

Algebraic Number Theory

Lectures by Ngô Bảo Châu
Notes by Zev Chonoles

The University of Chicago, Spring 2013

Lecture 1 (2013-04-02)	1	Lecture 3 (2013-04-09)	9
Lecture 2 (2013-04-04)	5	Lecture 4 (2013-04-11)	13

Introduction

I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to the lecturer, not to me.

Please email any corrections or suggestions to chonoles@math.uchicago.edu.

Copyright

Copyright © 2013 Zev Chonoles.

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License. This means you are welcome to do essentially anything with this work, including editing, adapting, distributing, and making commercial use of it, as long as you

- include an attribution of Ngô Bảo Châu as the lecturer of the course these notes are based on, and Zev Chonoles as the person taking the notes,
- do so in a way that does not suggest either of us endorses you or your use of this work, and
- if you alter, transform, or build upon this work, you must apply to your work the same, or similar, license to this one.

More details are available at https://creativecommons.org/licenses/by-sa/3.0/deed.en_US.

Lecture 1 (2013-04-02)

This course will be about algebraic number theory. Last year, I followed Neukirch's book. This year, I'll do a different approach, more in the spirit of Weil's book, by starting with adèles.

The prerequisites include basics of commutative algebra and Fourier analysis. My plan is to write a series of books on algebraic number theory and automorphic forms, and my notes for this course will make up the first book, so I appreciate any feedback.

My basic plan for the course is as follows:

1. Valuations of $\mathbb{Q}$
2. Adèles, idèles of $\mathbb{Q}$
3. Integers in number fields
4. Valuations of number fields
5. Local fields
6. Ideal class groups
7. Finiteness theorems in algebraic number theory
8. Adèles and idèles for number fields
9. Haar measure
10. Fourier transform and Pontryagin duality
11. Poisson summation formula
12. Laplace-Mellin transform
13. Iwasawa-Tate construction of the Riemann zeta function, Dirichlet L functions
14. Dedekind zeta functions, Chebotarev density theorem
15. Artin L -functions

There will be one problem set each week (starting next week), and homework will count for 50% of your grade.

Valuations of the field of rational numbers

Recall that $\mathbb{Q}$ has a total order defined by the semigroup $\mathbb{Q}_+$, namely $|\cdot| : \mathbb{Q} \rightarrow \mathbb{Q}_+$ defined by

$$|x| = \begin{cases} x & \text{if } x \in \mathbb{Q}_+, \\ -x & \text{if } x \notin \mathbb{Q}_+. \end{cases}$$

This leads to the notion of $\mathbb{Q}_+$ -valued distance on $\mathbb{Q}$, and then to the notion of Cauchy sequence. The set of real numbers, $\mathbb{R}$, can be defined to be the set of equivalence classes of Cauchy sequences (α_n) in $\mathbb{Q}$ for the equivalence relation $(\alpha_i) \sim (\beta_i)$ when their interlacing / shuffling together forms a Cauchy sequence.

The function $|\cdot|$ extends to a function $\mathbb{R} \rightarrow \mathbb{R}_+$, and $\mathbb{R}$ is complete with respect to this distance.

The Bolzano-Weierstrass theorem says that closed intervals in $\mathbb{R}$ are compact, so we see that $\mathbb{R}$ is locally compact.

Now let's consider different definitions of distance on the rationals. The p -adic valuation of a rational number $\alpha \in \mathbb{Q}$ is defined to be $|\alpha|_p = p^{\text{ord}_p(n) - \text{ord}_p(n)}$ when $\alpha = \frac{m}{n}$, and $\text{ord}_p(k)$ is the exponent of the highest power of p dividing k . Note that this means that a rational number is smaller the more it is divisible by p .

Note that the p -adic valuation satisfies the multiplicative property $|\alpha\beta|_p = |\alpha|_p|\beta|_p$, as well as the ultrametric inequality $|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p)$.

The set of p -adic numbers $\mathbb{Q}_p$ is defined to be the set of equivalence classes of Cauchy sequences of rational numbers with respect to the p -adic valuation. If (α_n) is a Cauchy sequence of p -adic numbers with respect to the p -adic valuation, then $(|\alpha_n|_p)$ is a Cauchy sequence of rational numbers with respect to the usual valuation, and thus $|\cdot|_p$ can be extended to a function $|\cdot|_p : \mathbb{Q}_p \rightarrow \mathbb{R}_+$.

Claim. *The range of the map $|\cdot|_p$ on $\mathbb{Q}_p^\times$ is $p^\mathbb{Z}$.*

Proof. Given a non-zero $\alpha = (\alpha_i)$ in $\mathbb{Q}_p$, the ultrametric inequality implies that there is an N for which all $n > N$ satisfies $|\alpha| = |\alpha_n| \in p^\mathbb{Z}$. $\square$

The ring of p -adic integers is defined to be

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\}.$$

Lemma. *All p -adic integers can be represented by a Cauchy sequence made only of integers.*

Proof. Assume that $|\alpha|_p \leq 1$. Let us represent α as a Cauchy sequence (α_i) of rationals, with $\alpha_i = \frac{p_i}{q_i}$ with $\gcd(p_i, q_i) = 1$.

There is an N such that for all $i > N$, we have

$$p^{-\text{ord}_p(p_i) + \text{ord}_p(q_i)} = \left| \frac{p_i}{q_i} \right|_p = |\alpha_i|_p \leq 1.$$

Therefore $p \nmid q_i$. Thus, there exist $q'_i \in \mathbb{Z}$ such that $|q_i q'_i - 1|_p \leq p^{-i}$. Take $\alpha' = (\alpha'_i) = (p_i q'_i)$. Then α is equivalent to α' , because $\frac{1}{q_i}$ is very close to q'_i . $\square$

$\mathbb{Z}_p$ is the p -adic completion of $\mathbb{Z}$; it cares about congruences modulo p^n . Algebraically,

$$\mathbb{Z}_p = \varprojlim_{n \rightarrow \infty} \mathbb{Z}/p^n \mathbb{Z} = \{\text{sequences of } \overline{\alpha_i} \in \mathbb{Z}/p^i \mathbb{Z} \mid \alpha_i \equiv \alpha_j \pmod{p^i} \text{ for all } i < j\}.$$

$\mathbb{Z}_p$ is a complete local ring, whose maximal ideal is $p\mathbb{Z}_p$, and whose residue field is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$. Note that $\mathbb{Z}_p$ is compact, and $\mathbb{Z}_p$ is a neighborhood of 0 in $\mathbb{Q}_p$, so that $\mathbb{Q}_p$ is locally compact.

