18.785: Algebraic Number Theory

(lecture notes)

Taught by Bjorn Poonen

Fall 2014, MIT

Last updated: January 17, 2015

Disclaimer

These are my notes from Prof. Poonen's course on algebraic number theory, given at MIT in fall 2014. I have made them public in the hope that they might be useful to others, but these are not official notes in any way. In particular, mistakes are my fault; if you find any, please report them to:

Eva Belmont
ekbelmont at gmail.com

Contents

Lecture 1: September 4

Office hours: Mon 3:30 - 4:30, Friday 9:30-10:30 and 3:30 - 4:30

Let K be an arbitrary degree-n extension of $\mathbb{Q}$. Question: is the ring of integers $\mathcal{O}_K$ a UFD? No, not always. But it's "almost" a UFD.

A number field is a finite extension of $\mathbb{Q}$.

You can, analogously, look at function fields – finite extensions of $\mathbb{C}(t)$. These extensions K correspond to curves over $\mathbb{C}$. The ring of integers is the coordinate ring of a regular affine curve.

You can also ask about $\mathbb{F}_q[t] \subset \mathbb{F}_p(t)$ and finite extensions of this. This is actually closer to the $\mathbb{Z} \subset \mathbb{Q}$ situation.

Primes in $\mathbb{Z}$ correspond to monic irreducible polynomials in $\mathbb{F}_q[t]$ and monic irreducible polynomials in $\mathbb{C}[t]$ – but those are just $t - a$. Reduction mod p in $\mathbb{Z}$ corresponds to the map $\mathbb{C}[t] \to \mathbb{C}[t]/(t-a)$, but that is just $\cong \mathbb{C}$ via the evaluation at a map.

One way to understand polynomials is to understand them locally – understand their power series around a point. That is often easier, and you can hope to piece together the local information to get global information. If you complete with respect to the prime $t - a$, you get the power series ring $\mathbb{C}[[t-a]]$. Similarly for $\mathbb{Z}$, it helps to understand things "one prime at a time".

We also care about analytic objects, like $\zeta(s) = \sum n^{-s}$. This extends to a meromorphic function on the entire complex plane. The BSD conjecture tells you about leading terms of zeta functions. The analytic class number formula relates zeta functions to failure of $\mathcal{O}_K$ to be a UFD.

Other topics: statements of class field theory in the modern adelic form; proofs of this; Galois cohomology; algorithmic number theory...

Open question: given a finite group G, can you find a finite extension of $\mathbb{Q}$ with G as the Galois group?

OK, let's start for real.

Books: Serre *Local fields*, ...

1.1. Absolute values.

Definition 1.1. An absolute value on a field k is a function

$$|\ |\ : k \to \mathbb{R}_{\geq 0}$$

such that for all $x, y \in k$:

- $|x| = 0 \iff x = 0$
- (multiplicativity) $|xy| = |x||y|$
- (triangle inequality) $|x + y| \leq |x| + |y|$.

If $|\ |$ satisfies

$$|x + y| \leq \max(|x|, |y|)$$

for all x, y, then we say that $|\ \ |$ is *nonarchimedean*.

It turns out that almost all absolute values that you care about are nonarchimedean; the one you're used to is the weird one.

Example 1.2 (Trivial absolute value)**.**

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

This is nonarchimedean.

Absolute values give a distance function, so you can make the field into a metric space; that is, k has a topology!

Definition 1.3. Two absolute values $|\ |$ and $|\ |'$ on k are *equivalent* if there is some $\alpha \in \mathbb{R}_{>0}$ for which $|x|' = |x|^\alpha$ for all x.

Example 1.4 (Absolute values on $\mathbb{Q}$)**.** Fix a prime p. Define the *p-adic valuation*

$$v_p : \mathbb{Q}^\times \to \mathbb{Z} \text{ where } \prod_{\substack{\text{primes} \\ q}} q^{e_n} \mapsto e_p$$

Also define $v_p(0) = +\infty$. Now define the *p-adic absolute value*

$$|x|_p = p^{-v_p(x)}$$

(interpret this to mean that $|0|_p = 0$). It is easy to check that this is an nonarchimedean absolute value.

There is also the usual absolute value on $\mathbb{Q}$, which we denote by $|\ |_\infty$. Infinity isn't a prime, but it "sort of is". Geometrically, you have one absolute value for every point on the affine line, including one for the "point at infinity".

Theorem 1.5 (Ostrowski)**.** *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\ |_p$ for some prime $p \leq \infty$.*

Proof. Homework. □

Definition 1.6. A *discrete valuation* on a field K is a projective homomorphism $v : K^\times \twoheadrightarrow \mathbb{Z}$, extended by defining $v(0) = +\infty$, with the added condition

$$v(x + y) \geq \min\{v(x), v(y)\}$$

for all x, y. (You get this by taking the log of the nonarchimedean triangle equality.)

Then
$$A := \{x \in K \,:\, v(x) \geq 0\}$$
is a subring. Any ring arising in this way is called a *discrete valuation ring* (DVR). We call this the valuation ring of K. Inside of A is the *unit group*
$$A^\times = \{x \,:\, v(x) = 0\}.$$
Fix $\pi \in A$ such that $v(\pi) = 1$; this is called a *uniformizer* or *uniformizing parameter*.

Think of K as a disjoint union of elements of the same valuation. π has valuation 1, π^2 has valuation 2, etc. Note that π is unique up to units (of A), and every element x looks like $u\pi^n$ for a unique $u \in A^\times$, and $n = v(x)$. This shows that this is a unique factorization domain.

Each nonzero ideal of A looks like
$$(\pi^n) = \{x \in A \,:\, v(x) \geq n\}$$
for some n. So you have this descending chain of ideals $(\pi) \supset (\pi^2) \supset \dots$.

There is a unique maximal ideal
$$\mathfrak{m} = \{x \in A \,:\, v(x) > 0\} = (\pi).$$
It is the only prime ideal except for the zero ideal.

The *residue field* is $k = A/\mathfrak{m}$.

Example 1.7. If $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is the p-adic valuation, then $A = \{\frac{a}{s} \,:\, a, s \in \mathbb{Z} \text{ and } p \nmid s\}$. This is just the localization $\mathbb{Z}_{(p)}$. This has unique maximal ideal (p), and the residue field is $\mathbb{Z}/p$.

Example 1.8. Let k be a field, and let $k((t))$ be the field of Laurent series. Then we have a valuation $v : k((t)) \to \mathbb{Z} \cup \{\infty\}$ defined by $\sum_{n \geq n_0} a_n t^n \mapsto n_0$ (if we've written the Laurent series such that $a_n \neq 0$). Then $A = k[[t]]$. The residue field is k, and the map $A \to k$ is the evaluate-at-0 map.

Example 1.9. For a connected open subset $U \subset \mathbb{C}$, define
$$\mathscr{M}(U) = \{\text{meromorphic functions on } U\}.$$
Define $\mathscr{M}$, the field of germs (this has nothing to do with biology!) of meromorphic functions
$$\mathscr{M} = \bigcup_{U \ni 0} \mathscr{M}(U).$$
So this is meromorphic functions that exist on some unspecified subset of U containing zero. This is a direct limit over the direct system of neighborhoods of 0. Because of the magic of complex analysis, you don't need to worry about the "$f \sim g$ if they are eventually equal" bit of the direct limit – if two functions agree on a little open set, they agree everywhere they're defined.

(This is also the stalk of the sheaf of meromorphic functions.)

Let v be the composition $\mathscr{M} \hookrightarrow \mathbb{C}((z)) \to \mathbb{Z} \cup \{\infty\}$ where the first map takes $f \mapsto$ its Laurent series, and the second map is the valuation we discussed previously. The effect of this is to compute the order of vanishing of f at 0.

The ring of integers A is the ring of germs of holomorphic functions at 0. A uniformizer is z. The residue field is $\mathbb{C}$, and the map $A \to k$ is evaluation at 0.

1.2. Properties of DVR's. (Until further notice, all rings are commutative.)

DVRs are Noetherian: every increasing sequence of ideals eventually stabilizes. Equivalently, every ideal is finitely generated. (This is obvious for the rings we talked about above – in fact, every ideal was generated by a single element.)

DVRs are local: there is a unique maximal ideal.

DVRs are 1-dimensional. (Dimension of a ring: length of the longest chain of primes $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$.) All nonzero ideals in a DVR have the form (π^n), so the only primes are 0 and (π), and the longest chain is $0 \subsetneq (\pi)$.

DVRs are PID's so they are unique factorization domains.

DVRs are integrally closed.

Theorem 1.10. *For a ring A, TFAE:*

(1) A is a DVR
(2) A is a PID with exactly one nonzero prime
(3) A is a 1-dimensional Noetherian local domain and A is integrally closed.
(4) A is a 1-dimensional regular local ring.

(A Noetherian local ring is regular if the unique maximal ideal $\mathfrak{m}$ satisfies $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim R$. Geometrically, $\dim \mathfrak{m}/\mathfrak{m}^2$ measures the dimension of the tangent space; a singular point in a variety has a tangent space that is "too big".)

Nonexample 1.11. Let $A = \mathbb{C}[[x, y]]/(y^2 - x^3)$. (In algebraic geometry, this is a cubic with a node.) This is a Noetherian local ring (quotients of Noetherian rings are Noetherian), where the unique maximal ideal is $\mathfrak{m} = (x, y)$. But this is not principal. $\dim A = 1$ but $\mathfrak{m}/\mathfrak{m}^2$ is 2-dimensional (with basis x, y), so A is not a regular local ring.

Integral extensions are kind of like algebraic extensions, but for arbitrary rings.

Definition 1.12. Given rings $A \subset B$ and $b \in B$, say that b is *integral over* A if b is the root of a monic polynomial $f(x) \in A[x]$.

B is *integral* over A if every b is integral over A.

For example, $\sqrt{2}$ is integral over $\mathbb{Z}$ but $\frac{1}{2}$ is not.

Proposition 1.13. *If α and β are integral over A, then $\alpha+\beta$ is integral over A.*

I think we're assuming A and B are domains.

PROOF. Suppose α is a root of f and β is a root of g:

$$f(x) = x^m + a_{m-1}x^{m-1} + \dots$$
$$g(x) = y^n + b_{n-1}y^{n-1} + \dots$$

It suffices to do the "generic case" for each n, m: the coefficients of the polynomials are indeterminants. That is, we are working over the polynomial ring $A' = \mathbb{Z}[a_0, a_1, \dots, b_0, b_1, \dots]$. To get the result for A' and B', just apply the homomorphism

$$\begin{array}{ccc} B & \xrightarrow{x\mapsto\alpha, y\mapsto\beta} & B' \\ \uparrow & & \uparrow \\ A & \longrightarrow & A' \end{array}$$

We're trying to show that $x+y \in B$ is integral over A. Let $K = \overline{\operatorname{Frac} B}$ (algebraic closure). Let $\alpha_1, \dots, \alpha_m$ be the roots of f in K, and $\beta_1, \dots, \beta_n$ be the roots of g in K. Then

$$\prod_{i,j}(x - (\alpha_i + \beta_j))$$

has coefficients expressible as polynomials in the elementary symmetric functions of the α_i (these are just the coefficients of f, because you can write that as a product of its roots), and same for the β_j (ditto, coefficients of g). It has $x+y$ as a root, because one of the α's is x, and one of the β's is y. □

Definition 1.14. A is integrally closed if everything that is integral in the fraction field is already in A. (Alternatively, if A = integral closure.)

LECTURE 2: SEPTEMBER 9

Office hours on Monday, September 15 adjusted to be 9:30 - 10:30 (not 3:30 - 4:30).

2.1. More about integrality. Last time, we said that b is integral over A iff there is a monic polynomial $f \in A[x]$ such that $f(b) = 0$.

Proposition 2.1. *If α and β are integral over A, then $\alpha+\beta$ is integral over A.*

PROOF CON'T. Remember from last time we'd reduced to the generic case where $A = \mathbb{Z}[a_0, \dots, b_0, \dots]$ where α satisfies $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_0$ and β satisfies $g(x) = x^n + \dots + b_0$. Then we can replace B with $A[x,y]/(f(x), g(y))$. We need $x+y \in B$ to be integral over A. We gave a proof last time using elementary symmetric functions.

Alternative proof: B is free as an A-module with basis $\{x^i y^j : 0 \le i < m, 0 \le j < n\}$. Look at the multiplication map $B \stackrel{x+y}{\to} B$; this is an A-linear transformation, and you can take its characteristic polynomial $h(T)$, which has coefficients in A. It is monic, because all characteristic polynomials are. The Cayley-Hamilton theorem says that $h(x+y) = 0$, in the sense that it acts as the zero map on B. But this shows that $h(x+y)$ is *actually* zero, because it acts as zero on 1. □

You can do something similar for $\alpha\beta$.

Proposition 2.2. *Suppose $A \subset B$. Then b is integral over A iff $A[b]$ is a finitely generated A-module.*

(See Atiyah-Macdonald.)

Corollary 2.3. *Suppose $A \subset B$. Then $\widetilde{A} = \{b : b \text{ is integral over } A\}$ is a subring of B, called the* integral closure of A in B.

Definition 2.4. Say that A is *integrally closed* if A is integrally closed in its fraction field.

Proposition 2.5. *$\mathbb{Z}$ is integrally closed [i.e., in $\mathbb{Q}$].*

So if $\frac{a}{b}$ satisfies a monic polynomial in $\mathbb{Q}$ then it was an integer to begin with.

Proof. Basically, rational root test.

Suppose $\frac{r}{s} \in \mathbb{Q}$ is expressed in lowest terms, and is integral over $\mathbb{Z}$; that is, it satisfies

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0.$$

Multiply out by s^n, to get $r^n = sx$ for some $x \in \mathbb{Z}$. We assumed $\gcd(r,s) = 1$, so s is just a unit. So $\frac{r}{s}$ was actually an integer. □

The same proof shows that any UFD is integrally closed (you need it to be a UFD in order to talk about gcd's).

This is also a nice way to prove that something is *not* a UFD.

Example 2.6. $\mathbb{Z}[\sqrt{5}]$ is not a UFD, because $\varphi = \frac{1+\sqrt{5}}{2} \in \operatorname{Frac}\mathbb{Z}[\sqrt{5}]$ satisfies $\varphi^2 - \varphi - 1 = 0$ but $\varphi \notin \mathbb{Z}[\sqrt{5}]$.

This is why we will start taking integral closures of things: "if you want it to have a chance at being a UFD, you need it to be integrally closed".

Definition 2.7. A *number field* k is a finite extension of $\mathbb{Q}$.

The ring of integers $\mathcal{O}_k$ of a number field k is the integral closure of $\mathbb{Z}$ in k.

Proposition 2.8. *Let L/K be an extension of fields, and assume $A \subset K$ is integrally closed and* $\operatorname{Frac} A = K$. *Let $\alpha \in L$ and let $f \in K[x]$ be the minimal polynomial of α over K. (Remember minimal polynomials are monic by definition.)*

α is integral over $K \iff f(x) \in A[x]$.

Proof. ($\Longleftarrow$) Obvious.

($\Longrightarrow$) Factor $f = \prod_{i=1}^{n}(x - \alpha_i)$ over the algebraic closure $\overline{K}$. There are K-homomorphisms $L \to \overline{K}$ sending $\alpha \mapsto \alpha_i$. By assumption, α is integral over A, and so α_i is integral over A (it satisfies the same minimal polynomial). So each coefficient of $f(x)$ is a sum of products of the α_i, hence integral over A.

A is integrally closed, so each coefficient is in A. □

2.2. Localization. Localization is like a partial fraction field: you invert some elements and not others.

Definition 2.9. Let $S \subset A$ be closed under finite products (including the empty product, a.k.a. 1). Also assume for simplicity that S contains no zerodivisors of A (i.e. $A \xrightarrow{s} A$ is injective for all $s \in S$).

Then $S^{-1} = A[S^{-1}] := \{\frac{a}{s} : a \in A, s \in S\}/\sim$ where we say $\frac{a}{s} \sim \frac{a'}{s'}$ if $s'a = sa'$ in A. This forms a ring.

There is a map

$$\{\text{primes of } S^{-1}A\} \longrightarrow \{\text{primes of } A \text{ that do not meet } S\}$$

sending $\mathfrak{q} \mapsto \mathfrak{q} \cap A$. This map is a bijection; the backwards map sends $\mathfrak{p} \mapsto \mathfrak{p} \cdot S^{-1}A$.

Important special case 2.10. Let A be a domain and fix a prime ideal $\mathfrak{p} \subset A$. Let $S = A - \mathfrak{p}$; the fact that $\mathfrak{p}$ is prime guarantees that S is multiplicative.

Localizing at S has another name: $A_\mathfrak{p} := S^{-1}A$. By the bijection above, primes of $A_\mathfrak{p}$ correspond to primes contained in $\mathfrak{p}$. So $A_\mathfrak{p}$ has a unique maximal ideal $\mathfrak{p} \cdot A_\mathfrak{p}$.

Even more special case: if $\mathfrak{p} = (0)$ then you get the fraction field.

But in general, you can say that $A \subset A_\mathfrak{p} \subset \operatorname{Frac} A$, and $\operatorname{Frac} A_\mathfrak{p} = \operatorname{Frac} A$.

Example 2.11. Let $A = k[x]$ and let $\mathfrak{p} = (x - 2)$ (this is the maximal ideal of polynomials that vanish at 2). Then $A_\mathfrak{p} = \{f \in k(p) : f(2) \text{ is defined.}\}$ The maximal ideal consists of the rational functions such that $f(2) = 0$.

$A_{\mathfrak{p}}$ is a PID (because $k[x]$ is a PID). Prime ideals of $k[x]$ are (0), and (f) for monic irreducible polynomials f. (0) is contained in all of them, and there is no more containment.

The primes of $A_{\mathfrak{p}}$ are just $(0) \subset (x-2)$. $A_{\mathfrak{p}}$ is a PID with one nonzero prime, hence a DVR.

Example 2.12. $\mathbb{Z}_{(p)} = \{\frac{a}{b} : p \nmid b\}$

Then $\mathbb{Z}_{(p)}$ is also a DVR with unique nonzero prime (p).

Generalization 2.13. Suppose A, S, and $\mathfrak{p}$ are as before. Let M be an A-module. Assume that no element of S acts as zero on M (i.e. $M \xrightarrow{s} M$ is injective for all $s \in S$).

