{\otimes}\tau_1^{-1}\tau_2 \otimes \cdots \otimes \tau_i^{-1}\tau_i & \longleftarrow\!\shortmid & \tau_0 \otimes \tau_1 \cdots \otimes \tau_i \end{array}$$

This clearly gives you a bijection of modules, and it's clearly G-equivariant. Now,

$$\partial_i(\sigma_0[\sigma_1, \cdots, \sigma_i]) \;=\; \sigma_0\sigma_1[\sigma_2, \cdots, \sigma_i] + \sum(-1)^j \sigma_0[\sigma_1, \cdots, \sigma_j\sigma_{j+1}, \cdots, \sigma - i] + (-1)^i \sigma_0[\sigma_1, \cdots, \sigma_{i-1}]$$

And this thing gets sent to or identified with or whatever

$$\tau_1 \otimes \cdots \otimes \tau_i + \sum_{j=1}^{i-1}(-1)^j \tau_0 \otimes \tau_1 \otimes \cdots \otimes \tau_{j-1} \otimes \breve{\tau}_j \otimes \tau_{j+1} \otimes \cdots \otimes \tau_i + (-1)^i \tau_0 \otimes \tau_1 \otimes \cdots \otimes \tau_{i-1}$$

which can be written as just

$$\sum_{j=0}^{i}(-1)^j \tau - 0 \otimes \cdots \otimes \breve{\tau}_j \otimes \cdots \otimes \tau_i.$$

So the advantage is that, in the homogeneous formulation, the differential looks really nice.

"My daughter would certainly not be able to understand anything I'm talking about."

Now, $H^0(G, M) = M^G$, and $H_0(G, M) = M_G$. What about $H^1(G, M)$? You take the complex $C_\bullet \to \mathbb{Z}$, and apply $\mathrm{Hom}(\bullet, M)$ to it. You get $\mathrm{Hom}_G(C_\bullet, M)$, and take the homology via $H^\bullet(\mathrm{Hom}_G(C_\bullet, M))$. Now, the things we're taking homology of are free modules. F'rinstance,

$C_\bullet$ is a free $\mathbb{Z}[G]$-module with basis $G^{\times i} = [\sigma_1, \cdots, \sigma_i]$. So you can identify the homology as $H^\bullet(C^\bullet(G \times \cdots \times G, M))$. Here, the C for some reason means maps. In fact, I'm going to write this as $H^\bullet(\mathrm{Maps}^\bullet(G \times \cdots \times G, M))$. So a typical element looks like $f(\sigma_1, \cdots, \sigma_i)$, it's an i-cochain. What's its differential? It's an $i+1$-cochain, given by

$$df(\sigma_0, \cdots, \sigma_i) \quad = \quad \sigma_0 f(\sigma_1, \cdots, \sigma_i) + \sum (-1)^j f(\sigma_1, \cdots, \sigma_{j-1}\sigma_j, \cdots, \sigma_i) + (-1)^i f(\sigma_0, \sigma_1, \cdots, \sigma_{i-1}).$$

So anyways, $H^1(G, M) = \{f \in \mathrm{Maps}(G, M) : \sigma_0 f(\sigma_1) - f(\sigma_0\sigma_1) + f(\sigma_0) = 0\}$. Some would write this, given the notation $(m^{\sigma_0})^{\sigma_1} = m^{\sigma_1\sigma_0}$ as, oh, never mind. It's a crossed homomorphism. Anyways, you have to mod out by those f so that $f(\sigma) = \sigma m - m$ fo some $m \in M$. This is nothing but coboundaries.

$$H^1(G, M) = \frac{\{\text{crossed homomorphisms}\}}{\{f : f(\sigma) = \sigma m - m \text{ for some } m \in M\}}.$$

Note that if G operates trivially on M, then $H^1(G, M) = \mathrm{Hom}(G, M) = \mathrm{Hom}(G^{\mathrm{ab}}, M)$.

Still playing with group cohomology, of course. We've seen that $H^0(G,M) = M^G$, and $H_0(G,M) = M_G = M/I_G M$ where I_G is the augmentation ideal, which by definition is the kernel in $0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$. So I_G is the $\mathbb{Z}$-span of all elements of the form $\sigma - 1$; it's the elements of the group ring whose coeffs add up to zero. We've seen that $H^1(G,M)$ consists of all classes of crossed homomorphisms. And $H^1(G,M) = (G^{\mathrm{ab}}, \mathbb{Z}) = \mathrm{Hom}_{\mathrm{gp}}(G, \mathbb{Z})$, the characters of G. More generally, $H^1(G,M) = \mathrm{Hom}(G^{\mathrm{ab}}, M)$ if G operates trivialy on M. It's also useful to know that what $H_1(G,\mathbb{Z})$ is. We'll see that this basically becomes the abelianization of G. Could compute it from the standard resolution. Or, could use the exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

Whenever you apply a derived functor to a short exact sequence, you get a long exact sequence. In our case, the functor will be the one taking a module to its coinvariants. Now, $\mathbb{Z}[G]$ is obviously a projective module. By definition, it doesn't have higher cohomology. So take the long exact sequence and get

$$0 \to H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}0 \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0.$$