The main difference between $\mathbb{R}$ and $\mathbb{Q}_p$ is that $\mathbb{R}$ admits derivations; we can integrate well on both of them, but there is not a good notion of derivation on $\mathbb{Q}_p$.

Note that $\mathbb{Q}_p$ is totally disconnected, and that every element has a basic of compact, open neighborhoods.

Let $|\cdot|_\infty$ denote the real valuation on $\mathbb{Q}$, and let $|\cdot|_p$ denote the p -adic valuation on $\mathbb{Q}$. For any $\alpha \in \mathbb{Q}^\times$, we have that $|\alpha|_p = 1$ for almost all p , and

$$|\alpha|_\infty \prod_{p \text{ prime}} |\alpha|_p = 1.$$

This is known as the product formula. For example, if $\alpha = 64$, we have that $|\alpha|_\infty = 64$, that $|\alpha|_2 = \frac{1}{64}$, and $|\alpha|_p = 1$ for all $p \neq 2$.

Definition. A valuation of $\mathbb{Q}$ is a group homomorphism $|\cdot| : \mathbb{Q}^\times \rightarrow \mathbb{R}_+$ such that $|\alpha + \beta| \leq |\alpha| + |\beta|$. We say that two valuations are equivalent if they define the same topology.

Both $|\cdot|_p$ and $|\cdot|_\infty$ are valuations. There are others, though: for all $t > 0$, $|\cdot|_p^t$ is a valuation, and for all $0 < t \leq 1$, $|\cdot|_\infty^t$ is a valuation. But $|\cdot|_p^t$ is equivalent to $|\cdot|_p$ and $|\cdot|_\infty^t$ is equivalent to $|\cdot|_\infty$.

Theorem (Ostrowski). *Every valuation of $\mathbb{Q}$ is either equivalent to the real valuation, or to a p -adic valuation for some prime p .*

Proof. A valuation $|\cdot| : \mathbb{Q}^\times \rightarrow \mathbb{R}_+$ is said to be a non-archimedean if it is bounded on $\mathbb{Z}$, and archimedean otherwise.

We claim that a valuation is non-archimedean if and only if it satisfies the ultrametric inequality, and in this case, for all $\alpha \in \mathbb{Z}$ we have $|\alpha| \leq 1$. If the ultrametric inequality holds, then $|\cdot|$ is obviously bounded on $\mathbb{Z}$, because for all $n \in \mathbb{N}$, we have $|n| = |1 + \dots + 1| \leq |1| = 1$. Conversely, if there is an A such that $|\alpha| \leq A$ for all $\alpha \in \mathbb{Z}$, then for any α and β (WLOG $|\alpha| \geq |\beta|$),

$$(\alpha + \beta)^n = \sum_{i=0}^n \binom{n}{i} \alpha^i \beta^{n-i},$$

we see that

$$|\alpha + \beta|^n \leq A(n+1)|\alpha|^n,$$

and hence

$$|\alpha + \beta| \leq A^{1/n}(n+1)^{1/n}.$$

As $n \rightarrow \infty$, this coefficient approaches 1, so we see that $|\alpha + \beta| \leq |\alpha|$.

Now, let $|\cdot| : \mathbb{Q}^\times \rightarrow \mathbb{R}_+$ be a non-archimedean valuation. As we've showed, it satisfies the ultrametric inequality, so that for all $n \in \mathbb{Z}$, we have $|n| \leq 1$. We claim that

$$\mathcal{P} = \{\alpha \in \mathbb{Z} \mid |\alpha| < 1\}$$

is a prime ideal of $\mathbb{Z}$. This is because, if $\alpha, \beta \notin \mathcal{P}$, then $|\alpha| = |\beta| = 1$, hence $|\alpha\beta| = 1$, hence $\alpha\beta \notin \mathcal{P}$. If $\mathcal{P} = (0)$, then the valuation is trivial, and if $\mathcal{P} = (p)$, then it is easy to show that $|\cdot|$ must be of the form $|\cdot|_p^t$ for some $t > 0$.

Now let $|\cdot| : \mathbb{Q}^\times \rightarrow \mathbb{R}_+$ be an archimedean valuation. Thus, $|\cdot|$ is not bounded on $\mathbb{Z}$. We claim that if $\beta \in \mathbb{Z}$, $\beta > 1$, then $|\beta| > 1$. If $|\beta| \leq 1$, then for all $\alpha \in \mathbb{N}$, we can write

$$\alpha = a_0 + a_1\beta + \dots + a_r\beta^r$$

by Euclidean division, with $0 \leq a_i \leq \beta - 1$ and $0 < a_r$. For any i , we have $|\beta^i| \leq 1$, and $|\alpha_i| \leq a_i < \beta$ by the triangle inequality. We have that $r \leq \frac{\log(\alpha)}{\log(\beta)}$, so that

$$|\alpha| \leq \left(1 + \frac{\log(\alpha)}{\log(\beta)}\right)\beta,$$

hence for all n ,

$$|\alpha| \leq \left(1 + \frac{n \log(\alpha)}{\log(\beta)}\right)^{1/n} \beta^{1/n},$$

which implies that $|\alpha| \leq 1$. But this contradicts the non-boundedness of $|\cdot|$.