Then $S^{-1}M = \{\frac{m}{s} : m \in M, s \in S\}/\sim$ where $\sim$ is analogous to before. This is an $S^{-1}A$-module.

If $S = A - \mathfrak{p}$, then you can define $M_{\mathfrak{p}}$.

Localization is "focusing on one prime at a time"; but there are a lot of theorems that relate information about all localizations to information about the whole ring.

Proposition 2.14. *Suppose A is a subring of a field K, and M is an A-module contained in a K-vector space V (this says that $M \to M \otimes_A K$ is injective, or alternatively: if $am = 0$ then $a = 0$ or $m = 0$).*

Then

$$M = \bigcap_{\mathfrak{m} \subset A} M_{\mathfrak{m}}.$$

Proof. It is clear that $M \subset \bigcap_{\mathfrak{m}\subset A} M_{\mathfrak{m}}$, where you identify $x \in M$ with $\frac{x}{1} \in M_{\mathfrak{m}}$.

Suppose $x \in \bigcap_{\mathfrak{m}\subset A} M_{\mathfrak{m}}$. Look at $I = \{a \in A : ax \in M\}$ (this is the set of all possible denominators for x). This is an ideal of A that is not contained in any $\mathfrak{m}$ (for every $\mathfrak{m}$, there's always a denominator not in $\mathfrak{m}$). So $I = (1)$, and in particular, $\frac{x}{1} \in A$. □

Example 2.15. Take $A = \mathbb{Z}$ and $M = \mathbb{Z}$. The maximal ideals of A are just (p). Then $\bigcap_p \mathbb{Z}_{(p)}$ is the set of fractions $\{\frac{a}{b}\}$ where b is contained in *no* (p). This is just $\mathbb{Z}$, as the proposition says.

2.3. Dedekind domains.

Proposition 2.16. *Suppose A is a Noetherian domain. TFAE:*

(1) For every nonzero prime $\mathfrak{p}$ of A, $A_{\mathfrak{p}}$ is a DVR.
(2) $\dim A \leq 1$ and A is integrally closed [in its fraction field].

Such an A is called a *Dedekind domain*. Note that fields satisfy these conditions.

PROOF. If A is a field, (1) and (2) hold.

Now assume A is not a field. Let $K = \operatorname{Frac} A$.

(1) $\implies$ (2) $\dim A = \sup\{\dim A_{\mathfrak{p}}\}$ (the longest chain ends in some $\mathfrak{p}$, and the length of this chain $= \dim A_{\mathfrak{p}}$). In a DVR, $\dim A_{\mathfrak{p}} = 1$ for all $\mathfrak{p}$, so $\dim A = 1$. Now check that A is integrally closed. Suppose that $a \in K$ is integral over A; I need to prove that $a \in A$.

Given $\mathfrak{p} \neq (0)$, a is integral over $A_{\mathfrak{p}}$, which is a DVR, and DVR's are integrally closed (this was on the homework). So $a \in A_{\mathfrak{p}}$ for every $\mathfrak{p}$. Recall that all maximal chains of primes have length 1, so all nonzero primes are maximal. Then by Proposition 2.14, $A = \bigcap A_{\mathfrak{p}}$. So $a \in A$.

(2) $\implies$ (1) The properties {Noetherian, domain, dimension 1, integrally closed} are inherited by any localization, and in particular by $A_{\mathfrak{p}}$. For $p \neq (0)$, $\dim A_{\mathfrak{p}} \geq 1$ so $\dim A_{\mathfrak{p}} = 1$.

One of the equivalent formulations of the definition of a DVR is a 1-dimension Noetherian local domain that is integrally closed. □

Corollary 2.17. *Every PID is a Dedekind domain.*

PROOF. Check (1) above. □

Corollary 2.18. $\mathbb{Z}$ *is a Dedekind domain.*

It is not true that every UFD is a Dedekind domain. For example, $k[x, y]$ is a UFD, but $\dim k[x, y] = 2$, so it is not a Dedekind domain.

It turns out that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain but not a UFD.

Later, we will show that every ring of integers in a number field is a Dedekind domain. (This is why they're important.)

LECTURE 3: SEPTEMBER 11

Important example: the coordinate ring of a smooth affine curve is a Dedekind domain.

Let A be a Noetherian domain, and let $K = \operatorname{Frac} A$.

Definition 3.1. A *fractional ideal* in A is a finitely generated A-submodule of K (f.g. as a module, not as an algebra).

Example 3.2. $\frac{1}{6}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$.

Example 3.3. If $x \in K$ then $(x) = x \cdot A$ is a fractional ideal. This is called a *principal fractional ideal.*

If I and J are fractional ideals, then $I + J$ and IJ are fractional ideals. Also define the *colon ideal*

$$(I : J) := \{x \in K \,:\, xJ \subset I\}.$$

Why is this finitely generated? If you just impose the condition for one $j \in J$ then you get $j^{-1}I \supset (I : J)$ and that is finitely generated (isomorphic to I *as a module*). Because the ring is Noetherian, submodules of finitely generated modules are finitely generated.

You should think of this as division.

Example 3.4. If $A = \mathbb{Z}$, then $((12) : (3)) = (4)$.

Definition 3.5. A fractional ideal I is *invertible* if there exists a fractional ideal J such that $IJ = (1) = A$.

If J exists, then it is unique (this is the same proof as showing in group theory that inverses are unique). More precisely, $J \subset (A : I)$, so the biggest that J could be is $(A : I)$. If there is an inverse, then $(A : I)$ works – anything that's bigger than the biggest thing that works and still maps I into A will also work.

Definition 3.6. The *ideal group* of A is the set of all invertible fractional ideals.

This is an abelian group under multiplication.

Note that nonzero principal fractional ideals are all invertible (and you can guess what the inverse is...). These form a subgroup of the ideal group.

Example 3.7. Suppose A is a DVR with uniformizer π. Then every nonzero fractional ideal has the form (π^n) for $n \in \mathbb{Z}$. (If you have a collection of generators, take the generator with the smallest valuation n, and that generates the rest of them. Generators of given valuation are unique up to unit, so this is (π^n).)

So the ideal group $\cong \mathbb{Z}$ and every nonzero fractional ideal is invertible.

$$(\pi^n)(\pi^m) = (\pi^{n+m}) \qquad (\pi^m) + (\pi^n) = (\pi^{\min\{m,n\}}) \qquad ((\pi^m) : (\pi^n)) = (\pi^{m-n})$$

The point is that "DVR's are easy".

The operations $I + J$, IJ, and $(I : J)$ respect localization. For example, $(I : J)_{\mathfrak{m}} = (I_{\mathfrak{m}} : J_{\mathfrak{m}})$

Proposition 3.8. *"Invertibility can be checked locally", i.e. in the context of a Noetherian domain A and a fractional ideal I, then*

$$I \text{ is invertible} \iff I_{\mathfrak{m}} \text{ is invertible } \forall \mathfrak{m}.$$

(You're checking that $I_{\mathfrak{m}}$ is invertible as an ideal of $A_{\mathfrak{m}}$*.)*

PROOF. I is invertible $\iff I \cdot (A : I) = A$. Recall that if you have a module $\subset$ a vector space, it is the intersection of its localizations at maximal ideals. So it is determined by its localizations; i.e. if you have an equality to check, it suffices to do so at every localization.

$$\begin{aligned} I \cdot (A : I) = A &\iff (I \cdot A : I)_{\mathfrak{m}} = A_{\mathfrak{m}} \\ &\iff I_{\mathfrak{m}} \cdot (A_{\mathfrak{m}} : I_{\mathfrak{m}}) = A_{\mathfrak{m}} \\ &\iff I_{\mathfrak{m}} \text{ is invertible.} \end{aligned}$$

□

From now on let A be a Dedekind domain.

Corollary 3.9. *Every nonzero fractional ideal in a Dedekind domain is invertible.*

PROOF. By the previous proposition, it suffices to check locally. But we already know that, over a DVR, every fractional ideal is invertible. □

This means you can make sense of things like $\mathfrak{p}^{-5}$.

Proposition 3.10. *Each nonzero $x \in A$ (in a Dedekind domain) belongs to only finitely many prime ideals.*

(This is also true without the word "prime", but this proof doesn't prove it.)

PROOF. There are order-reversing bijections

$$\begin{aligned} \{\text{ideals between } (x) \text{ and } A\} &\longleftrightarrow \{\text{fractional ideals between } (x^{-1}) \text{ and } A\} \\ &\longleftrightarrow \{\text{ideals between } A \text{ and } (x)\} \end{aligned}$$

where the first map sends $I \mapsto I^{-1}$ and the second sends $J \mapsto xJ$. An ascending chain of ideals between (x) and A gives rise to a descending chain of ideals between (x) and A. The Noetherian condition says that ascending chains stabilize; thus descending chains between (x) and A stabilize. (We have not actually proved that A is Artinian.)

Suppose $x \in \mathfrak{p}_1, \mathfrak{p}_2, \ldots$. Then $\mathfrak{p}_1 \supset \mathfrak{p}_1 \cap \mathfrak{p}_2 \supset \cdots \ni x$. By what we said above, this has to stabilize. So there exists k such that for all $i \geq k$, $\mathfrak{p}_i \supset \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_k$; but the latter contains the product $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_k$. Since $\mathfrak{p}_i$ is prime, it contains one of the $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$.

Since A is a Dedekind domain, every localization has dimension ≤ 1, hence $\dim A \leq 1$ there are no nontrivial inclusion relations. So $\mathfrak{p}_i =$ every $\mathfrak{p}_k$ for $k \geq i$. □

But it is possible to have uncountably many primes in a Dedekind domain: look at all the ideals $(t - a)$ in $\mathbb{C}[t]$. The point is that any particular element, say $t^2 - 4$, is only contained in finitely many primes (in this case $t - 2$ and $t + 2$).

Corollary 3.11. *Let $v_{\mathfrak{p}}$ be the valuation associated to $A_{\mathfrak{p}} \subset K$.*

If $x \in K$, then $v_\mathfrak{p}(x) = 0$ for all but finitely many $\mathfrak{p}$.

PROOF. This is true if $x \in A\backslash\{0\}$. The valuation is already ≥ 0, and it's > 0 iff $x \in \mathfrak{p}$. If this property is true for x and y, then it is also true for $\frac{x}{y}$ (finitely many that are bad for x, and finitely many that are bad for y). □

If I is a nonzero fractional ideal of A, then $I_\mathfrak{p}$ is a nonzero fractional ideal of $A_\mathfrak{p}$. This is good because we already know what the fractional ideals of a DVR are: $I_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n$ (this is just another way of writing the ideal (π^n)). This number n is uniquely determined by $I_\mathfrak{p}$, which is determined by I. Call this the *valuation of I*.

I is a finitely generated A-module $I = (x_1, \dots, x_n)$ where x_i are nonzero elements of K. Then $v_\mathfrak{p}(I) = \min_i\{v_\mathfrak{p}(x_i)\}$.

Corollary 3.12. *Given I, $v_\mathfrak{p}(I) = 0$ for all but finitely many $\mathfrak{p}$.*

Lemma 3.13. *If $\mathfrak{p}, \mathfrak{q}$ are distinct nonzero primes in a Dedekind domain, $\mathfrak{p} \cdot A_\mathfrak{q} = A_\mathfrak{q}$.*

PROOF. It suffices to say that there exists some $s \in \mathfrak{p}\backslash\mathfrak{q}$. This is the same old fact that there are no nontrivial inclusions of primes. □

Theorem 3.14. *Let A be a Dedekind domain. There is an isomorphism of groups*

$$\bigoplus_{\substack{\text{nonzero} \\ \text{primes } \mathfrak{p}}} \mathbb{Z} \longrightarrow \{\text{nonzero fractional ideals of } A\}.$$

In particular: a tuple $(e_\mathfrak{p})$ gets sent to $\prod \mathfrak{p}^{e_\mathfrak{p}}$ (this is a finite product where you ignore the terms with $e_\mathfrak{p} = 0$). In the other direction, send I to the tuple $(v_\mathfrak{p}(I))$. We already proved that this makes sense as an element of $\bigoplus_\mathfrak{p} \mathbb{Z}$.

Remember that elements of $\bigoplus$ are tuples with finitely many elements nonzero.

PROOF. We show that $\to$ is injective. I is determined by its localizations $(\dots, I_\mathfrak{p}, \dots)$ (it's the intersection of these). But these are fractional ideals in a DVR, so knowing $I_\mathfrak{p} \subset A_\mathfrak{p}$ is the same as knowing $v_\mathfrak{p}(I)$.

Now show that $\to$ is surjective: given $(\dots, e_\mathfrak{p}, \dots)$, there is an obvious ideal that might give rise to this, namely $I = \prod \mathfrak{p}^{e_\mathfrak{p}}$. Then $I_\mathfrak{q} = \prod_\mathfrak{p} (\mathfrak{p}A_\mathfrak{q})^{e_\mathfrak{p}}$. But by Lemma 3.13, none of these terms matter except for $(\mathfrak{q}A_\mathfrak{q})^{e_\mathfrak{q}}$. So localizing I at $\mathfrak{q}$ picks out the part of the factorization at $\mathfrak{q}$. So $v_\mathfrak{q}(I) = e_\mathfrak{q}$. □

So every ideal of a Dedekind domain has unique factorization.

If $I = \prod \mathfrak{p}^{e_\mathfrak{p}}$ and $J = \prod \mathfrak{p}^{f_\mathfrak{p}}$ then $I + J = \prod \mathfrak{p}^{\min\{e_\mathfrak{p}, f_\mathfrak{p}\}}$, and the other operations $(I : J)$ and IJ are similarly easy to write. Also $J \subset I \iff f_\mathfrak{p} \geq e_\mathfrak{p}$ for all $\mathfrak{p}$.

Special case: for $x \in K^\times$, $(x) \subset I \iff v_\mathfrak{p}(x) \geq e_\mathfrak{p}$ for all $\mathfrak{p}$. Of course, $(x) \subset I \iff x \in I$. Thus

$$I = \{x \in K : v_\mathfrak{p}(x) \geq e_\mathfrak{p}\}.$$

So if all the $e_\mathfrak{p}$ were zero, then you get all of A. (Alternatively, notice that $A = \bigcap A_\mathfrak{p}$.)

Special case: If $J \subset A$ then say that J is an *integral ideal* (this means it is just an ideal of A). This is the same as saying that all the $f_\mathfrak{p}$ are ≥ 0.

If A is the coordinate ring of a regular affine curve X over a field, then A is a Dedekind domain. Let $K = \operatorname{Frac} A$; this is called the function field of the curve – ratios of polynomials on X. Maximal prime ideals arise as functions that vanish at a particular point (maximal ideals are kernels of surjective homomorphisms to a field, e.g. "evaluate at a", and the Hilbert Nullstellensatz says that this describes everything). Prime ideals of A correspond to *closed points* p on X (i.e. in the topology of a scheme), and these correspond to irreducible closed subschemes of codimension 1, i.e. *prime divisors* on X.

Fractional ideals are just finite products of these. You can define a *divisor* to be a formal sum $D = \sum_{\substack{\text{closed} \\ \text{points } P \in X}} e_P P$. Fractional ideals $\prod \mathfrak{p}^{e_\mathfrak{p}}$ correspond to divisors where $e_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p}$.

Integral ideals correspond, by definition, to effective divisors. (Nonzero) principal fractional ideals correspond to principal divisors (f), i.e. a divisor that measures the order of vanishing of the rational function f at every point.

Example 3.15. If $X = \mathbb{A}^1_\mathbb{C}$ then the coordinate ring is $\mathbb{C}[t]$. If $f = \frac{t^2-4}{(t+3)^7}$ then $(f) = 1 \cdot [2] + 1 \cdot [-2] - 7 \cdot [-3]$ where $[2]$ is the point 2 on the affine line.

Helpful for the homework:

Theorem 3.16 ("Pretty strong approximation theorem")**.** *Let A be a Dedekind domain, $K = \operatorname{Frac} A$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ distinct nonzero primes. Let $a_1, \ldots, a_n \in K$ and $e_1, \ldots, e_n \in \mathbb{Z}$.*

Then there exists $x \in K$ such that $v_{\mathfrak{p}_i}(x - a_i) \geq e_i$ ("x is close to a_i") and at all other (nonzero) primes $\mathfrak{q}$, we have $v_\mathfrak{q}(x) \geq 0$.

Lecture 4: September 16

Definition 4.1. A *number field* is a finite extension of $\mathbb{Q}$.

A *global function field* is a finite extension of $\mathbb{F}_q(t)$ (the function field of a curve over $\mathbb{F}_q$).

These are both global fields.

Theorem 4.2 (Weak approximation theorem)**.** *Let K be a field, let $|\ |_1, \dots, |\ |_n$ be pairwise inequivalent (equivalent would mean $|\ |_i = |\ |_j^\alpha$), let $a_1, \dots, a_n \in K$ and $\varepsilon_1, \dots, \varepsilon_n \in \mathbb{R}_{>0}$.*

Then there exists $x \in K$ such that $|x - a_i|_i < \varepsilon_i$.

PROOF. Homework. □

Theorem 4.3 (Strong approximation theorem)**.** *Let K be a global field. Let $|\ |_0, \dots, |\ |_n$ be pairwise inequivalent nontrivial absolute values on K. Let $a_1, \dots, a_n \in K$ and $\varepsilon_1, \dots, \varepsilon_n \in \mathbb{R}_{>0}$.*

Then there exists $x \in K$ such that $|x - a_i|_i < \varepsilon_i$ for $i \geq 1$, and $|x| \leq 1$ for all absolute values not equivalent to one of $|\ |_0, \dots, |\ |_n$.

I claim that this is really just fancy Chinese Remainder theorem, but requires more advanced techniques to prove.

Example 4.4. Let $K = \mathbb{Q}$ and let $|\ |_0$ be the usual absolute value. There exists $x \in \mathbb{Q}$ such that $|x - 5|_2 \leq \frac{1}{8}$, $|x - 7|_3 \leq \frac{1}{9}$, and $|x|_p \leq 1$ for all (non-infinite) primes. The last condition shows that $x \in \bigcap_p \mathbb{Z}_{(p)} = \mathbb{Z}$. But the first conditions say that $x \equiv 5 \pmod 8$ and $x \equiv 7 \pmod 9$.