Since G operates trivially, the coinvariants $H_0(G,\mathbb{Z}) = \mathbb{Z}$. And $H_0(G, \mathbb{Z}[G])$. So we can split the original long exact sequence into the dumb one and

$$0 \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to 0.$$

From which we conclude that $H_1(G,\mathbb{Z}) = H_0(G, I_G) = I_G/I_G^2$. How do we understand this? One way is, well, there's a map

$$\begin{array}{rcl} G & \to & I_G/I_G^2 \\ \sigma & \mapsto & [\sigma - 1]. \end{array}$$

Try to define it on the quotient by the commutator subgroup, the derived group G/G'. So gotta check that $\tau\sigma\tau^{-1}$ goes to the same element. But

$$\begin{array}{rcl} \sigma & \mapsto & [\sigma - 1] \\ \tau & \mapsto & [\tau - 1] \\ \sigma\tau & \mapsto & [\sigma\tau - 1] \\ [\tau\sigma\tau^{-1} - 1] & = & \end{array}$$

So since we're modding out by the square, we ultimately get a map

$$\frac{G}{G'} \to \frac{I_G}{I_G^2}.$$

Surjectivity should be obvious, since the image is just generated by elements of the form $[\sigma - 1]$. How do we prove that it's an injection? Try to define an inverse map

$$\begin{array}{rcl} I_G & \to & G/G' \\ \sum n_\sigma(\sigma - 1) & \mapsto & \prod \sigma^{n\sigma} \end{array}$$

Since the LHS is a free abelian group, this is certainly well-defined. Gotta check that it's really defined on the quotient. But

$$(\sigma - 1)(\tau - 1) \quad \mapsto \quad [\sigma\tau][\sigma]^{-1}[\tau]^{-1} \equiv 1 \bmod G'$$

When all is said and done, we have an isomorphism

$$\frac{I_G}{I_G^2} \cong \frac{G}{G'}.$$

Change of groups Suppose there's a homomorphism $H \to G$, generalizing the situation when $H \subseteq G$ or G is a quotient of H. Let M be an H-module, N a G-module. There are a couple of situations we might be worried about.

1. Suppose $N \to M$ is H-equivariant. We get $H^i(G, N) \to H^i(H, M)$.
2. Suppose $M \to N$ is H-equivariant. Then there's $H_i(H, M) \to H_i(G, N)$.

We'll see shortly how to define them.

1. Let $f \in Z^i(G, N)$, and i^{th} cocycle with coefficients in N; it's a map on $G \times \cdots \times G \to N$ whose derivative is zero. We want to associate to it something in $Z^i(H, N)$. Just do the obvious thing:

$$f \in Z^i(G, N) \to Z^i(H, N) \to Z^i(H, M).$$

This is defined on the level of cochains. Gotta make sure that coboundaries work. But everything commutes with the differentials, so that works.

Can we express this in a more conceptual way? Maybe. Take the standard resolution $C_\bullet(G) \to \mathrm{Z} \to 0$. And $C_\bullet(H) \to \mathrm{Z} \to 0$. These are the bar resolutions, defined in a natural, functorial way. But there's an idiot proof map $C_\bullet(H) \to C_\bullet(G)$ that commutes with the differentials. We've got

$$\begin{tikzcd}
C_\bullet(G) \arrow[r] & \mathrm{Z} \arrow[r] & 0 \\
C_\bullet(H) \arrow[r] \arrow[u] & \mathrm{Z} \arrow[r] \arrow[u, "="'] & 0
\end{tikzcd}$$

From this, get $\mathrm{Hom}_G(C_\bullet(G), N) \to \mathrm{Hom}_H({}_\bullet(G), M)$.

2. We can act similarly in this situation.

$$C_\bullet(H) \otimes_H M \longrightarrow C_\bullet(G) \otimes_G N.$$

Generality of homological algebra says you can extend a map of H^0 to a map on derived functors.

The first map is called the restriction map, and the second one is the corestriction map; Res and Cor. That's cause we're thinking of $H \hookrightarrow G$. But we can also do it where $H \rightharpoonup$; and then this is called inflation Inf. In general, these maps aren't particularly injective or surjective, although they're certainly natural.

1. If $H \hookrightarrow G$ a subgroup, and N a G-module, we often take M to be the same module, N, with the restricted action so we think of it as an H-module.

   If $H \rightharpoonup G$ with kernel K. In this case take an H-module M, and for the G-module take (G, M^K) so that the quotient really acts on it.

2. In the homology case, well, it'll be different from the cohomological story. Start with a G-module (G, N), and restrict its action to get (H, N).

Assume $H \hookrightarrow G$, and M a left H-module. There are two ways to produce a G-module. Both correspond to representation-theory inductions. Recall that a module is a representation. The question becomes, given a representation of a small group, how do you get a representation for a bigger group? The answer, of course, is induction. Two ways to do this.

- $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$. This is naturally a left G-module.
- $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M)$. This is naturally a left G-module.

These look like good things for quiet time.

The second thing is like the group ring for analysts; functions on the group. If you take H trivial and $M = \mathbb{Z}$, the second thing is much bigger than the first.

Lemma [Shapiro]

- $H^i(H, N) = H^i(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], N))$.
- $H_i(H, N) = H_i(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N)$.

This is an easy exercise. The easiest way is probably this. Well, both identities are obvious or $i = 0$. Then use dimension shifting to juice it up.

We used dimension shifting before when we used the long exact sequence associated to

$$I_g \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

Since there are lots of projectives, you can build a sequence like this. And that changes the i^{th} homology to the $(i-1)^{th}$ homology of something else. So that's how you crank up.

Similarly for the cohomological statement, except that we resolve with injections.