Thus, for all $\beta \in \mathbb{Z}$, $\beta > 1$, we have that $|\beta| > 1$. Now we prove that for all $\alpha, \beta \in \mathbb{Z}$, $\alpha, \beta > 1$,

$$|\alpha|^{1/\log(\alpha)} = |\beta|^{1/\log(\beta)} \implies |\alpha| = |\alpha|_\infty^t$$

for some t . Again write

$$\alpha = a_0 + a_1\beta + \cdots + a_r\beta^r$$

with $0 \leq a_i \leq \beta - 1$ and $0 < a_r$. We have $|a_r| \leq a_r < \beta$, and for all i , we have $|\beta|^i \leq |\beta|^r$. The triangle inequality implies that

$$|\alpha| \leq \left(1 + \frac{\log(\alpha)}{\log(\beta)}\right) \beta^{|\log(\alpha)/\log(\beta)|}.$$

Replacing α by α^n ,

$$|\alpha| \leq \left(1 + \frac{\log(\alpha)}{\log(\beta)}\right)^{1/n} \beta^{1/n} |\beta|^{\log(\alpha)/\log(\beta)}.$$

Letting $n \rightarrow \infty$, we see that for all $\alpha, \beta \in \mathbb{Z}$, $\alpha, \beta > 1$ we have

$$|\alpha|^{1/\log(\alpha)} \leq |\beta|^{1/\log(\beta)}.$$

By switching the roles of α and β , we see that this is an equality. Thus, $|\alpha| = |\alpha|_\infty^t$ for some $t > 0$. The triangle inequality forces $0 \leq t \leq 1$. $\square$

Adèles and idèles for $\mathbb{Q}$

An adèle for $\mathbb{Q}$ is a sequence $(x_p; x_\infty)$ where $x_\infty \in \mathbb{R}$ and $x_p \in \mathbb{Q}_p$, and for almost all p , we have $x_p \in \mathbb{Z}_p$.

This notion was introduced by Chevalley, and the terminology "adèle" was introduced by Weil. We can study the Riemann zeta function very well by doing Fourier analysis on the adèles, though this is not clear from the definition; it seems rather random at first.

The adèles are denoted by $\mathbb{A}$. We break it down as $\mathbb{A} = \mathbb{A}_{\text{fin}} \times \mathbb{R}$, where

$$\mathbb{A}_{\text{fin}} = \{(x_p) \mid x_p \in \mathbb{Q}_p, \text{ and } x_p \in \mathbb{Z}_p \text{ for almost all } p\}.$$

Note that $\prod \mathbb{Z}_p$ is contained in $\mathbb{A}_{\text{fin}}$, and that $\prod \mathbb{Z}_p$ is compact by Tychonoff's theorem. An alternative construction of $\prod \mathbb{Z}_p$ is as

$$\prod \mathbb{Z}_p = \varprojlim_{\substack{n \leq m \\ \text{when } n|m}} \mathbb{Z}/n\mathbb{Z}$$

$$\widehat{\mathbb{Z}} \subset \mathbb{A}_{\text{fin}} \subset \mathbb{Q}.$$

Lecture 2 (2013-04-04)

Adèles and Idèles for $\mathbb{Q}$

Definition. An adèle is a sequence $(x_p; x_\infty)$ such that

- $x_\infty \in \mathbb{R}$
- For all prime numbers p , $x_p \in \mathbb{Q}_p$.
- For almost all prime numbers p , $x_p \in \mathbb{Z}_p$.

The set of adeles is denoted $\mathbb{A}$.

We can decompose the adeles as $\mathbb{A} = \mathbb{A}_{\text{fin}} \times \mathbb{R}$, where

$$\mathbb{A}_{\text{fin}} = \{(x_p) \mid x_p \in \mathbb{Q}_p \text{ for all } p, x_p \in \mathbb{Z}_p \text{ for almost all } p\}$$

Note that

$$\mathbb{A}_{\text{fin}} \supset \prod_p \mathbb{Z}_p = \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}},$$

where the projective limit is taken over the natural numbers with respect to the divisibility order.

This is basically the Chinese remainder theorem. For all natural numbers,

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & & \prod_{i=1}^r \mathbb{Z}/p_i^{m_i}\mathbb{Z} \\ \uparrow & & \uparrow \\ \prod_p \mathbb{Z}_p & \longrightarrow & \prod_{p|n} \mathbb{Z}_p \end{array}$$

Thus the map $\prod_p \mathbb{Z}_p \rightarrow \varprojlim \mathbb{Z}/n\mathbb{Z}$ is injective and surjective, and thus $\mathbb{A}_{\text{fin}} \supset \widehat{\mathbb{Z}}$. By definition, we see that

$$\mathbb{A}_{\text{fin}} = \bigcup_{n \in \mathbb{Z}} n^{-1} \widehat{\mathbb{Z}},$$

where

$$n^{-1} \widehat{\mathbb{Z}} = \{u \in \mathbb{A}_{\text{fin}} \mid nu \in \widehat{\mathbb{Z}}\}.$$

Only finitely many primes divide the denominator of a rational number, so we obtain a diagonal embedding $\mathbb{Q} \hookrightarrow \mathbb{A}_{\text{fin}}$, by sending $\alpha \in \mathbb{Q}$ to (x_p) where each $x_p = \alpha$ in $\mathbb{Q}_p$.

We claim that $\mathbb{A}_{\text{fin}} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$. There is a natural map

$$\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \mathbb{A}_{\text{fin}}$$

because $\widehat{\mathbb{Z}} \subset \mathbb{A}_{\text{fin}}$ and $\mathbb{A}_{\text{fin}}$ is a $\mathbb{Q}$ -vector space. This map is surjective because $\mathbb{A}_{\text{fin}} = \bigcup n^{-1} \widehat{\mathbb{Z}}$. One can check that the map is also injective.

Topology on $\mathbb{A}_{\text{fin}}$

Recall that we give $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ the profinite topology, in which it is compact. This is the same as the product topology on $\prod_p \mathbb{Z}_p$. This can be characterized as the coarsest topology such that all projections $\widehat{\mathbb{Z}} \rightarrow \mathbb{Z}_p$ to be continuous. We can see that this is compact because of Tychonov's theroem.