This is why I said this is just the Chinese Remainder Theorem.

Note: if we also required $|x|_0 < \frac{1}{2}$ then we'd be in trouble.

The theorem last time we called the "pretty strong approximation theorem" is a special case of this for nonarchimedean absolute values only (so $|\ |_0$ in the strong approximation theorem corresponds to some archimedean absolute value in the theorem below).

Theorem 4.5 (Pretty strong approximation theorem)**.** *Let A be a Dedekind domain, let $K = \operatorname{Frac} A$, let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be nonzero primes of A, $a_1, ., a_n \in K$, and $e_1, \dots, e_n \in \mathbb{Z}$.*

Then there is some $x \in K$ such that $v_{\mathfrak{p}_i}(x - a_i) \geq e_i$ and $v_{\mathfrak{q}}(x) \geq 0$ for every other nonzero prime.

PROOF. I can assume that $n \geq 2$.

Case 1: $a_1 \in A$ and all other $a_i = 0$. Increase the e_i to assume $e_i > 0$ for all i. Consider $\mathfrak{p}_1^{e_1} + \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_n^{e_n}$; I claim this is A (these ideals are relatively prime). So I can write $a_1 = y + x$ where $y \in \mathfrak{p}_1^{e_1}$ and $x \in \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_n^{e_n}$. Then $x \equiv a_1 \pmod{\mathfrak{p}_1^{e_1}}$ and $x \in \mathfrak{p}_i^{e_i}$ for all other i (since $x \in \mathfrak{p}_i^{e_i}$). Also, $x \in A$ so $v_{\mathfrak{q}}(x) \geq 0$ for all other $\mathfrak{q}$.

Case 2: $a_1, a_2, \dots, a_n \in A$. Approximate $(a_1, 0, \dots, 0)$ by x_1, approximate $(0, a_2, 0, \dots)$ by x_2, etc. Let $x = x_1 + \dots + x_n$ and use the previous case.

Case 3: $a_1, \dots, a_n \in K$ *(general case).* Write $a_i = \frac{b_i}{s}$ with $b_i \in$ and $s \in A$ (this is the common denominator). Take $x = \frac{y}{s}$; we need $v_{\mathfrak{p}_i}(x - a_i) \geq e_i$ and $v_{\mathfrak{q}}(x) \geq 0$. This is $v_{\mathfrak{p}_i}\left(\frac{y-b_i}{s}\right) = v_{\mathfrak{p}_i}(y - b_i) - v_{\mathfrak{p}_i}(s)$. Use Case 2 to find y such that $v_{\mathfrak{p}_i}(y - b_i) \geq e_i + v_{\mathfrak{p}_i}(s)$ for $i = 1, \dots, n$, and $v_{\mathfrak{q}}(y) \geq v_{\mathfrak{q}}(s)$ for all other $\mathfrak{q}$.

(Issue: Case 2 only allowed you to say that $v_{\mathfrak{q}}(y) \geq 0$ for all other $\mathfrak{q}$. But y has nonzero valuation at finitely many $\mathfrak{q}$, so just move those to the set of $\mathfrak{p}_i$'s where you can specify valuation more precisely.) □

A common use of this is to find elements x where $v(x) = 3$. Suppose you already have an element a of valuation 3. If you know $v(x - a) \geq 4$, then "x is closer to a than a is to zero" so then $v(x) = 3$.

Corollary 4.6. *Given nonzero primes* $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ *and* $e_1, \dots, e_n \in \mathbb{Z}$*, there exists* $x \in K$ *such that* $v_{\mathfrak{p}_i}(x) = e_i$ *and* $v_{\mathfrak{q}}(x) \geq 0$ *for all other* $\mathfrak{q}$*.*

Definition 4.7. If A has only finitely many maximal ideals, then it is called *semilocal*.

Example: $\mathbb{Z}_{(3)} \cap \mathbb{Z}_{(5)}$.

Corollary 4.8. *A semilocal Dedekind domain is a PID.*

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the nonzero primes. Any nonzero ideal of A is $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$ for some $e_1, \dots, e_n \in \mathbb{Z}_{\geq 0}$. Then you can find some x such that $v_{\mathfrak{p}_i}(x) = e_i$ for all i. Then $(x) = \mathfrak{p}_1^{e_i} \dots \mathfrak{p}_n^{e_n}$. □

4.1. Review of separable field extensions. Let L/K be an algebraic extension of fields.

Definition 4.9. $f \in k[x]$ is *separable* if $\gcd(f, f') = 1$. Equivalently, f has distinct zeros in any field extension.

$\alpha \in L$ is *separable over* k if there is a separable polynomial $f \in k[x]$ such that $f(\alpha) = 0$. Equivalently (this is a theorem), the minimal polynomial of α is separable.

L is *separable over* k if every $\alpha \in L$ is separable over k. Otherwise, it is *inseparable*.

If $\operatorname{char} k = 0$, then it is automatic that the minimal polynomial of α is separable. So every field extension of a characteristic zero field is separable.

Proposition 4.10. *If* $F_1, F_2 \subset L$ *are separable over* K*, then* F_1F_2 *is separable over* K*.*

Corollary 4.11. *If $[L : k] < \infty$ then let F be the compositum of all separable extensions of K in L. (This is separable, so it is the maximal separable extension of K in L. Equivalently, $F = \{\alpha \in L : \alpha \text{ is separable/} k\}$.)*

Then F is separable/k.

Note that you get a tower of fields $L/F/k$.

Definition 4.12. The *separable degree* $[L : k]_s$ is defined to be $[F : k]$.

The *inseparable degree* $[L : k]_i$ is defined to be $[L : F]$.

These are multiplicative in towers.

Definition 4.13. L/k is *purely inseparable* if $[L : k]_s = 1$ ("there is no separable part").

A tower of separable extensions is separable. So if F is the maximal separable extension of k as above, then L/F is purely inseparable. This still works for infinite algebraic extensions.

Warning 4.14. L/k can't be both separable and inseparable (inseparable *means* "not separable"). But k/k *is* both separable and purely inseparable.

Theorem 4.15 (Primitive Element Theorem)**.** *If L/K is a finite separable extension, then $L = k(\alpha)$ for some $\alpha \in L$. (Equivalently, $L \cong k[x]/(f(x))$ where f is an irreducible polynomial.)*

Theorem 4.16. *Let k have characteristic $p \neq 0$. If L/k is purely inseparable of degree p, then $L = k(a^{1/p})$ for some $a \in k \backslash k^p$. Equivalently, $L \cong k[x]/(x^p - a)$.*

Every purely inseparable finite extension is a tower of such degree p extensions.

That is, you can get from F to L by repeatedly adjoining p^{th} roots of elements. A common proof strategy is to prove something for separable extensions, and for degree p extensions.

Corollary 4.17. *The inseparable degree is always a power of p as long as it's finite?.*

Example 4.18. If $k = \mathbb{F}_p(t)$ and $L = \mathbb{F}_p(t^{1/p})$ then L/k is a degree p purely inseparable extension.

Definition 4.19. k is *separably closed* if k has no finite separable extensions (except for k/k).

Definition 4.20. L is a *separable algebra* (or *finite étale algebra*) over k if L is a finite product of finite separable extensions of k.

Example 4.21. If k is already a separably closed field, then the separable algebras are $k \times \ldots \times k$.

Why do we care about separable algebras as opposed to just separable fields?

Proposition 4.22. *Suppose L/k is a separable algebra, and K'/k is any field extension, then $L \otimes_k K'$ is a separable algebra over K'.*

(This is similar to changing a real vector space V into a complex vector space $V \otimes_{\mathbb{R}} \mathbb{C}$.)

Even if L is a field, the base change $L \otimes_k K'$ might not be a field.

PROOF. Without loss of generality assume that L is a finite separable *field* extension of k (if not, just do this argument to each factor). By the Primitive Element Theorem, $L \cong k[x]/(f(x))$ for some irreducible separable polynomial f. (It is irreducible because L is a field.) Suppose f factors as $f_1(x) \ldots f_m(x)$ in K'. These are separable (no repeated roots in f, so these are distinct factors that also have no repeated roots). Then $L \otimes_k K' \cong K'[x]/(f(x))$; use the Chinese Remainder Theorem to show this is $\cong \prod_i K'[x]/(f_i(x))$. Each of these factors is a finite separable extension of K'. □

Proposition 4.23. *Suppose L/k is a separable algebra, and Ω is a separably closed field extension of k. Then*

$$L \otimes_k \Omega \cong \prod_{\sigma \in \Sigma} \Omega$$

where the indexing set Σ is $\mathrm{Hom}_k(L, \Omega)$ (ring homomorphisms that act as the identity on k).

In particular, the map $L \otimes_k \Omega \to \prod_\Sigma \Omega$ sends $\ell \otimes 1 \mapsto (\sigma(\ell))_\sigma$.

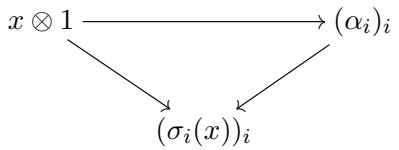
All of the pieces $K'[x]/(f_i(x))$ are finite separable extensions, so they must be Ω.

PROOF. Without loss of generality reduce to the case where $L = k[x]/(f(x))$ is a field generated by one element. Then f factors as $(x - \alpha_1) \ldots (x - \alpha_n)$ over the separably closed field, and these are distinct because we're talking about a separable extension. Each $\sigma : L \cong k[x]/(f(x)) \to \Omega$ is specified by sending x to a possible root α_i; conversely, each choice of root corresponds to a homomorphism.

I just need to show that

$$\begin{array}{ccc} L \otimes_k \Omega & \xrightarrow{x \otimes 1 \mapsto (\alpha_i)} & \prod \Omega[x]/(x - \alpha_i) \\ & \searrow^{(\sigma_i)} \quad \swarrow & \\ & \prod \Omega & \end{array}$$

commutes. Since $x \otimes 1$ generates $L \otimes_k \Omega$ over Ω, it suffices to check commutativity for $x \otimes 1$, and this is



which commutes by definition of σ_i. □

Lecture 5: September 18

Maybe you think of number fields as subfields of $\mathbb{C}$. But that requires choosing an embedding: there are two ways of embedding $\mathbb{Q}[z]/(x^2-2)$ in $\mathbb{C}$ – one sending $x \mapsto \sqrt{2}$ and one sending $x \mapsto -\sqrt{2}$. Is one better than the other? Just think of this as an abstract extension.

5.1. Norm and trace.

Definition 5.1. Let $A \subset B$ be rings such that B is free of rank n as an A-module. Let $b \in B$ and consider the multiplication-by-b map $B \to B$ as an A-linear map. This is a matrix, and the norm $N_{B/A}(b)$ is defined to be its determinant. The trace $\mathrm{Tr}_{B/A}(b)$ is the trace of $B \xrightarrow{b} B$.

Example 5.2. Let $A \subset B$ be $\mathbb{R} \subset C$ and choose the element $b = 2+3i$. Then $(2+3i)\cdot 1 = 2+3i$ and $(2+3)\cdot i = -3+2i$. The matrix is $\begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix}$. So $N_{\mathbb{C}/\mathbb{R}}(2+3i) = 13$ and $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(2+3i) = 4$.

Proposition 5.3. *"N and Tr respect base change." That is, let $A \subset B$ where B is free of rank n over A, and let $\varphi : A \to A'$ be any ring homomorphism. Then $B' = B \otimes_A A'$ is free of rank n over A (with essentially the same basis). Then*

$$\varphi\left(N_{B/A}(b)\right) = N_{B'/A'}(b \otimes 1) \text{ and } \varphi\left(\mathrm{Tr}_{B/A}\, b\right) = \mathrm{Tr}_{B'/A'}(b \otimes 1).$$

The idea is that it's essentially the same matrix (you just apply φ to everything).

Theorem 5.4. *In the setup of Proposition 4.23, we have:*

$$N_{L/K}(b) = \prod_{\sigma \in \Sigma} \sigma b$$

$$\mathrm{Tr}_{L/K}(b) = \sum_{\sigma \in \Sigma} \sigma b$$

PROOF. By Proposition 5.3, $N_{L/K}(b) = N_{L\otimes_k\Omega/\Omega}(b\otimes 1)$ and that is $N_{\Omega\times\ldots\times\Omega/\Omega}((\sigma b)_\sigma)$. There is an obvious basis for $\prod_\sigma \Omega$, and the matrix is just the diagonal matrix $\begin{pmatrix} \ddots & & \\ & \sigma b & \\ & & \ddots \end{pmatrix}$. □

Useful trick: if you want to prove something over a field that isn't algebraically closed, base change to an algebraically closed field; fields might turn into algebras.

Theorem 5.5. *Let C be free of rank m over B, and B be free of rank n over A. Then $N_{C/A}(c) = N_{B/A}(N_{C/B}(c))$ and $\mathrm{Tr}_{C/A}(c) = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(c))$.*

Proofs of this are unpleasant. But it has to do with the following fact: if you have matrices $A, B, C, D \in M_n$ that commute pairwise, then $\det_{2n}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det_n(AD - BC)$.

5.2. Bilinear pairings. Let K be a field, and let V be a finite-dimensional vector space. Let $\langle -,-\rangle : V \times V \to K$ be a symmetric bilinear pairing.

Definition 5.6. The *discriminant* of $\langle -,-\rangle$ with respect to a basis $e_1, \ldots, e_n$ of V is $\det(\langle e_i, e_j\rangle)_{1\le i,j\le n} \in K$. (I mean the determinant of the $n \times n$ matrix where the ij-entry is $\langle e_i, e_j\rangle$.) Write this as $disc(\langle -,-\rangle ; e_1, \ldots, e_n)$.

Applying a change-of-basis matrix A to (e_i) gives a new basis, and the discriminant gets multiplied by $(\det A)^2$.

$\langle -,-\rangle$ induces a map $V \to V^* = \mathrm{Hom}_{K\text{-linear}}(V, K)$ sending $v_0 \mapsto (w \mapsto \langle v_0, w\rangle)$.

Definition 5.7. The *left kernel* is the set $\{v_0 \in V : \langle v_0, w\rangle = 0\ \forall w\}$. The right kernel is analogous. If the pairing is symmetric, then these are the same thing.

Proposition 5.8. *TFAE:*

(1) $V \to V^*$ is an isomorphism
(2) the left kernel is 0
(3) $disc(\langle -,-\rangle ; any\ basis) \neq 0$

If any of these happen, say the pairing is nondegenerate.

PROOF. Elementary linear algebra. □

Given a basis (e_i) of V, you get a dual basis (f_i) of V^*, characterized by the fact that $f_j(e_i) = \delta_{ij}$.

If $\langle -, - \rangle$ is nondegenerate, you get a dual basis (e_i') of (f_i), characterized by the property that

$$\langle e_i', e_j \rangle = \delta_{ij}.$$

5.3. Extensions of Dedekind domains. Consider the finite separable extension $\mathbb{Q}(i)/\mathbb{Q}$. It turns out that the ring of integers $\mathbb{Z}[i]$ is a Dedekind domain. This is true in more generality.

Let A be a Dedekind domain, let $K = \operatorname{Frac} A$, let L be a finite separable extension (still a field), and let B be the integral closure of A in L.

Proposition 5.9. *$B \cap K = A$.*

PROOF. A is integrally closed. □

Proposition 5.10. *$K \cdot B = L$ ($K \cdot B$ is the K-vector space spanned by B).*

Idea: elements of L can be scaled to be in B.

PROOF. Use the fact that integral closure commutes with localization (this was on the HW). Let $S = A \backslash \{0\}$. Then S^{-1}(integral closure of A in L) = integral closure of $S^{-1}A$ in L. This is just $K \cdot B$ = integral closure of K in L, which is just L (every element of L satisfies a monic polynomial over K). □

Proposition 5.11. *If $x \in B$ then $\operatorname{Tr}_{L/K}(x) \in A$.*

PROOF. Fix a separably closed $\Omega \supset K$. Then $\operatorname{Tr}_{L/K}(x) = \sum \sigma s x$. If you apply a homomorphism to something integral, it stays integral, because you can just apply the homomorphism to the entire monic polynomial. So σx is integral over A, and so is $\sum_\sigma \sigma x$. But we already know that the trace is in K. Since A is integrally closed, anything that is in K and integral over A, is also A. □

Since L/K is separable, $\operatorname{Tr} : L \to K$ is not identically zero (this is on the HW – hint: base-change to an algebraic closure). Take the trace pairing $L \times L \to K$ given by $(x, y) \mapsto \operatorname{Tr}(xy)$. This is nondegenerate: if $\operatorname{Tr}(a) \neq 0$, then given nonzero x, its pairing with $\frac{a}{x}$ is nondegenerate.

(Note: it's possible that $\operatorname{Tr}(1) = 0$, if you're in characteristic p and there are p things on the diagonal.)

Given an A-submodule M in L (this is analogous to a $\mathbb{Z}$-lattice), define the dual module

$$M^* := \{x \in L \,:\, \operatorname{Tr}(xm) \in A \ \forall m \in M\}.$$

Example 5.12. If M is free of rank n with basis $e_1, \ldots, e_n$ then M^* is free of rank n with basis $e_1', \ldots, e_n'$ (the dual basis we defined earlier using the pairing).

Proposition 5.13. *B is a finitely generated A-module.*

PROOF. By Proposition 5.10, we know that B spans L as a K-vector space. So we can find a K-basis $e_1, \dots, e_n \in B$ of L. (Or, if they weren't in B to begin with, scale them by K to assume they are in B.) Let $M =$ the A-span of $e_1, \dots, e_n$; this is contained in B. Then $B \subset B^*$ (this is by Proposition 5.11). But it's harder to be in B^* than M^*, so we get inclusions $M \subset B \subset B^* \subset M^*$. M and M^* are finitely generated free A-modules. Since A is Noetherian (it's a Dedekind domain), any submodule of M^* is also finitely generated.

(Bonus: B^* is finitely generated.) □

Lemma 5.14. *Suppose B is integral over A (these are just rings; we're forgetting the previous setup for now). Let $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ be primes of B. Then $\mathfrak{q}_0 \cap A \subsetneq \mathfrak{q}_1 \cap A$.*

PROOF. Map everything into $B/\mathfrak{q}_0$ to reduce to the case where $\mathfrak{q}_0 = 0$ and B is a domain. The assumption on $\mathfrak{q}_1$ is now just that it is not the zero ideal. Choose nonzero $x \in \mathfrak{q}_1$. We proved that the minimal polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for x has coefficients in A. We have $a_0 \neq 0$, because otherwise you could divide by x and get a lower-degree polynomial. Write $a_0 = -x^n - \cdots = x(\text{element of } B)$. Since $x \in \mathfrak{q}_1$, this shows $a_0 \in \mathfrak{q}_1$. Also $a_0 \in A$, Therefore $\mathfrak{q}_1 \cap A$ is not the zero ideal (i.e. not $\mathfrak{q}_0 \cap A$), because it contains a_0. □

Corollary 5.15. *Under the hypotheses of Lemma 5.14,* $\dim B \leq \dim A$.

PROOF. If B has an n-step chain of distinct primes, then intersect this with A to get a chain of distinct primes in A. □

Theorem 5.16. *Back to the setting at the beginning of this subsection. B is a Dedekind domain.*

PROOF. **B is Noetherian:** B is finitely generated over A.

B is integrally closed: any x that is integral over B is integral over A, and A is integrally closed.

$\dim B \leq 1$: By Corollary 5.15, $\dim B \leq \dim A$, and that's ≤ 1 by assumption. □

It turns out that if L/K is not separable, this is still true, but it's harder, because B is *not* finitely generated as an A-module.

Corollary 5.17. *The ring of integers of any number field is a Dedekind domain.*

If you have some prime $\mathfrak{p} \subset A$, then $\mathfrak{p}B$ is an ideal, but not necessarily a prime. But it is a fractional ideal in a Dedekind domain, so it factors as $\mathfrak{p}B = \prod_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}}}$ (product over nonzero

prime ideals of B). The $\mathfrak{q}$'s that appear are the ones that, if you intersect them with A, you get $\mathfrak{p}$.

Definition 5.18. $e_\mathfrak{q}$ is called the *ramification index* of $\mathfrak{q}$ over $\mathfrak{p}$.

$A/\mathfrak{p}$ is a field, because nonzero primes in a Dedekind domain are maximal; similarly, $B/\mathfrak{q}$ is a field. The inclusion $A/\mathfrak{p} \subset B/\mathfrak{q}$ has finite degree: B is a finite A-module, so generators of B over A also become generators of $B/\mathfrak{q}$ over $A/\mathfrak{p}$.

Definition 5.19. The *residue field degree* $f_\mathfrak{q}$ *of* $\mathfrak{q}$ *over* $\mathfrak{p}$ is defined to be $[B/\mathfrak{q} : A/\mathfrak{p}]$.

Note: e and f are standard notation.

Example 5.20. Let $\mathfrak{p} = (5) \subset \mathbb{Z}$; this splits into $(2+i)(2-i)$ in $\mathbb{Z}[i]$. Let $\mathfrak{q} = (2+i)$. Then $e_\mathfrak{q} = 1$ (there's no exponent in this product expansion). Now look at $\mathbb{Z}/5\mathbb{Z} \subset \mathbb{Z}[i]/(2+i)$ and count the elements in $\mathbb{Z}[i]/(2+i)$; there are 5 elements, so $f_\mathfrak{q} = 1$.

(One way to see this: it is clear that $\mathbb{Z}[i]/(5)$ contains 25 elements, and $\mathbb{Z}[i]/(2+i)$ has fewer elements, and still contains $\mathbb{Z}/5\mathbb{Z}$, *and* is still a field extension.)

Definition 5.21. If $\mathfrak{q}$ is a prime of B and $\mathfrak{p}$ is a prime of A, then write $\mathfrak{q} \mid \mathfrak{p}$ if $\mathfrak{q} \supset \mathfrak{p}$ (the ones that actually appear in the factorization).

Theorem 5.22. *Suppose $A \subset B$ are Dedekind domains. Suppose $\mathfrak{p} \subset A$ and $\mathfrak{p}$ splits as $\prod \mathfrak{q}^{e_\mathfrak{q}}$ in B. Then $\sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q} = [L : K]$.*

Lecture 6: September 23

Last time, we talked about a finite separable extension L/K of degree n and a Dedekind domain $A \subset K$; we proved that the integral closure B of A in L is a Dedekind domain.

Recall we defined $\mathfrak{q} \mid \mathfrak{p}$ to mean that $\mathfrak{q}$ appears in the factorization of $\mathfrak{p}B$. Equivalently, $\mathfrak{q} \supset \mathfrak{p}B$, or $\mathfrak{q} \supset \mathfrak{p}$ (as a B-ideal), or $\mathfrak{q} \cap A = \mathfrak{p}$.

Example 6.1. Let $A = \mathbb{Z}$, $B = \mathbb{Z}[i]$, $\mathfrak{p} = (5)$ then $\mathfrak{q} = (2+i) \mid \mathfrak{p}$.

If we write $\mathfrak{p}B = \prod_\mathfrak{q} \mathfrak{q}^{e_\mathfrak{q}}$ then $e_\mathfrak{q}$ is the ramification index of $\mathfrak{q}$ and $f_\mathfrak{q} := [B/\mathfrak{q} : A/\mathfrak{p}]$ is the residue field degree. Today, we will prove:

Proposition 6.2. $[B/\mathfrak{p}B : A/\mathfrak{p}] = n$ *(the degree of the field extension L/K)*

Proof. Let $S = A \backslash \mathfrak{p}$ so $A' := S^{-1}A = A_\mathfrak{p}$. Write $B' = S^{-1}B$. $A'/\mathfrak{p}A' = S^{-1}(A/\mathfrak{p}) = A/\mathfrak{p}$ since each $s \in S$ acts invertibly on $A/\mathfrak{p}$. Similarly, $B'/\mathfrak{p}B' = S^{-1}(B/\mathfrak{p}B) = B/\mathfrak{p}B$. So

we can reduce to the case where A is a DVR, hence a PID. Since B is finitely generated and torsion-free as an A-module, B is free as an A-module. Also $K \cdot B = L$, so L is free over K of the same rank. Thus B is free of rank n as an A-module, so $B/\mathfrak{p}B$ is free of rank n as an $A/\mathfrak{p}$-module. □

Proposition 6.3. $\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = n$

Proof. Use the Chinese Remainder Theorem to show $B/\mathfrak{p}B = \prod B/\mathfrak{q}^{e_{\mathfrak{q}}}$ (you need any two factor ideals to generate the unit ideal, which is true here). We already checked that $B/\mathfrak{p}B$ has dimension n over $A/\mathfrak{p}$. We need to show that $B/\mathfrak{q}_{e_{\mathfrak{q}}}$ has dimension $e_{\mathfrak{q}} f_{\mathfrak{q}}$. There is a chain of ideals $B \supset \mathfrak{q} \supset \mathfrak{q}^2 \supset \ldots \mathfrak{q}^{e_{\mathfrak{q}}}$. To get the dimension, add up the dimensions of successive quotients. $\mathfrak{q}^i/\mathfrak{q}^{i+1}$ is a 1-dimensional $B/\mathfrak{q}$-vector space, hence an $f_{\mathfrak{q}}$-dimensional $A/\mathfrak{p}$-vector space. There were $e_{\mathfrak{q}}$ steps in the chain, so $\dim B/\mathfrak{q}^{e_{\mathfrak{q}}} = e_{\mathfrak{q}} f_{\mathfrak{q}}$. □

Corollary 6.4. *Given $\mathfrak{p}$, the number of $\mathfrak{q}$ dividing $\mathfrak{p}$ is between 1 and n.*

Proof. Count the number of terms in $\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}} = n$. □

Definitions 6.5.

- L/K is *totally ramified at* $\mathfrak{q}$ if $e_{\mathfrak{q}} = n$. (In that case, $f_{\mathfrak{q}} = 1$, and $\mathfrak{q}$ is the only prime lying over $\mathfrak{p}$.)
- L/K is *unramified at* $\mathfrak{q}$ if $e_{\mathfrak{q}} = 1$ and $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$.
- L/K is *unramified above* $\mathfrak{p}$ if it is unramified at every $\mathfrak{q} \mid \mathfrak{p}$. Equivalently, using the Chinese Remainder Theorem, $B/\mathfrak{p}$ is a separable algebra (finite étale algebra) over $A/\mathfrak{p}$. (For the other direction of this equivalence, $B/\mathfrak{p}B = \prod B/\mathfrak{q}^{e_{\mathfrak{q}}}$ is not even a product of fields unless $e_{\mathfrak{q}} = 1$.)
- L/K is *inert* if $\mathfrak{p}B$ is prime (so $e = 1$ and $f = n$).
- L/K *splits* (or *splits completely*) if $e_{\mathfrak{q}} = f_{\mathfrak{q}} = 1$ for all $\mathfrak{q} \mid \mathfrak{p}$.

Definitions 6.6.

- $\mathcal{I}_A := \{\text{nonzero fractional ideals of } A\}$
- The *class group* is $Cl(A) := \mathcal{I}_A/\{\text{principal fractional ideals}\}$. This is sometimes called the Picard group $\mathrm{Pic}(A)$ (and coincides with $\mathrm{Pic}(\operatorname{Spec} A)$ in algebraic geometry).

Definition 6.7. Let L/K be a finite separable field extension; let v be a discrete valuation on K and w a discrete valuation on L. Say that w *extends* v *with index* $e \in \mathbb{N}$ if $w|_K = e \cdot v$.

Proposition 6.8. *Fix $\mathfrak{p}$. Then there is a bijection*

$$\{\textit{primes dividing } \mathfrak{p}\} \longleftrightarrow \{\textit{discrete valuations on } L \textit{ extending } v_{\mathfrak{p}}\}$$

sending $\mathfrak{q} \mapsto v_{\mathfrak{q}}$.

PROOF. First check this is well defined – that $v_{\mathfrak{q}}$ extends $v_{\mathfrak{p}}$. Suppose that $\mathfrak{q} \mid \mathfrak{p}$ and let $e = e_{\mathfrak{q}}$. Localize at $\mathfrak{q}$: $\mathfrak{p}B_{\mathfrak{q}} = (\mathfrak{q}B_{\mathfrak{q}})^e$ (localizing gets rid of the other factors in the product). Take the valuation of $\mathfrak{p}^m B_{\mathfrak{q}} = (\mathfrak{q}B_{\mathfrak{q}})^{em}$ to get $v_{\mathfrak{q}}(\mathfrak{p}^m B_{\mathfrak{q}}) = em$. More generally, $v_{\mathfrak{q}}(IB_{\mathfrak{q}}) = e \cdot v_{\mathfrak{p}}(I)$ for any $I \in \mathcal{I}_A$ since all that matters is the $\mathfrak{p}$-part of I, which looks like $\mathfrak{p}^m$ for some m. Take $I = (x)$ to get $v_{\mathfrak{q}}(x) = e \cdot v_{\mathfrak{p}}(x)$.

Injective: if $\mathfrak{q} \neq \mathfrak{q}'$, by weak approximation there exists $x \in L^\times$ such that $v_{\mathfrak{q}}(x) = 3$ and $v_{\mathfrak{q}'}(x) = 5$, so $v_{\mathfrak{q}}$ and $v_{\mathfrak{q}'}$ are different functions.

Surjective: Now suppose w is any discrete valuation on L extending $v_{\mathfrak{p}}$. So $w(x) = e \cdot v_{\mathfrak{p}}(x)$ for all $x \in K$. Let $W = \{x \in L : w(x) \geq 0\}$ (this is supposed to be $B_{\mathfrak{q}}$) and $\mathfrak{m} = \{x \in L : w(x) > 0\}$ (this is supposed to be the maximal ideal $\mathfrak{q}B_{\mathfrak{q}}$). Since $w|_K = e \cdot v_{\mathfrak{p}}$, which is ≥ 0 on A, $W \supset A$. Suppose W is integrally closed in L, so $W \supset B$. Let $\mathfrak{q} = \mathfrak{m} \cap B$; this is a prime ideal containing $\mathfrak{m} \cap A = \mathfrak{p}$. Since $w(x) = e \cdot v_{\mathfrak{p}}(x)$, $w(x) > 0 \iff v_{\mathfrak{p}}(x) > 0$. Now we have to show that $W = B_{\mathfrak{q}}$ (i.e. that w comes from $\mathfrak{q}$). We showed on the HW that there are no rings between L and $B_{\mathfrak{q}}$ except for L and $B_{\mathfrak{q}}$. It's not all of L, so it is $B_{\mathfrak{q}}$. □

Example 6.9. Let $A = \mathbb{Z}$ and $B = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[x]/(x^2+5)$ inside the field extension $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. Pick $\mathfrak{p} = (3)$; then $B/\mathfrak{p}B = \mathbb{Z}[x]/(x^2+5)/(3) = \mathbb{Z}[x]/(3, x^2+5) = \mathbb{Z}[x]/(3)/(x^2+5) = \mathbb{F}_3[x]/(x^2+5) = \mathbb{F}_3[x]/(x^2-1) \cong \mathbb{F}_3[x]/(x+1) \times \mathbb{F}_3[x]/(x-1)$ (by the Chinese Remainder theorem). You can undo this as $\mathbb{Z}[x]/(3, x+1) \times \mathbb{Z}[x]/(3, x-1)$. So $(3) = (3, \sqrt{-5}+1) \cdot (3, \sqrt{-5}-1)$. By Proposition 6.3, $e = 1 = f$ for both of these. So this splits completely.

If you do it with $\mathfrak{p} = (2)$, it's totally ramified (mod 2, you get $x^2 + 5 \equiv (x+1)^2$).

(5) is also totally ramified; (7) splits; (11) is inert.

Theorem 6.10. *Let A, B, K, L be as usual. Suppose $B = A[\alpha]$ and let $f(x)$ be the minimal polynomial of α over K (this is actually in $A[x]$). If $f(x) = \prod (g_i(x) \pmod{\mathfrak{p}})^{e_i}$ (where $g_i(x)$ are distinct monic irreducible polynomials) is a factorization in $A/\mathfrak{p}[x]$, then*

$$\mathfrak{p} = \prod \mathfrak{q}_i^{e_i} \text{ where } \mathfrak{q}_i = (\mathfrak{p}, g_i(\alpha)).$$

$B/\mathfrak{q}_i \cong A/\mathfrak{p}[x]/(g_i(x) \pmod{\mathfrak{p}})$ has residue field degree $f_i = \deg g_i$.

Note that if you take the degrees of both sides of $f(x) = \prod (g_i(x))^{e_i}$ as polynomials over $A/\mathfrak{p}$, you recover $n = \sum e_i f_i$.

In our example above, the g_i's were $x - 1$ and $x + 1$.

Warning 6.11. This works only if B is generated over A by one element. If this is not true, you could try localizing at $\mathfrak{p}$ and see if this assumption now holds.

Example 6.12. Let $A = \mathbb{C}[x]$ (so all the residue fields are $\cong \mathbb{C}$). Use the extension $L = \mathbb{C}(y)$ where $y = \sqrt{x}$, over $K = \mathbb{C}(x)$. Then y is integral over A (it satisfies $y^2 - x = 0$), and in fact this is the entire integral closure: $B = \mathbb{C}[x, y]/(y^2 - x) \cong \mathbb{C}[y]$; this is integrally closed because it's a UFD.

The primes of A all have the form $x - a$. Choose $a = 4$; then $(x-4)B = (y^2-4)B = (y+2)\cdot(y-2)$, so it splits completely. If $a = 0$, then $(x)B = (y^2)B = (y)^2B$; this has $e = 2$ and $f = 1$ (totally ramified).

(The picture of $\operatorname{Spec} B$ over $\operatorname{Spec} A$ is the branched cover $y^2 = x$ over the x-axis. There are two preimages everywhere except 0, the point of ramification. Really, you should be drawing the 2-sheeted cover over $\mathbb{C}$, where the sheets are indexed by $\mathbb{Z}/2$ and are attached at the origin. Alternatively, "unramified" is the analogue of a covering space. We will show that there are only finitely many primes that ramify (where it's not a covering space).)

Note: for curves over $\mathbb{C}$, all the f's are 1: there aren't any (nontrivial) possibilities for $B/\mathfrak{q}$ over $\mathbb{C}$. If it's also unramified, then $\sum e_i f_i = n$ tells you that you have the "right" number of preimages.

Lecture 7: September 25

Let A be a Dedekind domain and $K = \operatorname{Frac} A$.

Definition 7.1. Let V be an r-dimensional vector space over K. An *A-lattice in V* is a finitely generated A-submodule $M \subset V$ such that $K \cdot M = V$ (i.e. the lattice actually spans the vector space over K).

Suppose M, N are free lattices (free as modules) in V. Then there are isomorphisms $M \cong A^r \cong N$; let $\varphi : M \to N$ be the composition. This induces a K-linear map $\varphi_K : V = M \otimes K \to N \otimes K = V$. Define

$$(M : N) := (\det \varphi_K)$$

(a fractional ideal of A). Changing bases changes $\det \varphi_K$ by a unit, so the fractional ideal is well-defined.

If M, N are not free, define $(M : N)$ as the fractional ideal such that $(M : N)_\mathfrak{p} = (M_\mathfrak{p} : N_\mathfrak{p})$ is as before. (The local ring is a DVR, hence a PID, and every module over a PID is free.)

Example 7.2. Think about the lattice spanned by, e.g. $(1, 2)$ and $(3, 1)$ in $\mathbb{Q}^2$.

More generally, if $A = \mathbb{Z}$ and $M \supset N$ then $(M : N)$ equals the index (viewed as usual).

Proposition 7.3. *If $M \supset N$ and $M/N \cong A/I_1 \oplus \ldots \oplus A/I_n$ then $(M : N) = I_1 I_2 \ldots I_n$.*

Proof. Everything involved in these constructions behaves nicely wrt localization, so without loss of generality assume A is a DVR. Then $M \cong A^r$, and there is some $\varphi : A^r \to A^r$ such that $N \cong \varphi(A^r)$. You can write $T_1 \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_r \end{pmatrix} T_2$ where $T_i \in GL_n(A)$ (changing the basis on both sides gives you more freedom than the usual diagonalization). This is called

Smith normal form. Then $M/N = \operatorname{coker}\varphi \cong A/(a_1)\oplus\ldots\oplus A/(a_r)$. In the problem statement we assumed that $M/N \cong A/I_1 \oplus \ldots \oplus A/I_n$.