Now, the topology we put on $\mathbb{A}_{\text{fin}}$ is the finest topology permitting $n^{-1}\widehat{\mathbb{Z}} \hookrightarrow \mathbb{A}_{\text{fin}}$ to be continuous. In particular, $\widehat{\mathbb{Z}}$ is an open, compact subset of $\mathbb{A}_{\text{fin}}$. Thus, we see that $\mathbb{A}_{\text{fin}}$ is locally compact, and therefore $\mathbb{A} = \mathbb{A}_{\text{fin}} \times \mathbb{R}$ is locally compact.

Recall that we can embed $\mathbb{Q} \hookrightarrow \mathbb{A}$ diagonally. You should think of this map as being $\mathbb{Z} \hookrightarrow \mathbb{R}$.

Proposition. *The diagonal embedding $\mathbb{Q} \hookrightarrow \mathbb{A}$ identifies $\mathbb{Q}$ with a discrete cocompact subgroup of $\mathbb{A}$. The quotient $\mathbb{A}/\mathbb{Q}$ can be identified with a profinite covering of $\mathbb{R}/\mathbb{Z}$; in fact it is actually the prouniversal covering of the circle.*

Proof. First, let's prove that the image of $\mathbb{Q}$ is discrete. To do so, it suffices to find a neighborhood of $0 \in \mathbb{A}$ whose intersection with $\mathbb{Q}$ contains only 0 . We consider

$$B = \widehat{\mathbb{Z}} \times (-1, 1) \subset \mathbb{A}_{\text{fin}} \times \mathbb{R}.$$

If $\alpha \in \mathbb{Q} \cap B$, then $\alpha \in \mathbb{Z}_p$ for all p , which implies that $\alpha \in \mathbb{Z}$; but because $\alpha \in (-1, 1)$, we must have $\alpha = 0$.

Consider the exact sequence

$$0 \longrightarrow \widehat{\mathbb{Z}} \times \mathbb{R} \longrightarrow \mathbb{A} \longrightarrow \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

where

$$\bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p = \{(x_p) \mid x_p \in \mathbb{Q}_p/\mathbb{Z}_p \text{ for all } p, x_p = 0 \text{ for almost all } p\}.$$

Including the diagonal embedding in our diagram,

$$\begin{array}{ccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \text{ker}=\mathbb{Z} \\ 0 & \longrightarrow & \widehat{\mathbb{Z}} \times \mathbb{R} & \longrightarrow & \mathbb{A} & \longrightarrow & \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0, \end{array}$$

by applying the snake lemma, we obtain an exact sequence

$$0 \longrightarrow \widehat{\mathbb{Z}} \longrightarrow \widehat{\mathbb{Z}} \times \mathbb{R} \longrightarrow \mathbb{A}/\mathbb{Q} \longrightarrow 0.$$

Thus,

$$\mathbb{A}/\mathbb{Q} \cong (\widehat{\mathbb{Z}} \times \mathbb{R})/\mathbb{Z},$$

where $\mathbb{Z}$ is embedded diagonally. If we divide both sides by $\widehat{\mathbb{Z}}$, we see that

$$\mathbb{A}/(\mathbb{Q} + \widehat{\mathbb{Z}}) \cong \mathbb{R}/\mathbb{Z} = \mathbb{S}^1.$$

For all $n \in \mathbb{N}$, we can instead divide both sides by $n\widehat{\mathbb{Z}} \subset \widehat{\mathbb{Z}}$, from which we obtain

$$\mathbb{A}/(\mathbb{Q} + n\widehat{\mathbb{Z}}) \cong \mathbb{R}/n\mathbb{Z} \xrightarrow{\text{degree } n \text{ covering}} \mathbb{R}/n\mathbb{Z}. \quad \square$$

The Idèles

For all p , we have the inclusion $\mathbb{Z}_p \subset \mathbb{Q}_p$. Recall that $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the p -adic topology. The p -adic absolute value restricts to

$$|\cdot|_p : \mathbb{Q}_p^\times \rightarrow p^{\mathbb{Z}} \subset \mathbb{R}_+.$$

Recall that

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Thus

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p^\times \mid |x|_p = 1\}.$$

We have an exact sequence

$$0 \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{Q}_p^\times \longrightarrow \mathbb{Z} \longrightarrow 0$$

An idèle for $\mathbb{Q}$ is a sequence $(t_p; t_\infty)$ where $t_\infty \in \mathbb{R}^\times$, $t_p \in \mathbb{Q}_p^\times$, and $t_p \in \mathbb{Z}_p^\times$ for almost all p .

The idèles are nothing but invertible adèles. Thus, the idèles are $\mathbb{A}^\times$. We have a decomposition $\mathbb{A}^\times = \mathbb{A}_{\text{fin}}^\times \times \mathbb{R}^\times$, and $\mathbb{Q}^\times$ embeds diagonally in $\mathbb{A}^\times$.

Lemma. $\mathbb{Q}^\times$ is a discrete subgroup of $\mathbb{A}^\times$, where the topology we put on $\mathbb{A}^\times$ is the coarsest topology such that both embedding $t \mapsto t$ and $t \mapsto t^{-1}$ of $\mathbb{A}^\times \hookrightarrow \mathbb{A}$ are continuous. A basis for this topology consists of subsets U of $\mathbb{A}^\times$ of the form

$$U = \prod_{p \in S} U_p \times \prod_{p \notin S} \mathbb{Z}_p^\times \times U_\infty.$$

Thus, $\mathbb{A}^\times$ is locally compact.