Over $\mathbb{Z}$, we could just count the number of elements on each side and compute the index. But these might not be finite as abelian groups. Instead, use *length*, the number of steps in a maximal chain of submodules. (For example, a maximal chain for $\mathbb{Z}/8$ is $\mathbb{Z}/8 \supset 2\mathbb{Z}/8\mathbb{Z} \supset 4\mathbb{Z}/8\mathbb{Z} \supset 0$.) It turns out (Jordan-Hölder) that this works for every Dedekind domain, and this length is well-defined (if finite).

So take the length of both sides of $\bigoplus A/(a_i) = \bigoplus A/I_i$ (as A-modules), to get $(a_1 \ldots a_n) = I_1 \ldots I_n$ and the former is $(\det\varphi) = (M : N)$. *Remember we are working over a DVR, so if you know the length of an ideal, then you know the ideal.* □

Let A, B, K, L as in the last lecture.

Definition 7.4 (i and N (ideal norm))**.** Let $i : \mathcal{I}_A \to \mathcal{I}_B$ be the map taking $I \mapsto IB$; let $N : \mathcal{I}_B \to \mathcal{I}_A$ be the map sending $J \mapsto (B : J)$.

(For example, in $\mathbb{Z}[i]/\mathbb{Z}$, if $J = (5)$ then $N(J) = (\mathbb{Z}[i] : (5))_{\mathbb{Z}} = (25)$.)

Proposition 7.5. *There are commutative diagrams*

$$\begin{array}{ccc} K^\times & \hookrightarrow & L^\times \\ \downarrow & & \downarrow \\ \mathcal{I}_A & \xrightarrow{i} & \mathcal{I}_B \end{array} \qquad\qquad \begin{array}{ccc} L^\times & \xrightarrow{N_{L/K}} & K^\times \\ \downarrow & & \downarrow \\ \mathcal{I}_B & \xrightarrow{N} & \mathcal{I}_A \end{array}$$

where the vertical maps are $x \mapsto (x)$.

Proof. The first diagram is really obvious.

By definition, if $x \in L^\times$ then $N((x)) = (B : xB)_A = (\det(L \xrightarrow{x} L))$ (since $B \xrightarrow{x} xB$ is an isomorphism), and this is the definition of the norm. □

Proposition 7.6. *i and N are homomorphisms.*

Proof. i: obvious.

N: this would be obvious if every ideal were principal (since we proved that it's just the norm, on "elements"). Localize to assume that A is a DVR. Then B is a semilocal Dedekind domain, hence a PID. $N_{L/K}$ is a homomorphism, so N is a homomorphism. □

Proposition 7.7. *For primes $\mathfrak{q} \mid \mathfrak{p}$, $N(\mathfrak{q}) = \mathfrak{p}^f$, where $f = f_q$.*

PROOF. $B/\mathfrak{q}$ is an $A/\mathfrak{p}$ vector space, so it breaks up as $B/\mathfrak{q} \cong A/\mathfrak{p} \oplus \ldots \oplus A/\mathfrak{p}$ (with f factors). This is also a decomposition as A-modules. So $N(\mathfrak{q}) = (B : \mathfrak{q})_A = \mathfrak{p}^f$. □

Aside 7.8. For smooth curves over $\mathbb{C}$: there should be n points over $\mathfrak{p}$, but at ramified points there are fewer. Let $Y = \operatorname{Spec} B$ and $X = \operatorname{Spec} A$; then $\mathcal{I}_A = \operatorname{Div} X$, and $\mathcal{I}_B = \operatorname{Div} Y$. The maps N and i give rise to maps $f_* : \operatorname{Div} Y \to \operatorname{Div} X$ and $f^* : \operatorname{Div} X \to \operatorname{Div} Y$, respectively. i sends $\mathfrak{p} \mapsto \mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$, so $f^*(P) = \sum_{\substack{\mathfrak{q} \text{ s.t.} \\ f(\mathfrak{q})=\mathfrak{p}}} e_{\mathfrak{q}}\mathfrak{q}$ (this is called the inverse image, or pullback, of divisors). So in the picture of $Y = \operatorname{Spec} B$ over $X = \operatorname{Spec} A$, this is taking the preimage of a point with multiplicity.

N sends $\mathfrak{q}$ to $\mathfrak{p}^f$, but f_* just takes $\mathfrak{q} \mapsto \mathfrak{p} = f(\mathfrak{q})$. (This is only since $X/\mathbb{C}$.) This is called the image, or pushforward.

If you start downstairs, go upstairs and then go downstairs (i.e. $f_* \circ f^*$), then this is multiplication by f.

Let A be a DVR with maximal ideal $\mathfrak{p} = (\pi)$; let $K = \operatorname{Frac} A$. Let $B = A[x]/(f(x))$ for some monic f. Let $\overline{f}$ be the image of f in $A/\mathfrak{p}[x]$, and let β be the image of x in B.

The aim is eventually to show that B *is* the integral closure.

Lemma 7.9 (Nakayama's lemma)**.** *Let A be a local ring with maximal ideal $\mathfrak{p}$, and let M be a finitely generated A-module. Suppose $x_1, \ldots, x_n$ generate $M/\mathfrak{p}M$ as an $A/\mathfrak{p}$-vector space. Then $x_1, \ldots, x_n$ generate M as an A-module.*

Lemma 7.10. *Any maximal ideal $\mathfrak{m}$ of B contains $\mathfrak{p}$.*

PROOF. If not, then $\mathfrak{m} + \mathfrak{p}B = B$ (it's strictly bigger than a maximal ideal). So $\mathfrak{m}$ generates $B/\mathfrak{p}B$. Since we're working over a Noetherian ring, $\mathfrak{m}$ is finitely generated. By Nakayama's lemma, the generators of $\mathfrak{m}$ are generators of B, i.e. $\mathfrak{m} = B$. This is a contradiction. □

Corollary 7.11. *There is a correspondence*

$$\{\text{maximal ideals of } B\} \longleftrightarrow \{\text{maximal ideals of } B/\mathfrak{p}B\} \longleftrightarrow \{\text{irreducible factors of } \overline{f}\}$$

given more precisely by

$$(\mathfrak{p}, g_i(\beta)) \longleftrightarrow (\overline{g}_i(x)) \longleftrightarrow \overline{g}_i.$$

(Recall β is the image of x in $B = A[x]/(f)$.)

PROOF. The first arrow is Lemma 7.10; the second is from writing $B/\mathfrak{p}B = A/\mathfrak{p}[x]/(\overline{f}(x))$. □

There are two special cases in which we can deduce that B is a DVR (and hence is integrally closed, and f is irreducible over K).

Case 1: $\overline{f}$ is irreducible. Then, according to this description, the only maximal ideal of B is $(\mathfrak{p}, f(\beta)) = \mathfrak{p}B = \pi B$. Also, π is not nilpotent (because it's not nilpotent in $A \subset B$). So B is a DVR.

Its residue field is $A/\mathfrak{p}[x]/(\overline{f})$. Also $e = 1$ and $f = n$, so $\mathfrak{p}$ is inert; it is ramified as long as the residue field extension is separable. This happens as long as $\overline{f}$ is a separable polynomial.

Case 2: f is an Eisenstein polynomial. (That is, $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with all $a_i \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$.) So $\overline{f} = x^n$, and again there is only one irreducible factor (x). By the correspondence, there is a unique maximal ideal of B, i.e. $(\mathfrak{p}, \beta) = (a_0, \beta)$ (since a_0 is in $\mathfrak{p}$ but not $\mathfrak{p}^2$). We need to show that it's a PID, with a non-nilpotent generator. Write $a_0 = -\beta^n(1 + \cdots + a_1)$. So a_0 is a multiple of β, so the ideal is just (β). Also a_0 is not nilpotent, so β is not nilpotent.

So B is a DVR, with residue field $B/(\beta) = A[x]/(x, \mathfrak{p}) = A/\mathfrak{p}$. In this case, $e = n$ and $f = 1$ (so it's totally ramified).

(There are converses: e.g. if you start with a totally ramified extension, you can show it comes in this way.)

Lecture 8: September 30

Let K be a field, and L a finite extension of K with $[L : K] = n$. Let A be a Noetherian, integrally closed domain, with $\operatorname{Frac} A = K$. Let B be the integral closure of A in L. (E.g. if $A = \mathbb{Z}$, $L = \mathbb{Q}$, then L is a number field and B is the ring of integers.)

Assume L/K is separable, and A is a Dedekind ring. We showed that this implies B is a Dedekind ring.

Let P be a prime ideal in B, $\mathfrak{p} := P \cap A$ (so in the picture of $\operatorname{Spec} B$ over $\operatorname{Spec} A$, P is a preimage of $\mathfrak{p}$). Say that $P \mid \mathfrak{p}$. Write

$$\mathfrak{p}B = \prod_{P \cap A = \mathfrak{p}} P^{e_P}$$

where e_P is the ramification index. B/P is a field that contains $A/\mathfrak{p}$, and denote $[B/P : A/\mathfrak{p}] =: f_P$ (the residue index). The extension $B/P \Big/ A/\mathfrak{p}$ is called the residue extension. Then $B/\mathfrak{p}B = \prod_{P \cap A = \mathfrak{p}} B/P^{e_\mathfrak{p}}$ (it's not a field, and it's not even a product of fields if there is nontrivial ramification). Say that

- $\mathfrak{p}$ is ramified if $e_P > 1$ for some P
- $\mathfrak{p}$ is unramified if for all P over $\mathfrak{p}$, $e_P = 1$
- $\mathfrak{p}$ is totally ramified if $\mathfrak{p}B = P^e$ for some single P
- $\mathfrak{p}$ splits completely if for all P lying over $\mathfrak{p}$, $e_\mathfrak{p} = f_\mathfrak{p} = 1$.

Different primes might have different ramification behavior; the way to unify this is to consider Galois extensions.

If, e.g. when $A = \mathbb{Z}$, $A/\mathfrak{p}$ is a finite field, the Galois extensions are cyclic, generated by Frobenius.

From now on, assume that L is a Galois extension of K. We have a Galois group $G(L/K)$.

Proposition 8.1. *The group $G(L/K)$ acts transitively on the set of primes P of B lying above any given prime $\mathfrak{p}$ of A.*

(Topology analogy: if you have a space with a cover, the cover is called "Galois" if the automorphism group acts transitively on the fibers.)

PROOF. Let's show that $G(L/K)$ does act on the set of such P. Let $s \in G(L/K)$. We need $s(P) \subset B$; it's clearly in L, but it's in B because B is integrally closed (all the Galois conjugates of an integral element are integral). You can check that it's an ideal, and that it's prime. $s(P) \cap A = P \cap A = \mathfrak{p}$ because s acts trivially on A.

Now we show that the action is transitive. Let P, P' be two primes above $\mathfrak{p}$. Assume for the sake of contradiction that, for all $s \in G(L/K)$, $s(P) \neq P'$ (i.e. P' is not in the orbit). Let $a \in P$ and $x = N_{L/K}(a)$; we know $x = \prod_{s \in G(L/K)} s(a) \in A$. By assumption, $s(a)$ does not belong to P' for any s. But $\prod_s s(a) \in A \cap P = \mathfrak{p} = P' \cap A$. This is a contradiction. □

Corollary 8.2. *The integers e_P and f_P do not depend on P as P varies among the primes above $\mathfrak{p}$.*

In the Galois case, we write $e_\mathfrak{p}, f_\mathfrak{p}$ for these integers. Let $g_\mathfrak{p}$ be the number of P's above $\mathfrak{p}$. Write $\mathfrak{p}B = \prod_{P \cap A = \mathfrak{p}} P^{e_\mathfrak{p}}$.

Corollary 8.3. $n = [L : K] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$

If it's an extension of prime degree, there aren't that many choices (two of these things are 1, and the other is p).

$G(L/K)$ acts on the set $\{P \text{ above } \mathfrak{p}\}$.

Definition 8.4. Let $D(P) = D_P(L/K)$ be the stabilizer of P, i.e.

$$D(P) = \{s \in G(L/K) \,:\, s(P) = P\}.$$

Question: how does D depend on P? Let P' be another prime with $P' \cap A = P \cap A$.

We know that $P' = t(P)$ for some $t \in G(L/K)$. So $D(P') = \{s \in G(L/K) \,:\, s(t(P)) = t(P)\} = tD(P)t^{-1}$. (E.g. this vanishes in an abelian extension.)

(When you talk about the fundamental group of a variety, changing the basepoint corresponds to conjugation of the group.)

The index of $D(P)$ in $G(L/K)$ is the size of the orbit $= g_{\mathfrak{p}}$. So $\#D(P) = e_{\mathfrak{p}} f_{\mathfrak{p}}$. $D(P)$ is a subgroup of my Galois group, so it is itself a Galois group. I will show that it is (related to) the Galois group of the residue extension.

Fix P, and define $D = D(P)$, $e = e_{\mathfrak{p}}$, $f = f_{\mathfrak{p}}$, $g = g_{\mathfrak{p}}$. D corresponds to an intermediate extension

$$K \hookrightarrow K_D \hookrightarrow L,$$

i.e. $D = G(L/K_D)$; this is an extension of degree f. K_D/K is not necessarily a Galois extension, but it has degree g. Galois theory says that K_D/K is Galois iff D is normal in $G(L/K)$.

In general, for any $K \hookrightarrow E \hookrightarrow L$, write $B_E = B \cap E$, $P_E = P \cap E$, $\overline{E} = B_E/P_E$. In particular, write $\overline{L} = B/P$ and $\overline{K} = A/\mathfrak{p}$.

Let $s \in D = D(P)$. s acts on B, and by definition, $s(P) = P$. s induces an automorphism of $B/P = \overline{L}$, and leaves $\overline{K}$ invariant. So we get a map

$$\varepsilon : D \to G(\overline{L}/\overline{K}).$$

Definition 8.5. Define $T := \ker \varepsilon$ to be the *inertia subgroup* of P.

Proposition 8.6. *$\overline{L}/\overline{K}$ is normal (but not necessarily separable), and ε is onto (so $D/T \xrightarrow{\cong} G(\overline{L}/\overline{K})$).*

(I.e., $\overline{L}$ is the splitting field of a bunch of polynomials – if you have one root of something, then you have all the roots.)

(This is a computational tool for finding $G(L/K)$; by reducing at different primes, you can hope to find different cyclic elements.)

Proof. Let $\overline{a} \in \overline{L}$. The goal is to show that $\overline{a}$ is a root of a monic polynomial in $\overline{K}[x]$, which is split in $\overline{L}$.

Let $a \in B$ have image $\overline{a}$. Define $P(x) = \prod_{s \in G(L/K)} (x - s(a)) \in A[x]$; then the reduction $\overline{P}$ of P vanishes at $\overline{a}$ and splits in $\overline{L}$. This proves normality.

Now let $\overline{L}_s$ be the separable closure of $\overline{K}$ in $\overline{L}$. Then there is a tower of fields $\overline{L}/\overline{L}_s/\overline{K}$, and $\overline{L}/\overline{L}_s$ is purely inseparable. (If you don't like this, you could assume instead that the field is perfect, so all the residue field extensions are separable.)

Find a generator $\overline{a} \in \overline{L}_s$.

Lemma 8.7. *We can find $a \in B$ mapping to $\overline{a}$ such that, for all $s \in G(L/K) \backslash D$, $a \in s^{-1}(P)$.*

(s^{-1} vs. s is just a notational convenience.) This is a consequence of the approximation theorem (you can find elements with the right residues). We only require things about $s(P)$ for $s \notin D$, i.e. for $s(P) \neq P$.

Now letting again $P(x) = \prod_{s \in G(L/K)}(x - s(a)) \in A[x]$, the roots of $\overline{P}$ in $\overline{L}$ are 0 if $s \notin D$, and $\overline{s(a)}$ if $s \in D$. This means that the conjugates of $\overline{a}$ are the $\overline{s(a)}$, for $s \in D$, i.e. D surjects onto $G(\overline{L}/\overline{K})$. □

Assume now that $\overline{L}/\overline{K}$ is separable (e.g. if $\overline{K}$ is finite).

Proposition 8.8. *Let K_T, K_D be the fixed fields of T, D. Then:*

(1) $\#T = [L : K_T] = e$
(2) $\#D/T = [K_T : K_D] = f$
(3) $[K_D : K] = g$
(4) $\overline{K_T} = \overline{L}$
(5) $\overline{K_D} = \overline{K}$

K_D/K is nontrivial only when you have ramification, and that only happens at finitely many primes so this is a phenomenon we can try to minimize.

Proof. Sum up the discussion above. □

Proposition 8.9. *Start with $K \subset E \subset L$, where L/K is Galois.*

(1) $D(L/E) = D(L/K) \cap G(L/E)$ *and* $T(L/E) = T(L/K) \cap G(L/E)$
(2) Assume E/K is Galois. Then the following diagram is commutative and all the sequences are exact:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & T(L/E) & \longrightarrow & T(L/E) & \longrightarrow & T(E/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & D(L/E) & \longrightarrow & D(L/K) & \longrightarrow & D(E/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G(\overline{L}/\overline{E}) & \longrightarrow & G(\overline{L}/\overline{K}) & \longrightarrow & G(\overline{E}/\overline{K}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Proof. This is supposed to be obvious. (E.g. for the first equality, $D(L/E)$ consists of the automorphisms of L leaving E invariant and also fixing the prime in question. For the diagram, the columns are exact, the last row is obviously exact, and that implies that the rest of the sequences are exact.) □

Now let's talk about the case where the residue fields are finite. Let L/K be Galois, $P \mid \mathfrak{p}$, where $\mathfrak{p}$ is unramified. Assume that $A/\mathfrak{p}$ is finite of cardinality q. Then $T = \{1\}$, and $D \cong G(\overline{L}/\overline{K})$ is cyclic, generated by Frobenius $x \mapsto x^q$. We get a unique element s_P of D such that for any $x \in B$, $s_P(x) \equiv x^q \pmod{P}$ (this is the element that maps to Frobenius). s_P is called the *Frobenius substitution*, and is denoted by $(P, L/K)$.

Frobenius depends on the extension, but in some sense it just depends on the base field, because it is $x \mapsto x^q$ where $q = |K|$. This is compatible with infinite field extensions – you still have a Frobenius element. It turns out that all the different Frobenius elements are dense in the Galois group (a profinite group).

Example 8.10. Let $d \equiv 3 \pmod 4$. Let $L = \mathbb{Q}(\sqrt{d})$ for square-free d, over $K = \mathbb{Q}$. Then $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ (you can work out the other case). Then $G(L/K) = G(\mathbb{Q}\sqrt{d}/\mathbb{Q}) = \{1, \sigma\}$ where $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.

Let $p \in \mathbb{Z}$; to make sure we are in the unramified case, require $p \nmid 2d$. Then $(a + b\sqrt{d})^p \equiv a^p + b^p(\sqrt{d})^p \equiv a + b \cdot d^{\frac{p-1}{2}}\sqrt{d} \pmod p$. Also, $d^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } d \text{ is a square mod } p \\ -1 & \text{otherwise.} \end{cases}$

So the Frobenius element is 1 if d is a square mod p, and σ otherwise.

Lecture 9: October 2

Recall, we had a finite, Galois extension L/K, an integrally closed ring $A \subset K$ with $\operatorname{Frac} A = K$, and the integral closure $B \subset L$ of A in L (finitely generated over A). Let $\mathfrak{p}$ be a prime in A, P a prime above $\mathfrak{p}$ in B.

Assume that P is unramified, and $A/\mathfrak{p}$ is finite of order q.

The decomposition group $D_P(L/K) = \{s \in G(L/K) : s(P) = P\}$ maps onto $G(\overline{L}/\overline{K})$. The Frobenius substitution is the unique element $s_P \in D_P$ mapping to Frobenius. It is characterized by $s_P(b) = b^q[P]$ for all $b \in B$. Denote $s_P =: (P, L/K)$. (You're supposed to be thinking of this as generalizing the quadratic residue symbol.)

Proposition 9.1. *If $t \in G(L/K)$ then*

$$(tP, L/K) = t(P, L/K)t^{-1}.$$

Proof. The RHS is in $tD_Pt^{-1} = D_{tP}$. Indeed, for $b \in B$, $s_Pt^{-1}(b) = t^{-1}(b)^q[P]$. Apply t:

$$ts_Pt^{-1}(b) = t(t^{-1}(b)^q)[tP] = b^q.$$

□

Now consider field extensions $K \subset E \subset L$. Write $B_E = B \cap E$ (the integral closure of A in E) and $P_E = P \cap E$. L/E was a Galois extension.

Proposition 9.2.

(1) $(P, L/E) = (P, L/K)^{[\overline{E}:\overline{K}]}$
(2) Assume E/K *is Galois; then* $(P_E, E/K)$ *is that* $(P, L/K)$ *in* $G(E/K)$.

PROOF. Check that the definition $s_P(b) = b^q[P]$ holds. □

Interesting case: Suppose L/K is abelian (i.e. $G(L/K)$ is abelian). Then $(P, L/K)$ only depends on $\mathfrak{p}$. We write

$$(P, L/K) = (\mathfrak{p}, L/K) = \left(\frac{L}{\mathfrak{p}}\right)$$

and call this the *Artin residue symbol*.

Extend by multiplicativity to get $\left(\frac{L}{I}\right)$ where I is an unramified ideal.

Remember that for $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$, this depends on whether d is a square mod p.

Example 9.3 (Cyclotomic fields)**.** Let $K = \mathbb{Q}$, $L = \mathbb{Q}[\zeta_n]$ where ζ_n is a primitive n^{th} root of unity.

First, I show that this is an abelian extension. Let $G = G(L/K)$. We have an injection $G \hookrightarrow (\mathbb{Z}/n)^\times$ sending $\sigma \mapsto x$ where $\sigma(\zeta_n) = \zeta_n^x$. Let p be prime to n (if not, there are problems corresponding to ramification). Then p does not ramify in L. Check that

$$\left(\frac{L}{p}\right) = [p] \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Corollary 9.4. *Cyclotomic polynomials are irreducible over* $\mathbb{Q}$*, i.e.* $G = (\mathbb{Z}/n\mathbb{Z})^\times$.

Application 9.5 (Quadratic reciprocity)**.** First, embed $\mathbb{Q}[\sqrt{d}]$ in $\mathbb{Q}[\zeta_n]$ using Gauss sums $\sum_r e^{\frac{2i\pi p}{r^2}}$ (their squares are either p^2 or ip^2, and I claim you can generate $\sqrt{d}$ this way). (Indeed, any abelian extension is contained in a cyclotomic extension; this is a deep theorem that will show up in the second half of the course.) Now, put together the statement in the previous lecture (about $d \pmod p$), and the statement we just made about cyclotomic extensions (about $p \pmod n$).

Theorem 9.6 (Artin reciprocity law)**.** *Let* L/K *be an abelian extension, where* K *is a number field. Let* $\mathfrak{p}_i$ *be the primes of* K *that ramify. Then there exist integers* n_i *such that if* $x \in A$ *satisfies*

(1) $v_{\mathfrak{p}_i}(x-1) \geq n_i$ *(e.g. in the* $\mathbb{Q}$ *case,* $x \equiv 1 \pmod p_i^{n_i}$*)*
(2) for any embedding $K \xhookrightarrow{i} \mathbb{R}$*,* $i(x) > 0$*. (Think of these as the "infinite primes".)*

Then $\left(\frac{L}{x}\right) = 1$*, and any* $\sigma \in G(L/K)$ *is of the form* $\left(\frac{L}{I}\right)$ *for some* I.

This is very much related to quadratic reciprocity. It is a consequence of class field theory.

Note about the comment about "infinite primes": ordinary primes are related to the completions of $\mathbb{Q}$, i.e. $\mathbb{Q}_p$, but $\mathbb{R}$ is also a completion of $\mathbb{Q}$.

9.1. Completion.

Intuition 9.7. In the picture of $\operatorname{Spec} B$ over $\operatorname{Spec} A$ for curves, taking the residue fields corresponds to *just* looking at $\mathfrak{p}$ on the bottom and the fiber above it. Instead of just looking at $\mathfrak{p}$, instead look at the preimage of a small disc around $\mathfrak{p}$ (this is a covering) – you get "little pieces of curves" so it says more about L/K than just taking points (residue fields) does. Idea: you are "zooming in on your curve".

I want to replace my algebraic functions by power series that have a fixed radius of convergence.

Let K be a field with a discrete valuation v. Let A be the valuation ring. Let $0 < a < 1$. Define, for $x \in K$, $\|x\| = a^{v(x)}$. (Recall "x is very close to 0 if its valuation is very large, i.e. it is very divisible by p".) Then $\| - \|$ is a *nonarchimedean* (or *ultrametric*) absolute value, i.e.

- $\|xy\| = \|x\|\|y\|$
- $\|x\| = 0 \iff x = 0$
- $\|x + y\| \leq \sup(\|x\|, \|y\|)$ (equality if $\|x\| \neq \|y\|$)

Theorem 9.8 (Ostrowski)**.** *These are the p-adic absolute values if $K = \mathbb{Q}$. For any K, the archimedean absolute values are of the form $x \mapsto |f(x)|^c$ with $f : K \hookrightarrow \mathbb{C}$ for $0 < c \leq 1$.*

Definition 9.9. Say that K is *complete* (w.r.t. v) if any Cauchy sequence has a limit in K.

Proposition 9.10. *There exists a unique completion $K \subset \widehat{K}$ (a complete field $\widehat{K}$ containing K as a dense subfield).*

Ignoring the field structure of $\widehat{K}$, this is a general topology fact: $\widehat{K}$ is the set of Cauchy sequences modulo those that converge to 0. Now we need to argue that $\widehat{K}$ is a field; you need to use the fact that the topology is compatible with the field structure of K.

v extends to a valuation $\widehat{v}$ on $\widehat{K}$ with integer values (this uses the last nonarchimedean axiom).

Let $\widehat{A}$ be the valuation ring of $\widehat{K}$; it is the closure of A in $\widehat{K}$.

Let π be a uniformizing parameter of v, i.e. $\pi \in A$, $v(\pi) = 1$.

Proposition 9.11.

$$\widehat{A} = \varprojlim_{n\to\infty} A/\pi^n A$$

where the limit is taken along the natural reduction maps $A/\pi^{n+1} \to A/\pi^n$.

Elements are compatible sequences of elements in $A/\pi^n A$; this is like how you define elements in $\mathbb{Q}_p$.

Proof. We have an isomorphism $A/\pi^n \xrightarrow{\cong} \widehat{A}/\pi^n$; this is because values of v do not change when you pass to $\widehat{v}$ (given an element of $\widehat{A}$, you can take an element of A/π^n that is very close). We get maps $\widehat{A} \to A/\pi^n$, and hence a map $\varphi : \widehat{A} \to \lim A/\pi^n$. This is surjective because $\widehat{A}$ is complete (an element in the limit corresponds to a Cauchy sequence, which has a limit). φ is also injective: $\ker\varphi = \bigcap_{n\geq 1} \pi^n \widehat{A}$. Any nonzero element in $\ker\varphi$ has valuation $\geq n$ for all n, so $\ker\varphi = 0$. □

Example 9.12. If $K = \mathbb{F}_q(T)$, and v is the valuation with respect to T, you can check that $\widehat{A} = \lim \mathbb{F}_q[T]/T^n = \mathbb{F}_q[[T]]$.

Proposition 9.13. *K is locally compact iff $\overline{K} = A/\pi A$ is finite,* and *K is complete.*

The $\pi^n A$'s form a basis of neighborhoods of 0 in K, and they are closed.

Proof. ($\implies$) If K is locally compact, then (using the fact that $\pi^n A$ form a basis of neighborhoods of 0), some $\pi^n A$ is compact. Divide by π^n to show that A is compact. $A/\pi A$ is compact (image of a compact set) and discrete (all the points are distance 1 apart). Therefore, it's finite. K is certainly complete (take a Cauchy sequence, scale it so it's in A, and use the fact that any Cauchy sequence that has a convergent subsequence is convergent).

($\impliedby$) $A = \varprojlim A/\pi^n A \subset \prod A/\pi^n A$, and products of compact spaces are compact. A is compact, so K is locally compact (because $\pi^n A$ form a basis of neighborhoods of 0). □

Remark 9.14. In that case, there is a natural absolute value obtained by taking $a = \frac{1}{\#\overline{K}} = \frac{1}{q}$, i.e. $\|x\| = q^{-v(x)}$.

Proposition 9.15. *Assume K is locally compact, and that μ is a Haar measure. Then if $x \in K$, and $E \subset K$ is measurable, then $\mu(xE) = \|x\|\mu(E)$.*

Example: to define a Haar measure on $\mathbb{Q}_p$, it suffices to define it on $\mathbb{Z}_p$; do this by defining $\mu(p^n\mathbb{Z}_p) = p^{-n}$.

Proof. Assume $x \neq 0$. Then $t \mapsto \mu(xE)$ is a Haar measure (measure that is compatible with the group structure). All Haar measures are proportional, so there exists $\chi = \chi(x)$ such that for all E, $\mu(xE) = \chi(x)\mu(E)$. We can assume $x \in A$ (and then do this for quotients,

etc.) Take $E = A$, and get $\chi(x)\mu(A) = \mu(xA)$. Since $xA \subset A$, A is a union of cosets of xA. How many cosets? $\mu(A) = \mu(xA) \cdot \underbrace{(xA : A)}_{\text{index?}} = \|x\|^{-1}\mu(xA)$ (exercise). □

Lecture 10: October 7

Lemma 10.1 (Hensel)**.** *Let A be a complete DVR, π the uniformizer, k the residue field. Let $F \in A[x]$; define $f := (F \pmod{\pi}) \in k[x]$. Let α be a simple root of f (i.e. $f(\alpha) = 0$ but $f'(\alpha) \neq 0$).*

Then some lift of α is a root: that is, there exists some $a \in A$ such that $F(a) = 0$ and $a \equiv \alpha \pmod{\pi}$.

Proof.

Claim 10.2. *There exists $a_n \in A$ such that $F(a_n) \equiv 0 \pmod{\pi^n}$, and $a_n \equiv \alpha \pmod{\pi}$. Also, $a_n \pmod{\pi^n}$ is uniquely determined.*

Proof of claim. Induction on n. For the base case ($n = 1$), let $a_1 \in A$ be any lift of α.

Inductive step: assume the claim for n, so we have a_n and we need a_{n+1}. Any possible a_{n+1} must be $\equiv a_n \pmod{\pi^n}$ so $a_{n+1} = a_n + \pi^n\varepsilon$ for some $\varepsilon \in A$. How do you estimate $F(a_n + \pi^n\varepsilon)$ if you know $F(a_n)$? Use calculus! There is a Taylor expansion

$$\begin{aligned} F(a_n + x) &= F(a_n) + F'(a_n)x + x^2 \overbrace{G(x)}^{\in A[x]} \\ F(a_n + \pi^n\varepsilon) &= F(a_n) + F'(a_n)\pi^n\varepsilon + (\pi^n\varepsilon)^2 G(\pi^n\varepsilon) \\ &\equiv F(a_n) + F'(a_n)\pi^n\varepsilon \pmod{\pi^{n+1}} \end{aligned}$$

This is $\equiv 0 \pmod{\pi^{n+1}}$ iff

$$\varepsilon = \frac{-F(a_n)/\pi^n}{F'(a_n)} \in A$$

and that can be accomplished because $F(a_n) \equiv 0 \pmod{\pi}^n$, and $F'(a_n) \equiv F'(a_1)$ and that is a unit. This choice of $\varepsilon \pmod{\pi}$ yields the unique $a_{n+1} \pmod{\pi^{n+1}}$. □

So we have a sequence of better and better approximations of a zero of F.

Existence: Since $a_{n+1} \equiv a_n \pmod{\pi^n}$ by uniqueness of $a_n \pmod{\pi^n}$, (a_n) is a Cauchy sequence (the differences are divisible by higher and higher powers of π). (Actually, you have to show that *any* difference starting above a certain a_n gets small; but because of non-archimedeanness, the absolute value of a sum of small things can't get very big. So it suffices to check consecutive differences.)

Since A is complete, there is a limit $a = \lim_{n\to\infty} a_n \in A$. Then $F(a) = \lim_{n\to\infty} F(a_n) = 0$, where $F(a_n)$ is divisible by π^n.

Uniqueness: If $\underline{a} \in A$ is such that $F(\underline{a}) = 0$, and $\underline{a} \equiv \alpha \pmod{\pi}$, then $\underline{a} \equiv a_n \pmod{\pi^n} \equiv a$ for all n (by uniqueness in the claim). So the difference $a - \underline{a}$ is divisible by an arbitrarily high power of π. This can only happen if $a = \underline{a}$. □

Example 10.3. Let $F(x) = x^2 - 6 \in \mathbb{Z}_5[x]$ reduces to $f(x) = x^2 - 1 \in \mathbb{F}_5[x]$. 1 is a simple root in $\mathbb{F}_5$; Hensel's lemma says that there exists $a \in \mathbb{Z}_5$ such that $a^2 - 6 \equiv 0 \pmod{5}$ and $a \equiv 1 \pmod{5}$.

That is, $\mathbb{Z}_5$ contains a $\sqrt{6}$; this means that there is a solution in every $\mathbb{Z}/5^n\mathbb{Z}$.

There is a generalization of Hensel's lemma, also called Hensel's lemma:

Lemma 10.4 (Hensel)**.** *Let A, π, k, F, f as before, and F is monic. If $f(x) = g(x)h(x)$, where g and h are coprime monic polynomials in $k[x]$ (this replaces the assumption that the root is simple), then $F(x) = G(x)H(x)$ for some monic polynomials $G, H \in A[x]$ that reduce to g, h.*

Proof. Homework. □

Any local ring satisfying this lifting property for coprime factorizations is called *henselian*.

Let L/K be a finite separable extension of degree n, and let B be the integral closure of A in L (where $\operatorname{Frac} A = K$). For a prime $\mathfrak{p} \subset A$, write $\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$.

Theorem 10.5. *If A is a complete DVR, then there is exactly one prime $\mathfrak{q}$ above $\mathfrak{p}$.*

Proof. *Existence of $\mathfrak{q}$:* We already proved that the number of $\mathfrak{q}$'s is between 1 and n (this is because $n = \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q}$).

Uniqueness of $\mathfrak{q}$: Suppose that there are ≥ 2 primes lying over $\mathfrak{p}$, say $\mathfrak{q}_1$ and $\mathfrak{q}_2$. They are both maximal, so you can choose $b \in \mathfrak{q}_1 \backslash \mathfrak{q}_2$. Then $\mathfrak{q}_1 \cap A[b]$ and $\mathfrak{q}_2 \cap A[b]$ are two different primes of $A[b]$ containing $\mathfrak{p}$. So $A[b]/\mathfrak{p}A[b]$ has at least two prime ideals.

Let $f(x)$ be the minimal polynomial of b over K. Then $f(x) \in A[x]$ and $A[b]/\mathfrak{p}A[b] \cong A[x]/(\mathfrak{p}, f(x)) \cong k[x]/(\overline{f}(x))$ (where $\overline{f}$ is the reduction mod $\mathfrak{p}$). We said that the last ring has two different primes, which means that $\overline{f}$ factors nontrivially (not just a power of an irreducible polynomial) into coprime $\overline{g}$, $\overline{h}$. By generalized Hensel's lemma, you can lift that factorization so that $f(x)$ factors nontrivially in $A[x]$. But this contradicts the fact that f was a minimal polynomial. □

Definition 10.6. If V is a K-vector space (where K is a field with an absolute value), a *norm* on V is a function $\| \ \| : V \to \mathbb{R}_{\geq 0}$ satisfying:

(1) $\|x\| = 0 \iff x = 0$
(2) (triangle inequality) $\|x + y\| \leq \|x\| + \|y\|$ for all $x, y \in V$

(3) $\|\lambda x\| = |\lambda| \cdot \|x\|$ (where $\lambda \in K, x \in V$)

Example 10.7 (sup norm)**.** Let $V = K^n$; define $\|(a_1, \ldots, a_n)\| = \max(|a_1|, \ldots, |a_n|)$.