Proof. Consider the following neighborhood of $1 \in \mathbb{A}^\times$:

$$U = \widehat{\mathbb{Z}}^\times \times \mathbb{R}^\times = \prod_p \mathbb{Z}_p^\times \times \mathbb{R}^\times.$$

If $\alpha \in \mathbb{Q}^\times \cap U$, then $\alpha \in \mathbb{Z}_p^\times$ for all p , so that $\alpha \in \mathbb{Z}^\times = \{\pm 1\}$. Thus, $\mathbb{Q}^\times$ is a discrete subgroup. $\square$

We can consider valuations $\mathbb{A}^\times \rightarrow \mathbb{R}_+$ on the idèles. There is the real valuation, defined by sending $(t_p; t_\infty)$ to $|t_\infty|_\infty$, and there are p -adic valuations, defined by sending $(t_p; t_\infty)$ to $|t_p|_p$. Because $t_p \in \mathbb{Z}_p^\times$ for almost all p , we have that $|t|_p = 1$ for almost all $t \in \mathbb{A}^\times$. Thus, we can define

$$|t| = |t|_\infty \prod_p |t|_p$$

for any $t \in \mathbb{A}^\times$. We have an exact sequence

$$1 \longrightarrow \mathbb{A}^1 \longrightarrow \mathbb{A}^\times \xrightarrow{|\cdot|} \mathbb{R}_+ \longrightarrow 1,$$

and the product formula tells us that $\mathbb{Q}^\times \subset \mathbb{A}^1$ (the group of idèles of norm one).

Proposition. $\mathbb{Q}^\times$ is a discrete cocompact subgroup of $\mathbb{A}^1$.

More precisely, $\mathbb{A}^\times$ can be decomposed as a direct product

$$\mathbb{A}^\times = \mathbb{Q}^\times \times \widehat{\mathbb{Z}}^\times \times \mathbb{R}_+.$$

where

- $\mathbb{Q}^\times$ is the diagonal subgroup $\mathbb{Q}^\times \subset \mathbb{A}^\times$,
- $\widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ is the compact subgroup $\{(t_p; t_\infty) \mid t_p \in \mathbb{Z}_p^\times, t_\infty = 1\}$, and
- $\mathbb{R}_+$ is the subgroup $\{(t_p; t_\infty) \mid t_p = 1 \text{ for all } p, t_\infty \in \mathbb{R}_+\}$.

We can think of

- $\mathbb{Q}^\times$ as “the discrete part”,
- $\widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ as “the compact part”, and
- $\mathbb{R}_+$ as “the norm part” (or “the module part”, if you want to use Weil’s terminology).

Let’s formulate this as a claim:

Claim. *For all $x \in \mathbb{A}^\times$ can be written uniquely in the form $x = \alpha u t$ where $\alpha \in \mathbb{Q}^\times$, $u \in \widehat{\mathbb{Z}}^\times$, and $t \in \mathbb{R}_+$.*

The idea of the proof is to use the fact that “integers can be written as the product of prime numbers”.

If $x = (x_p, x_\infty)$, then $x_\infty \in \mathbb{R}_+$, $x_p \in \mathbb{Q}_p^\times$, and $x_p \in \mathbb{Z}_p^\times$ for almost all p . We can write every x_p as $x_p = m_p p^{-r_p}$ where x

Lecture 3 (2013-04-09)

We've talked about adèles over the rationals; now let's move to number fields.

A number field is a finite extension of $\mathbb{Q}$. We can construct number fields by taking $p \in \mathbb{Q}[x]$, an irreducible polynomial of degree n , and forming the quotient $\mathbb{Q}[x]/(p)$. Note that this is an n -dimensional $\mathbb{Q}$ -vector space. This is a domain because p is irreducible. For all $\alpha \in \mathbb{Q}[x]/(p)$ other than the zero element, multiplication by α is an injective map, and finite-dimensionality implies it is also surjective. Thus, $\mathbb{Q}[x]/(p)$ is a field.

In fact, all number fields can be constructed this way. Given a finite extension $L/\mathbb{Q}$, if we want to write L as $L \cong \mathbb{Q}[x]/(p)$ for some irreducible polynomial p , we just need to find an element of L that can correspond to x . This exists because all finite extensions of characteristic zero fields can be generated by a single element. We won't prove this now; a reference is Lang's *Algebra*, V.4.6.

Let $L/\mathbb{Q}$ be a finite extension of degree n , and let $\alpha \in L$. We define the trace $\text{tr}_{L/\mathbb{Q}}(\alpha)$ and the norm $N_{L/\mathbb{Q}}(\alpha)$ to be the trace and determinant, respectively, of the linear transformation $L \rightarrow L$ defined by multiplication by α . We define $\text{ch}(\alpha)$ to be the polynomial

$$\text{ch}(\alpha) = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n \in \mathbb{Q}[x]$$

that is the characteristic polynomial of the $\mathbb{Q}$ -linear transformation that is multiplication by α . Note that $c_1 = \text{tr}_{L/\mathbb{Q}}(\alpha)$ and $c_n = N_{L/\mathbb{Q}}(\alpha)$. Thus, if $\alpha_1, \dots, \alpha_n$ are the roots of $\text{ch}(\alpha)$, then

$$\text{tr}_{L/\mathbb{Q}}(\alpha) = \alpha_1 + \cdots + \alpha_n \quad N_{L/\mathbb{Q}}(\alpha) = \alpha_1 \cdots \alpha_n.$$

Proposition. *Let L be a finite extension of $\mathbb{Q}$ and let $\alpha \in L$. Then the following properties are equivalent:*

1. *The ring $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$ -module.*
2. *All the coefficients $c_1, \dots, c_n$ of $\text{ch}(\alpha)$ are integers.*

When this is the case, we say that α is an integral element of L .

Proof. Assume that $\mathbb{Z}[\alpha]$ is a finitely generated sub- $\mathbb{Z}$ -module of L . Note that we have

$$\mathbb{Z}[\alpha] \subset \mathbb{Q}(\alpha) \subseteq L,$$

and that $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$. Let r be the dimension of L over E .

Choose a basis of the $\mathbb{Z}$ -module $\mathbb{Z}[\alpha]$. Because multiplication by α defines a $\mathbb{Z}$ -linear transformation of $\mathbb{Z}[\alpha]$, we see that its matrix is integral, and thus $\text{ch}_{E/\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. This implies that

$$\text{ch}_{L/\mathbb{Q}}(\alpha) = \text{ch}_{E/\mathbb{Q}}(\alpha)^r \in \mathbb{Z}[x],$$

because $L = Ev_1 \oplus \cdots \oplus Ev_r$.