Definition 10.8. Say two norms $\| \ \|_1$ and $\| \ \|_2$ are equivalent if there exist $c, d \in \mathbb{R}_{>0}$ such that $\|x\|_1 \leq c \cdot \|x\|_2$ and $\|x\|_2 \leq d \cdot \|x\|_1$.

If you make V into a metric space using each of these norms, they define the same topology.

Theorem 10.9. *If K is complete, and V is finite-dimensional, then any two norms on V are equivalent.*

Proof. Omitted. □

Now we can give another proof of Theorem 10.5. Each $\mathfrak{q}$ above $\mathfrak{p}$ defines a norm, and that satisfies the absolute value $\| \ \|_\mathfrak{q}$ on L (thought of as a K-vector space). $x \in$ valuation ring of $\mathfrak{q} \iff \|x\|_\mathfrak{q} \leq 1 \iff x^{-1}, x^{-2}, x^{-3}, \ldots$ does not converge in the topology defined by $\| \ \|_\mathfrak{q}$. By Theorem 10.9, these topologies are all the same. So the valuation rings are all the same – that is, $\mathfrak{q}$ is unique.

Corollary 10.10 (Corollary of Theorem 10.5)**.** *If L, K, A, B are as above, with A a complete DVR, then B is a DVR, and B is a free A-module of rank n. There is a unique discrete valuation w extending $v = v_\mathfrak{p}$ (with index e).*

Proof. Second statement: structure theorem of finitely generated modules over a PID. □

The formula $\sum e_\mathfrak{q} f_\mathfrak{q} = n$ becomes, in this case, $ef = n$ (since there is only one $\mathfrak{q}$).

Corollary 10.11. *L is complete w.r.t. w.*

Proof. $\| \ \|_\mathfrak{q} \sim$ the sup norm on $L \equiv K^n$. □

Corollary 10.12. *If $x, y \in L$ are conjugate over K (i.e. there exists $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(x) = y$) then $w(x) = w(y)$.*

Proof. Otherwise, w and $w \circ \sigma$ would be two valuations extending v ($w \circ \sigma$ extends v because σ acts trivially on K). □

Corollary 10.13. *$w(x) = \frac{1}{f} v(N_{L/K}(x))$ for all $x \in L$.*

Recall that, if $\mathfrak{q} \mid \mathfrak{p}$, then $N(\mathfrak{q}) = \mathfrak{p}^f$, and the ideal norm is compatible with the element norm.

This normalization is chosen so that w takes values in $\mathbb{Z} \cup \{\infty\}$, but there are other normalizations: e.g. $\frac{1}{e}w$ restricts to v.

Theorem 10.5 and its corollaries *above here* work for inseparable fields too (but we will not discuss this) – you just have to analyze the degree-p pieces of a purely inseparable field extension.

Corollary 10.14. *$v : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ is the restriction of a valuation $\overline{K} \twoheadrightarrow \mathbb{Q} \cup \{\infty\}$.*

If π is a uniformizer of K, then $\pi^{1/e} \in \overline{K}$ has valuation $\frac{1}{e}$. By taking powers, you can get any multiple of $\frac{1}{e}$.

We've really only talked about valuations that take values in $\mathbb{Z} \cup \{\infty\}$, but all you need is an abelian group where you can talk about min. The ordered abelian group that the valuation surjects onto is called the *value group*.

For example, the valuation on $\mathbb{Q}_p$ extends to $\overline{\mathbb{Q}}_p$. But this isn't complete, so you want to complete again. This field $\widehat{\overline{\mathbb{Q}}}$ is called $\mathbb{C}_p$; thankfully, it is also algebraically closed. (This is the p-adic analogue of $\mathbb{C}$.) These all have the same cardinality as $\mathbb{R}$, but the extensions have infinite transcendence degrees.

Warning 10.15. Each finite extension of K is complete, but infinite extensions of K, like $\overline{K}$, are not.

Field	Value group	Residue field
$\mathbb{C}_p$	$\mathbb{Q}$	$\overline{\mathbb{F}}_p$
$\overline{\mathbb{Q}}_p$	$\mathbb{Q}$	$\overline{\mathbb{F}}_p$
$\mathbb{Q}_p$	$\mathbb{Z}$	$\mathbb{F}_p$

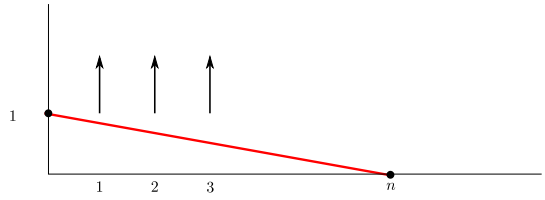
Why are the value groups the same when you take the completion? If you have a convergent sequence $(a_n) \to a$ (in a nonarchimedean context) then $|a| = |a_n|$ for all sufficiently large n. (This is because $|a_n + \varepsilon| = |a_n|$ ("bigger term wins").) Similarly, the difference will eventually be so small that it reduces to zero, so you get the same residues.

Weird fact 10.16. $\mathbb{C}_p$ is abstractly isomorphic to $\mathbb{C}$: they're both extensions of $\mathbb{Q}$ with transcendence basis of the same cardinality (you need the axiom of choice to do this). This actually has uses...

Newton polygons. Let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation. (This need not be a surjection.) Let $f(x) = a_n x^n + \cdots + a_0 \in K[x]$.

Definition 10.17. The *Newton polygon* $NP(f)$ is the lower convex hull of $\{(i, v(a_i))\}_{0 \le i \le n}$ in $\mathbb{R}^2$.

Example 10.18. An Eisenstein polynomial is $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $v_p(a_0) = 1$ and $v_p(a_i) \ge 1$ for $i < n$.



Lecture 11: October 9

Let K be a field, and $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation.

Definition 11.1. If $S \subset \mathbb{R}^2$, the lower convex hull of S is the boundary of the intersection of all regions $y \ge mx + b$ containing S.

Theorem 11.2. *Let K be an algebraically closed field. Let $v : K \to \mathbb{R} \cup \{\infty\}$ be a nonarchimedean* valuation, and let $f \in K[x]$. For each $s \in \mathbb{R}$,

$$\text{width}\begin{pmatrix}\text{slope } s \text{ segment}\\ \text{of } NP(f)\end{pmatrix} = \#\left\{\begin{array}{c}\text{zeros of } f \text{ having valuation } -s\\ \text{(with multiplicity)}\end{array}\right\}$$

(here width means horizontal displacement).

Notice that if you add up all the segments, they have total width $= \deg f$.

In the Eisenstein polynomial example, there is one segment of slope $-\frac{1}{n}$, which has width n. Therefore, $f(x)$ has n zeros of valuation $\frac{1}{n}$ (and this accounts for all the zeros).

Proof. If $v(\alpha) = c$, then changing $f(x)$ to $f(\alpha x)$

- multiplies zeros by $\frac{1}{\alpha}$ (hence subtracts c from their valuations), and
- multiplies the coefficient a_i of x^i by α^i, hence adds ic to the valuation; this applies the shear transformation $(x, y) \mapsto (x, y + cx)$ to the Newton polygon, hence adds c to the slopes.

We have just proved that if the theorem is true for $f(x)$, it is true for $f(\alpha x)$. By doing this adjustment, we can assume that $s = 0$. Then f looks like

$$f(x) = \text{const} \cdot (x - r_1)(x - r_2) \dots (x - r_a)(x - u_1) \dots (x - u_b)\left(1 - \frac{x}{R_1}\right) \dots \left(1 - \frac{x}{R_c}\right)$$

where the r_i's are roots of positive valuation, the R_i's are roots of negative valuation, and u_i's are zeros of valuation zero. Multiplying f by a constant just shifts the Newton polygon up or down (and doesn't change the roots), so without loss of generality we can assume that the constant is 1.

Let $\overline{f}$ be $f \pmod{\mathfrak{m}}$: this changes every $(x - r_i)$ term to just x, and every $1 - \frac{x}{R_i}$ to just 1, so $\overline{f}(x) = x^a(x - \overline{u}_1)\dots(x - \overline{u}_b) = x^a + \dots + (\text{unit}) \cdot x^{a+b}$.

So in the Newton polygon (for f, not just $\overline{f}$), we have zeros at $(a, 0)$ and $(a + b, 0)$ (and so there is a segment of slope zero from $(a, 0)$ to $(a + b, 0)$); because the reduction outside $[a, a + b]$ is zero for $\overline{f}$, we know that these terms in f have positive valuation. So the width of the slope zero segment is *exactly* b. And indeed, there were b zeros $u_1, \dots, u_b$ of valuation zero. □

11.1. p-adic analysis. Let K be complete w.r.t. a nonarchimedean absolute value $|\ |$. Let $a_0, a_1 \dots \in K$. Then:

Proposition 11.3.

(1) $\sum a_n$ *converges* $\iff a_n \to 0$
(2) Series can be rearranged without affecting the sum
(3) Given $\sum a_n x^n \in K[[x]]$*, the radius of convergence is*

$$R := \frac{1}{\limsup_{n\to\infty} |a_n|^{1/n}} \in \mathbb{R}_{\geq 0} \cup \{\infty\}.$$

This has the usual meaning: if $|x| < R$ *then* $f(x)$ *converges; if* $|x| > R$ *then* $f(x)$ *diverges; if* $|x| = R$ *then you don't know (but if it converges somewhere on the circle, it converges everywhere, because it only depends on* $|a_n|$*).*
(4) f *and* f' *have the same radius of convergence*

Example 11.4. Define $\exp(x) := \sum_{n\geq 0} \frac{x^n}{n!} \in \mathbb{Q}_p[[x]]$.

$v_p(n!) = \frac{n - S_n}{p-1}$ where S_n is the sum of the digits of n, written in base p. Then the radius of convergence is

$$\begin{aligned} R &= \frac{1}{\limsup_{n\to\infty} |\frac{1}{n!}|^{1/n}} = \lim_{n\to\infty} \left|\frac{1}{n!}\right|^{-1/n} \\ &= \lim_{n\to\infty} \left(p^{-v_p(\frac{1}{n!})}\right)^{-1/n} = \lim_{n\to\infty} \left(p^{v_p(n!)}\right)^{-1/n} \\ &\overset{(*)}{=} \lim_{n\to\infty} \left(p^{n/(p-1)}\right)^{-1/n} = p^{-1/(p-1)} < 1 \end{aligned}$$

where (*) is using the fact that S_n grows logarithmically.

The Newton polygon theorem applies also to power series over a complete algebraically closed field with valuation; it computes the valuations of zeros inside the disk of convergence – it only works on s such that $-s$ corresponds to valuations of things inside the disk of convergence.

Example 11.5. Look at $\exp(x) \in \overline{\mathbb{C}}_p[[x]]$. We're computing $(n, v_p\left(\frac{1}{n!}\right))$. It's 0 until you get to p, at which point it's -1 until you get to $2p$, etc. When you hit p^2 it goes down by 2 instead of by 1.

The Newton polygon has just one segment, of slope $-\frac{1}{p-1}$; this corresponds to looking at zeros of valuation $\frac{1}{p-1}$. But that's not allowed – this is on the boundary of the disk of convergence, and you're not allowed to apply the theorem to those. So we conclude that $\exp(x)$ has no zeros inside the disk of convergence ($|x| < p^{-1/(p-1)}$).

Reference: Koblitz, p-adic Numbers, p-adic Analysis, and Zeta Functions.

Proposition 11.6. *There is a unique homomorphism* $\log : \mathbb{C}_p^\times \to \mathbb{C}_p$ *(where* $\mathbb{C}_p^\times$ *is thought of as a group under multiplication and* $\mathbb{C}_p$ *is a group under addition) such that*

(1) if $|x| < 1$*, then*

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

(this is only enough to specify the log on things of valuation > 0*)*
(2) $\log p = 0$ *(this is an arbitrary choice).*

The radius of convergence is 1.

This is called the Iwasawa p-adic logarithm.

Some people write $\log_p$ instead for this; but it does not mean log base p.

Proof. Let $\mathfrak{m} = \{x \in \mathbb{C}_p : |x| < 1\}$. For $x \in \mathfrak{m}$, use (1) as a definition of $\log(1+x)$. To check it's a homomorphism, we need

$$\log(1+x) + \log(1+y) = \log(1 + (x + y + xy))$$

This holds as an identity of real analytic functions for small x, y. I claim that it also holds on the level of formal power series (i.e. in $\mathbb{R}[[x,y]]$): the difference is a power series that is zero in a neighborhood, hence identically zero. All the coefficients are in $\mathbb{Q}$, so this is true in $\mathbb{Q}[[x,y]]$, and is also true in $\mathbb{C}_p[[x,y]]$ (it's still the same power series). As long as everything converges, you're allowed to rearrange terms. So this holds when you plug in any $x, y \in \mathbb{C}_p$ such that everything converges, i.e. whenever $x, y \in \mathfrak{m}$.

Now extend to $\log : G := p^{\mathbb{Z}}(1+\mathfrak{m}) \to \mathbb{C}_p$ by defining $\log(p^n(1+x)) = \log(1+x)$ (the only choice that makes it a homomorphism).

Now I will show that you can define it everywhere, by showing that everything in $\mathbb{C}_p^\times$ has a power that lands in G. So if $x^n \in G$, then define $\log(x) = \frac{\log(x^n)}{n}$.

Lemma 11.7. $\mathbb{C}_p^\times/G$ *is torsion.*

Proof. There is a well-defined valuation $\mathbb{C}_p^\times/G \to \mathbb{Q}/\mathbb{Z}$. There is an isomorphism $\mathcal{O}_{\mathbb{C}_p}^\times/(1+\mathfrak{m}) \xrightarrow{\cong} \overline{\mathbb{F}}_p^\times$. $\mathbb{Q}/\mathbb{Z}$ is torsion, and so is $\overline{\mathbb{F}}_p^\times$. Then $\mathbb{C}_p^\times/G$ fits in a torsion sandwich

$$\overline{\mathbb{F}}_p^\times \cong \mathcal{O}_{\mathbb{C}_p}^\times/(1+\mathfrak{m}) \to \mathbb{C}_p^\times/G \to \mathbb{Q}/\mathbb{Z}.$$

□

Lemma 11.8. *Suppose G'/G is torsion, and suppose we are given*

$$\begin{array}{ccc} G' & \overset{\psi}{\dashrightarrow} & V \\ \uparrow & \nearrow_{\varphi} & \\ G & & \end{array}$$

where $G \hookrightarrow G'$ is a homomorphism of abelian groups and V is a $\mathbb{Q}$ vector space. Then there is a unique dotted extension ψ.

Proof. If $g' \in G'$ choose $n \geq 1$ such that $ng' \in G$ and define $\psi(g') = \frac{1}{n}\varphi(ng') \in V$. (Check it's well-defined, etc.) □

To finish the proof of Proposition 11.6, apply this to

$$\begin{array}{ccc} \mathbb{C}_p^\times & \overset{\log}{\dashrightarrow} & \mathbb{C}_p \\ \uparrow & \nearrow & \\ G & & \end{array}$$

□

Lecture 12: October 14

Example 12.1.

$$\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \mathbb{Q}[x]/(x^2+1) \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \mathbb{Q}_5[x]/(x^2+1)$$

Question: is this a field? (i.e. is x^2+1 irreducible?) It factors mod 5 as $x^2+1 \equiv (x+2)(x-2)$, so by Hensel's lemma these roots can be lifted to $\mathbb{Q}_5$. So $\mathbb{Q}_5[x]/(x^2+1) \cong \mathbb{Q}_5 \times \mathbb{Q}_5$. This matches the way 5 splits in $\mathbb{Q}(i)$.

If we try this with $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}_7 \cong \mathbb{Q}_7[x]/(x^2+1)$, we have that x^2+1 is irreducible over $\mathbb{F}_7$ so $\mathbb{Q}_7[x]/(x^2+1)$ is a field (more precisely, you need the converse – if x^2+1 had a root in $\mathbb{Q}_7$ then you could reduce it to get a root over $\mathbb{F}_7$).

Now do this for $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}_2 \cong \mathbb{Q}_2[x]/(x^2+1)$; recall that x^2+1 has a double root over $\mathbb{F}_2$. Do a change of variables $x = t+1$ (which doesn't change irreducibility) to get $\mathbb{Q}_2[t]/(t^2+2t+2)$. That polynomial is Eisenstein, hence irreducible, and this is totally ramified as a field extension over $\mathbb{Q}_2$. This reflects the fact that $(2) = (1+i)^2$.

Theorem 12.2. *L/K is a finite separable extension of degree n, A is a Dedekind domain such that* Frac $A = K$*, and B is integral over A. Fix a prime $\mathfrak{p} \subset A$; we saw that the valuation $v := v_{\mathfrak{p}}$ splits into a bunch of valuations of B arising from the splitting of $\mathfrak{p}B$. Let $\widehat{K}$ be the completion of K at v, and $\widehat{L}_i$ be the completion of L at w_i. Then:*

(1) $\widehat{L}_i$ is a field extension of $\widehat{K}$.
(2) The induced valuation $\widehat{w}_i$ on $\widehat{L}_i$ is the unique valuation extending $\widehat{v}$ on K.

(3) $e(\widehat{w}_i/\widehat{v}) = e_i := e(w_i/v)$ *(i.e. the ramification doesn't change when you complete)*
$f(\widehat{w}_i/\widehat{v}) = f_i := f(w_i/v)$
(4) $[\widehat{L}_i : \widehat{K}] = e_i f_i$
(5) $L \otimes_K \widehat{K} \xrightarrow{\varphi} \prod \widehat{L}_i$ *is an isomorphism.*

PROOF. (1) The completion of a field is a field (same proof that $\mathbb{R}$ is a field). The inclusion $K \hookrightarrow L$ induces a homomorphism $\widehat{K} \to \widehat{L}_i$, and field homomorphisms are always injective.

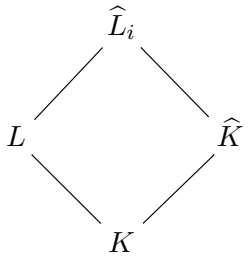
(2) Fact about complete DVR's: you only have one prime over a given prime. Since $\widehat{K}$ is complete, there can be only one other extension of $\widehat{v}$ to $\widehat{L}_i$.