Now we prove the other direction. Assume that $\text{ch}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. Then $1, \alpha, \dots, \alpha^{n-1}$ forms a $\mathbb{Z}$ -basis of $\mathbb{Z}[\alpha]$, because any higher powers can be written as $\mathbb{Z}$ -linear combinations of $1, \alpha, \dots, \alpha^{n-1}$. Thus $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$ -module. $\square$

We define

$$\mathcal{O}_L := \{\text{integral elements of } L\}.$$

If $\alpha, \beta \in \mathcal{O}_L$, then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$ -modules, hence $\mathbb{Z}[\alpha, \beta]$ is finitely generated, and because $\alpha + \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$, we have that $\mathbb{Z}[\alpha + \beta]$ and $\mathbb{Z}[\alpha\beta]$ are finitely generated as well. Thus $\alpha + \beta$ and $\alpha\beta$ are elements of $\mathcal{O}_L$, and we see that $\mathcal{O}_L$ is a ring.

Canonical symmetric form on L

We define a form on L via

$$\langle \alpha, \beta \rangle \mapsto \operatorname{tr}_{L/\mathbb{Q}}(\alpha\beta) \in \mathbb{Q}.$$

This is a symmetric bilinear form on L (viewed as a $\mathbb{Q}$ -vector space).

Proof. For any number field L , there is a generating element α . Thus $L \cong \mathbb{Q}[x]/(p)$ where p is the characteristic polynomial of α . Thus, $1, \alpha, \dots, \alpha^{n-1}$ is a $\mathbb{Q}$ -basis of L . Because the characteristic polynomial is irreducible over a field of characteristic 0, we know that it is separable, and thus $p'(\alpha) \neq 0$.

Recall the Euler formula

$$\operatorname{tr}_{L/\mathbb{Q}}\left(\frac{\alpha^i}{p'(\alpha)}\right) = \begin{cases} 0 & \text{if } i = 0, \dots, n-2, \\ 1 & \text{if } i = n-1. \end{cases}$$

Proof of the Euler formula: Expanding $\frac{1}{p}$ as a linear combination of $\frac{1}{x-\alpha_1}, \dots, \frac{1}{x-\alpha_n}$, we have

$$\frac{1}{p} = \frac{1}{p'(\alpha_1)(x-\alpha_1)} + \dots + \frac{1}{p'(\alpha_n)(x-\alpha_n)}.$$

Expanding this equality as power series in $\frac{1}{x}$,

$$\frac{1}{p} = \frac{1}{x^n - c_1 x^{n-1} + \dots} = \frac{1}{x^n} + \frac{d_{n-1}}{x^{n-1}} + \dots$$

and

$$\frac{1}{x - \alpha_i} = \frac{1}{x} + \frac{\alpha_i}{x^2} + \frac{\alpha_i^2}{x^3} + \dots,$$

so that

$$\sum_{j=1}^n \frac{\alpha_j^i}{p'(\alpha_j)} = \begin{cases} 0 & \text{if } i = 0, \dots, n-2, \\ 1 & \text{if } i = n-1. \end{cases}$$

Thus, if we write the matrix of $\langle \alpha, \beta \rangle \mapsto \operatorname{tr}_{L/\mathbb{Q}}(\alpha\beta) \in \mathbb{Q}$ as starting in the basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ and ending in the basis $\{\frac{1}{p'(\alpha)}, \dots, \frac{\alpha^{n-1}}{p'(\alpha)}\}$, it is lower triangular, of the form

$$\begin{bmatrix} 1 & & \\ \vdots & \ddots & \\ * & \dots & 1 \end{bmatrix}$$

and therefore, in particular, invertible. □

Proposition. *The ring of integers $\mathcal{O}_L$ of L is a finitely generated $\mathbb{Z}$ -module.*

Proof. The bilinear form $\langle \alpha, \beta \rangle = \operatorname{tr}_{L/\mathbb{Q}}(\alpha\beta)$, restricted to $\mathcal{O}_L$, defines a bilinear form $\mathcal{O}_L \times \mathcal{O}_L \rightarrow \mathbb{Z}$.

Assume there is a finitely generated $\mathbb{Z}$ -module of rank n , where $M \subset \mathcal{O}_L$. Then

$$0 \subseteq M \subseteq \mathcal{O}_L \subseteq \mathcal{O}_L^\perp \subseteq M^\perp,$$

where

$$\mathcal{O}_L^\perp = \{\beta \in L \mid \operatorname{tr}_{L/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}\}.$$

Since M is finitely generated of rank n , so is $M^\perp$, and thus so is $\mathcal{O}_L$.

Now it remains to construct M . Let $\alpha \in L$ be a generating element of L ; note that α may not be an element of $\mathcal{O}_L$. However, we can find an $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}_L$ (get rid of denominators in the coefficients of the characteristic polynomial). Then set $M = \mathbb{Z}[\alpha]$. Because $\alpha \in \mathcal{O}_L$, we know that it is finitely-generated, and it has rank n because $1, \alpha, \dots, \alpha^{n-1}$ is a basis of L . $\square$

$$\begin{array}{ccc} \mathbb{Q}\text{-vector spaces} & L \times L & \longrightarrow \mathbb{Q} \\ & \uparrow & \uparrow \\ \text{f.g. } \mathbb{Z}\text{-modules of rank } n & \mathcal{O}_L \times \mathcal{O}_L & \longrightarrow \mathbb{Z} \end{array}$$

We have that $\mathcal{O}_L \subseteq \mathcal{O}_L^\perp$; because both are of rank n , the index $[\mathcal{O}_L^\perp : \mathcal{O}_L]$ is finite. This quantity is known as the discriminant of L .

Valuations of number fields

A valuation of a number field L is a homomorphism $|\cdot| : L^\times \rightarrow \mathbb{R}_+$ such that $|\alpha + \beta| \leq |\alpha| + |\beta|$. We say that $|\cdot|$ is non-archimedean if its restriction to $\mathcal{O}_L$ is bounded, and that it is archimedean if it is unbounded.

Let $|\cdot| : L^\times \rightarrow \mathbb{R}_+$ be a valuation. Then its restriction to $\mathbb{Q}^\times$ is a valuation of $\mathbb{Q}$, which we know is equivalent to either the real valuation, or to a p -adic valuation.

Proposition. *A valuation of L is archimedean if and only if its restriction to $\mathbb{Q}$ is equivalent to the real valuation, and non-archimedean if and only if its restriction to $\mathbb{Q}$ is equivalent to a p -adic valuation. In the non-archimedean case, the valuation satisfies the ultrametric inequality, and for all $\alpha \in \mathcal{O}_L$, we have that $|\alpha| \leq 1$.*

Proof. If $|\cdot|_{\mathbb{Q}}$ is equivalent to the real valuation, then it is unbounded on $\mathbb{Z}$, and hence it is unbounded on $\mathcal{O}_L$.

If $|\cdot|_{\mathbb{Q}}$ is equivalent to a p -adic valuation, then we claim that it is bounded on $\mathcal{O}_L$. Recall that for all $a \in \mathbb{Z}$, we have that $|a| \leq 1$. Thus, for all $\alpha \in \mathcal{O}_L$, α satisfies an equation of the form

$$\alpha^n + c_1\alpha^{n-1} + \dots + c_n = 0,$$

where $c_1, \dots, c_n \in \mathbb{Z}$. Thus,

$$|\alpha^n| \leq |\alpha^{n-1}| + \dots + 1,$$

and therefore $|\alpha|$ is bounded by some constant. The fact that $|\cdot|$ is bounded implies that $|\alpha| \leq 1$ for all $\alpha \in \mathcal{O}_L$, by the same argument as we used for the integers. $\square$

Definition. We say that two valuations on L are equivalent if they induce the same topology. A place of L is defined to be an equivalence class of valuations on L . We write

$$\overline{\mathcal{P}}_L = \mathcal{P}_L \cup \mathcal{P}_\infty,$$

to express that the places of L can be broken into the finite (non-archimedean) places and infinite (archimedean) places of L . They restrict to the places of $\mathbb{Q}$,

$$\overline{\mathcal{P}} = \{\text{primes}\} \cup \{\infty\}.$$

When u , a place of L , restricts to v , a place of $\mathbb{Q}$, we write $u|v$.

Exercises.

1. What are the places $\{u \in \overline{\mathcal{P}}_L \mid u|v\}$?
2. What is L_u , the completion of L with respect to u ?

Lecture 4 (2013-04-11)

Proposition. *Let L be a number field and let v be a place of $\mathbb{Q}$. Then $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a product of finite extensions of $\mathbb{Q}_v$. The set of places $u|v$ is in bijection with the factors in this product, via $u \mapsto L_u$.*

Proof. We can write $L = \mathbb{Q}[x]/(p)$ where $p \in \mathbb{Q}[x]$ is a separable polynomial. Thus,

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong \mathbb{Q}_v[x]/(p) \cong \prod_{i=1}^n \mathbb{Q}_v[x]/(p_i)$$

where the p_i are the irreducible factors of p in $\mathbb{Q}_v[x]$ (distinct because p is separable).

Because we have inclusions $L \hookrightarrow L_u$ and $\mathbb{Q}_v \hookrightarrow L_u$, we know that we have a map $L \otimes_{\mathbb{Q}} \mathbb{Q}_v \rightarrow L_u$. Because $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a finite dimensional $\mathbb{Q}_v$ -vector space, its image in L_u is also finite dimensional. Thus, it is closed in L_u . But L is dense in L_u (by definition), so the map $L \otimes_{\mathbb{Q}} \mathbb{Q}_v \rightarrow L_u$ is surjective. Therefore, L_u is finite dimensional, and a factor of $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$. This shows that the set of places $u|v$ is a subset of the set of factors of $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$.

It remains to prove that every factor of $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$ can be obtained as the completion of L with respect to a valuation.

Let F be a finite extension of $\mathbb{Q}_v$. We can define a valuation on F by

$$|\alpha| = |N_{F/\mathbb{Q}_v}(\alpha)|_v^{1/[F:\mathbb{Q}_v]}$$

The exponent is there to ensure that if $v = p$, then $|p| = p^{-1}$. For any map, $L \otimes_{\mathbb{Q}} \mathbb{Q}_v \rightarrow F$ by composing with the inclusion $L \hookrightarrow L \otimes_{\mathbb{Q}} \mathbb{Q}_v \rightarrow F$, this defines a valuation on L extending v :

$$\begin{array}{ccc} L^\times & \longrightarrow & \mathbb{R}_+ \\ | & & | \\ \mathbb{Q}_v^\times & \longrightarrow & \mathbb{R}_+ \end{array}$$

Check that this is a valuation (triangle inequality), and show that F is the completion of L with respect to this valuation (this is because L is dense in $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$, hence its image is dense in F , and since $|\cdot|$ extends to F , we must have that F is the completion of L . $\square$

Basic local fields

The completions of $\mathbb{Q}$ are the various $\mathbb{Q}_p$ and $\mathbb{R}$; we say that these are the basic local fields. Local fields are just finite extensions of basic local fields. The only non-trivial extension of $\mathbb{R}$ is $\mathbb{C}$.

Lemma. *All continuous homomorphisms $\chi : \mathbb{C}^\times \rightarrow \mathbb{R}_+$ are of the form $z \mapsto |z|^t$ for some $t \in \mathbb{R}_+$. This satisfies the triangle inequality if and only if $0 \leq t \leq 1$.*

Proof. Because $\mathbb{S}^1 \subset \mathbb{C}$ is compact, we have that $\chi(\mathbb{S}^1)$ is a compact subgroup of $\mathbb{R}_+$, so it must be the trivial subgroup. It is easy to show that the only continuous homomorphisms $\mathbb{R}_+ \rightarrow \mathbb{R}_+$ are of the form $x \mapsto x^t$ for some $t \in \mathbb{R}_+$. $\square$

Proposition. *Let $F/\mathbb{Q}_p$ be a finite extension. Then all continuous homomorphisms $F^\times \rightarrow \mathbb{R}_+$ are of the form $\alpha \mapsto |\mathbf{N}_{F/\mathbb{Q}_p}(\alpha)|_p^t$ for some $t \in \mathbb{R}_+$. These satisfy the triangle inequality (in fact, the ultrametric inequality).*

Proof. Let $\alpha \in F$ and let $\text{ch}(\alpha) \in \mathbb{Q}_p[x]$. As in the case of a number field, we define

$$\mathcal{O}_F = \{\alpha \in F \mid \text{ch}(\alpha) \in \mathbb{Z}_p[x]\}.$$

This is a subring of F , and $\mathcal{O}_F$ is finitely generated as a $\mathbb{Z}_p$ -module.

Let $|\cdot| : F^\times \rightarrow \mathbb{R}_+$ be a continuous homomorphism extending the p -adic valuation on $\mathbb{Q}_p$. We claim that $\mathcal{O}_F = \{\alpha \in F \mid |\alpha| \leq 1\}$.

To prove this claim, let us first prove that for any $\alpha \in \mathcal{O}_F$, we have $|\alpha| \leq 1$. Because $\mathcal{O}_F$ is a $\mathbb{Z}_p$ -module of finite type, we have that it is a compact subset of F , and $|\cdot|$ is continuous, so $|\cdot|$ is bounded on $\mathcal{O}_F$. As we've seen before, this implies that it is in fact bounded by 1.

Now, we prove the other direction of the claim: we want to show that if $|\alpha| \leq 1$, then α is an integral element of F . We know that F is a finite dimensional $\mathbb{Q}_p$ -vector space, say of dimension r , so let's choose a basis $v_1, \dots, v_r$, which specifies a (topological and algebraic) isomorphism $\mathbb{Q}_p^r \xrightarrow{\cong} F$. The set $\bigoplus_{i=1}^r \mathbb{Z}_p v_i$ is a compact open neighborhood of 0.

We define the sets $F_t = \{\alpha \in F \mid |\alpha| < t\}$. These are a neighborhood base of 0, so there is some t such that $F_t \subset \bigoplus_{i=1}^r \mathbb{Z}_p v_i$. Because F_t is a $\mathbb{Z}_p$ -module contained in $\bigoplus_{i=1}^r \mathbb{Z}_p v_i$, we know that F_t is finitely generated. For all α with $|\alpha| \leq 1$, we have that multiplication by α stabilizes F_t , so that $\text{ch}(\alpha) \in \mathbb{Z}_p[x]$.

Thus, the set $\mathfrak{m}_F = \{x \in F \mid |x| < 1\}$ is independent of whatever $|\cdot|$ was, and moreover this is an ideal. We have that

$$\mathcal{O}_F - \mathfrak{m}_F = \{x \in F \mid |x| = 1\} = \mathcal{O}_F^\times,$$

so that $\mathfrak{m}_F$ is the unique maximal ideal of $\mathcal{O}_F$. We also see that $|\cdot|$ is ultrametric, because it is bounded on $\mathcal{O}_F$.

Now we will prove that $\mathfrak{m}_F$ is generated by a single element x_1 . This will imply that, for all $x \in F^\times$, there is an $n \in \mathbb{Z}$ such that $x = x_1^n y$, for some $y \in \mathcal{O}_F^\times$, and hence $|x| = |x_1|^n$ because $|y| = 1$. Thus, we can classify all valuations from a single value $|x_1|$.

The ring $\mathcal{O}_F$ is a finitely generated $\mathbb{Z}_p$ -module, so that $\mathcal{O}_F$ is noetherian. Thus $\mathfrak{m}_F$ is a finitely generated as a $\mathcal{O}_F$ -module. Pick generators $x_1, \dots, x_n$ of $\mathfrak{m}_F$, and WLOG we have $|x_1| \geq \dots \geq |x_n|$. For all $x \in \mathfrak{m}_F$, we have

$$x = x_1 y_1 + \dots + x_n y_n$$

Thus $|x| \leq |x_1|$ for all $x \in \mathcal{O}_F$. □

Let ϖ be a generator of $\mathfrak{m}_F$. We call this a uniformizing parameter. Because $p \in \mathbb{Z}_p$, there is some $e \in \mathbb{N}$ such that $p = \varpi^e$. This number e is known as the absolute ramification index.

There is an extension of residue fields $\kappa_F = \mathcal{O}_F/\mathfrak{m}_F$ over $\mathbb{F}_p$, and the degree d of this extension is known as the residue degree.

Lemma. *For any finite extension $F/\mathbb{Q}_p$, we have $[F : \mathbb{Q}_p] = de$.*

Proof. We have that $\mathcal{O}_F/p\mathcal{O}_F = \mathcal{O}_F/\varpi^e\mathcal{O}_F$, and this clearly has a filtration

$$\mathcal{O}_F/\varpi^e\mathcal{O}_F \longrightarrow \mathcal{O}_F/\varpi^{e-1}\mathcal{O}_F \longrightarrow \cdots \longrightarrow \mathcal{O}_F/\varpi\mathcal{O}_F = \kappa_F$$

with κ_F the kernel at each step. Equivalently, one can show that $\mathcal{O}_F/p\mathcal{O}_F$ is a κ_F -vector space with basis $1, \varpi, \dots, \varpi^{e-1}$ by induction, so that $\dim_{\kappa_F}(\mathcal{O}_F/p\mathcal{O}_F) = e$, and hence

$$r = \dim_{\mathbb{F}_p}(\mathcal{O}_F/p\mathcal{O}_F) = de. \quad \square$$

Recall that we defined $\text{disc} = [\mathcal{O}_L^\perp : \mathcal{O}_L]$. There is a formula relating $\text{disc}_u := [\mathcal{O}_F^\perp : \mathcal{O}_F]$ to e .