(3) $(\widehat{K}, \widehat{v})$ has the same value group as (K, v). (If $a_i \in K$ converge to nonzero $a \in \widehat{K}$, then $\widehat{v}(a) = v(a_i)$ for sufficiently large i, because of the nonarchimedean triangle inequality – use the triangle between $0, a$, and a_i; the segment between a and a_i is really small, so it just loses.)

You can make the same argument for residue fields – if $a - a_i \in \mathfrak{m}$ then they have the same image in the residue field. More formally: if $a_i \in K$ is a Cauchy sequence representing $a \in \widehat{K}$ and $\widehat{v}(a) \geq 0$, then $v(a_i) \geq 0$ for large i, and $a_i - a \in \mathfrak{m}$ (the maximal ideal of "$\widehat{K}$") for large enough i, so a_i has the same image in the residue field.

(4) There is only one prime, since it's complete. So $[\widehat{L}_i : \widehat{K}] = e(\widehat{L}_i/\widehat{K}) f(\widehat{L}_i/\widehat{K})$; by (3) this is $e_i f_i$.

(5) You have a diamond of fields



which gives rise to a homomorphism $L \otimes_K \widehat{K} \xrightarrow{\varphi_i} \widehat{L}_i$ via $\ell \otimes x \mapsto \ell x$. Let $\varphi = \prod \varphi_i : L \otimes_K \otimes \widehat{K} \to \prod \widehat{L}_i$.

Choose a $\widehat{K}$-basis $\alpha_1, \ldots, \alpha_n$ of $\prod \widehat{L}_i$ (this n is $\sum e_i f_i$ by (4)). Use strong approximation for nonarchimedean valuations to find $\ell \in L$ close to α_i. ($\prod \widehat{L}_i$ has the product topology; being close to an element is the same as being close in each coordinate. So you approximate elements of each $\widehat{L}_i$ by elements of L_i, and approximate all of those by an element of L. This is what the strong approximation theorem does.)

If there's an earthquake, and the basis vectors move a little, then it's still a basis; check this by looking at the change-of-basis matrix (and noting that the determinant is continuous).

Similarly, the matrix in $M_n(\widehat{K})$ expressing the ℓ_i in terms of the α_i so the determinant is close to 1 in $\widehat{K}$, hence not 0.

Thus $\ell_1, \dots, \ell_n$ is another $\widehat{K}$-basis of $\prod \widehat{L}_i$. Thus $L \otimes_K \widehat{K} \xrightarrow{\varphi} \prod \widehat{L}_i$ is surjective.

Both have dimension n as $\widehat{K}$-vector spaces, so φ is injective too. □

Corollary 12.3. *If in addition L/K is Galois, then $\widehat{L}_i/\widehat{K}$ is Galois with Galois group D_i (elements of $G(L/K)$ fixing the prime corresponding to L_i).*

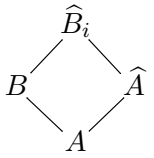
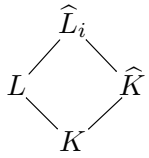
Proof. Each $\sigma \in D_i$ acts on L respecting w_i (i.e. $w_i \circ \sigma = w_i$). So it also respects the process of taking the completion. You get an induced action on the completion $\widehat{L}_i$. That is, you get a homomorphism $D_i \to \mathrm{Aut}(\widehat{L}_i/\widehat{K})$ (I'm writing Aut instead of Gal because I don't yet know it's a Galois extension).

Injective: If $\sigma \in D_i$ acts as the identity on $\widehat{L}_i$ then $\sigma|_L$ is the identity (since $L \subset \widehat{L}_i$). So $\sigma = 1$. (I'm identifying σ with its extension.)

Surjectivity: It suffices to show the groups have the same size. Since it's injective, $\#D_i \leq \#\,\mathrm{Aut}(\widehat{L}_i/\widehat{K})$; for any field extension, this is $\leq [\widehat{L}_i : \widehat{K}]$. So we have

$$e_i f_i = \#D_i \leq \#\,\mathrm{Aut}(\widehat{L}_i/\widehat{K}) \leq [\widehat{L}_i : \widehat{K}] = e_i f_i$$

so equality holds in the middle. □

Let B_i be the value ring of w_i on L (this is B localized at $\mathfrak{q}_i$), and let $\widehat{B}_i$ be the completion of B_i. This is the ring version  of the previous diamond of fields: 

Corollary 12.4. $B \otimes_A \widehat{A} \cong \prod \widehat{B}_i$

Proof. A is a DVR, B is a free A-module of rank n (if you tensor with K you get L^n), $B \otimes_A \widehat{A}$ is a free $\widehat{A}$-module of rank n, and $\prod \widehat{B}_i$ is a free $\widehat{A}$-module of rank $\sum e_i f_i = n$.

If you have two modules contained in the same $\widehat{K}$-vector space, to check they're the same it suffices to check they're the same after reducing mod $\widehat{\mathfrak{p}}$; that is, we want to check that $B \otimes \widehat{A} \to \prod \widehat{B}_i$ is an isomorphism of $\widehat{A}$-modules after reducing mod $\widehat{\mathfrak{p}}$.

On the LHS: $\widehat{A}/\widehat{\mathfrak{p}} = A/\mathfrak{p}$, so $B \otimes \widehat{A}/\widehat{\mathfrak{p}} = B \otimes A/\mathfrak{p} = B/\mathfrak{p}B$; on the RHS, $\prod \widehat{B}_i/\widehat{\mathfrak{p}}\widehat{B}_i = \prod \widehat{B}_i/\mathfrak{p}\widehat{B}_i = \prod B_i/\mathfrak{p}B_i$; normally $\mathfrak{p}$ would split, but since I localized at $\mathfrak{q}_i$, this is just $\prod B_i/\mathfrak{q}_i^{e_i}B_i$. This is isomorphic to the LHS $= B/\mathfrak{p}B$ since $\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$. □

The different. Let L, K, A, B be as above; let n be the degree of L/K. Recall there is a pairing $L \times L \to K$ sending $(x, y) \mapsto \mathrm{Tr}(xy)$. Since our extension is separable, this is a perfect pairing. For a finitely generated A-module $M \subset L$, define the dual module

$$M^* := \{\ell \in L \,:\, \mathrm{Tr}(\ell m) \in A \ \forall m \in M\}.$$

If M is a free lattice with basis $e_1, \ldots, e_n$, then M^* is a free lattice with the dual basis. If M is a B-module, so is M^* (proof: if $x \in M^*$, $b \in B$, and $m \in M$ then $\mathrm{Tr}(bx \cdot m) = \mathrm{Tr}(x \cdot \underbrace{bm}_{\in M}) \in A$ since $x \in M^*$).

If $M \in \mathcal{I}_B$ (this is the group of fractional ideals), then so is M^*. (Proof: M contains a free A-module F of rank n, so $M^* \subset F^*$, which is free of rank n, so M^* is finitely generated.)

Definition 12.5. $B^* = \{\ell \in L \,:\, \mathrm{Tr}(\ell b) \in A \ \forall b \in B\}$ is called the *inverse different* (of the extension). We just showed that it is a fractional ideal.

$(B^*)^{-1}$ is called the *different* of the extension.

Sometimes people write $\mathscr{D}_{B/A} = (B^*)^{-1}$. If A is obvious from context (e.g. $\mathbb{Z}$), write $\mathscr{D}_{L/K}$ instead.

I claim that $B^* \supset B$. I just have to check that elements of b satisfy the condition on B^*; this is because $\mathrm{Tr}(\ell b) \in A$ (the trace is a sum of conjugates, which are integral, so it lands in A).

If you take inverses, the inclusions are reversed: $\mathscr{D}_{B/A} \subset B$ (recall B, the unit ideal, is its own inverse). So $\mathscr{D}_{B/A}$ is an ideal of B.

$\mathscr{D}_{B/A}$ respects localization: the different of the localized extension of rings is the part of $\mathscr{D}_{B/A}$ involving the prime.

$\mathscr{D}_{B/A}$ also respects completion: if $\mathfrak{q}$ lies over $\mathfrak{p}$, then $\mathscr{D}_{\widehat{B}_\mathfrak{q}/\widehat{A}_\mathfrak{p}} = \mathscr{D}_{B/A} \cdot \widehat{B}_\mathfrak{q}$. Proof: without loss of generality assume A is a DVR (just localize). Let $\widehat{L} := L \otimes K\widehat{K} \cong \prod \widehat{L}_\mathfrak{q}$ (this is not a field). The ring version of this is $\widehat{B} = B \otimes_A \widehat{A} \cong \prod \widehat{B}_\mathfrak{q}$. Even though $\widehat{L}$ is not a field, it still has a trace pairing, and you can define $\widehat{B}^* = \prod \widehat{B}^*_\mathfrak{q}$ (the trace form breaks up as a sum of all the trace forms, etc., so you can compute everything one prime at a time). This equals $B^* \otimes_A \widehat{A}$. In other words, B^* generates the fractional ideal $\widehat{B}^*_\mathfrak{q} \in \mathcal{I}_{\widehat{B}_\mathfrak{q}}$. Now just take inverses of these fractional ideals: $\mathscr{D}_{B/A}$ generates $\mathscr{D}_{\widehat{B}_\mathfrak{q}/\widehat{A}_\mathfrak{p}}$.

Lecture 13: October 16

Let L/K be a finite separable extension, $A \subset K$ a Dedekind domain with $\mathrm{Frac}\, A = K$, and $B =$ the integral closure of A in L.

If A is a DVR, then B is free over A.

Recall we defined the *different* as

$$\mathscr{D}_{B/A} := (B^*)^{-1} \in \mathcal{I}_B.$$

We also had the trace map $\mathrm{Tr} : L \to K$.

Definition 13.1. Let $e_1, \ldots, e_n \in L$. Then define

$$\mathrm{disc}(e_1, \ldots, e_n) := \det \mathrm{Tr}(e_i e_j)_{1 \le i,j \le n} \in K.$$

(If all the e_i are in B, then $\mathrm{disc}(e_1, \ldots, e_n) \in A$ (it's a sum of conjugates).)

Proposition 13.2. *Let $\Omega \supset K$ be a field such that there are n distinct K-homomorphisms $\sigma_1, \ldots, \sigma_n : L \to \Omega$. ($L$ is generated by one element so Ω is big enough to be a splitting field.) Then:*

$$\mathrm{disc}(e_1, \ldots, e_n) = \left(\det \sigma_i(e_j)_{1 \le i,j \le n}\right)^2.$$

Proof.

$$\begin{aligned}(\mathrm{Tr}(e_i e_j)) &= \left(\sum_{h=1}^{n} \sigma_h(e_i e_j)\right) \\ &= \left(\sigma_h(e_i)_{i,h}\right)\left(\sigma_h(e_j)_{h,j}\right) \\ &= \left(\sigma_h(e_i)_{i,h}\right)\left(\sigma_h(e_i)_{i,h}\right)^T\end{aligned}$$

Take determinants; a matrix and its transpose have the same determinant. □

Proposition 13.3. $\mathrm{disc}(1, x, x^2, \ldots, x^{n-1}) = \left(\det \sigma_i(x)^j{}_{\substack{1 \le i \le n \\ 0 \le j \le n-1}}\right)^2 = \prod_{i<j} (\sigma_i x - \sigma_j x)^2$

(It's a Vandermonde matrix.)

Definition 13.4. If $f = \prod_{i=1}^{n} (X - \alpha_i)$, then define

$$\mathrm{Disc}(f) := \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Example 13.5.

$$\begin{aligned}\mathrm{Disc}(x^2 + bx + c) &= b^2 - 4c \\ \mathrm{Disc}(x^3 + Ax + B) &= -4A^3 - 27B^2\end{aligned}$$

If f is monic and separable of degree n in $A[x]$ and α is the image of x in $A[x]/(f(x))$, then

$$\mathrm{Disc}\, f = \mathrm{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}). \tag{13.1}$$

Let M be an A-lattice (i.e. a finitely generated A module such that $KM = L$) in L. Suppose $e_1, \ldots, e_n$ and $e'_1, \ldots, e'_n$ are two A-bases for $M \subset L$, then

$$\mathrm{disc}(e'_1, \ldots, e'_n) = (\det Q)^2 \,\mathrm{disc}(e_1, \ldots, e_n)$$

where Q is the change of basis matrix. (Why squared? look at Proposition 13.2.) In particular, $\det Q$ is a unit in A.

Definition 13.6. In the case that $A = \mathbb{Z}$, define $\operatorname{disc} M := \operatorname{disc}(e_1, \dots, e_n) \in \mathbb{Z}$ for any $\mathbb{Z}$-basis $e_1, \dots, e_n$ of M.

In the general case where M is free over A with basis $e_1, \dots, e_n$, define

$$D(M) := \text{fractional ideal generated by } \operatorname{disc}(e_1, \dots, e_n) \in \mathcal{I}_A.$$

For any A, M (not necessarily free), define

$$D(M) := \text{ the } A\text{-module generated by } \operatorname{disc}(e_1, \dots, e_n) \text{ for all } e_1, \dots, e_n \in M.$$

Why is $D(M)$ finitely generated in the most general case? For any free A-lattice N in L, there exists nonzero $a \in A$ such that $M \subset a^{-1}N$. Then $D(M) \subset D(a^{-1}N)$. Since $a^{-1}N$ is free, $D(a^{-1}N)$ is finitely generated, and since we're working over a Noetherian ring, so is $D(M)$.

All of this stuff behaves well w.r.t. localization: if you want to know the exponent of $\mathfrak{p}$ in $D(M)$, then look at $D(M_{\mathfrak{p}})$.

Definition 13.7. The *discriminant ideal* $D_{B/A}$ is defined to be $D(B)$ (where B is thought of as an A-lattice). This is an ideal of A.

Example 13.8. What is the discriminant of $\mathbb{Q}(i)$ (over $\mathbb{Q}$)? (We're implicitly choosing $A = \mathbb{Z}$ and $B = \mathbb{Z}[i]$.)

Solution 1: use the definition.

$$\operatorname{disc}(1, i) = \det \begin{pmatrix} \operatorname{Tr}(1 \cdot 1) & \operatorname{Tr}(i \cdot 1) \\ \operatorname{Tr}(1 \cdot i) & \operatorname{Tr}(i \cdot i) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = -4$$

Solution 2: use Proposition 13.2. Two embeddings of our basis $(1, i)$ are $(1, i)$ and $(1, -i)$.

$$\left(\det \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \right)^2 = (-2i)^2 = -4.$$

Solution 3: use (13.1). Since $B = \mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 + 1)$,

$$\operatorname{disc} = \operatorname{Disc}(x^2 + 1) = -4$$

(using Example 13.5).

We will prove that the only primes that ramify are the ones that divide the discriminant.

Theorem 13.9.

$$D_{B/A} = N_{L/K} \mathscr{D}_{B/A}$$

(where $N_{L/K}$ is the ideal norm (Definition 7.4)).

PROOF. Localize to assume that A is a DVR. So B is free, say with basis $e_1, \ldots, e_n$. Then B^* is free, with basis $e_1', \ldots, e_n'$. $\mathrm{Tr}(m_i e_j)$ is the matrix ending $e_1', \ldots, e_n'$ to $m_1, \ldots, m_n$ (notice that if $m_i = e_i'$ for all i, then this would just be the identity matrix). Now take $m_i = e_i$: $\mathrm{Tr}(e_i e_j)$ is the matrix ending (e_i') to (e_i). Take the determinant: $D_{B/A} = (B^* : B)$.

If I is a nonzero ideal, then $\frac{I^{-1}}{B} \cong \frac{B}{I}$ as B-modules. In our case,

$$\begin{aligned} D_{B/A} &= (B^* : B) \\ &= (B : (B^*)^{-1}) \\ &= (B : \mathscr{D}_{B/A}) \\ &= N_{L/K} \mathscr{D}_{B/A} \end{aligned}$$

by definition of ideal norm. □

Theorem 13.10. *A, B, L, K as always. The extension L/K is unramified at $\mathfrak{q}$ iff $\mathfrak{q} \nmid \mathscr{D}_{B/A}$.*

PROOF. Without loss of generality assume A is a DVR with maximal ideal $\mathfrak{p}$. We can also assume that A is complete (so there is only one prime $\mathfrak{q}$ above $\mathfrak{p}$). This implies that B is a complete DVR, and $\mathfrak{p}B = \mathfrak{q}^e$. B is automatically free; so we can choose an A-basis $b_1, \ldots, b_n$; let $\overline{b}_1, \ldots, \overline{b}_n$ be the reductions in $B/\mathfrak{p}B$. We know that $\mathscr{D}_{B/A}$ looks like $\mathfrak{q}^m$ for some $m \geq 0$; $D_{B/A}$ is the norm of this, i.e. $\mathfrak{p}^{fm}$.

$$\begin{aligned} L/K \text{ is unramified at } \mathfrak{q} &\iff e = 1 \text{ and } B/\mathfrak{q} \text{ is separable over } A/\mathfrak{p} \\ &\iff B/\mathfrak{q}^e = B/\mathfrak{p}B \text{ is a separable field extension of } A/\mathfrak{p} \end{aligned}$$

(recall $\overline{b}_1, \ldots, \overline{b}_n$ is a basis for this over $A/\mathfrak{p}$)

$$\overset{(*)}{\iff} \det \mathrm{Tr}(\overline{b}_i \overline{b}_j) \neq 0 \text{ in } A/\mathfrak{p}$$

(This is because traces of nilpotent elements are zero, and the determinant will be zero if $B/\mathfrak{p}B$ has any nonzero nilpotent – choose a basis containing that nilpotent. Actually, see better explanation below.)

$$\iff \det \mathrm{Tr}(b_i b_j) \not\equiv 0 \pmod{\mathfrak{p}}$$

This *is* the discriminant, so:

$$\begin{aligned} &\iff \mathfrak{p} \nmid D_{B/A} \\ &\iff m = 0 \\ &\iff \mathfrak{q} \nmid \mathscr{D}_{B/A}. \end{aligned}$$

Now more explanation for (*).

General fact: let k be a field and R a finite-dimensional k-algebra (as a vector space). These are Artinian rings, and there is a structure theorem which implies that

$$R \text{ is a separable } k\text{-algebra} \iff D_{R/k} \neq 0.$$

Case 1: there is a nonzero nilpotent element r. Then $\mathrm{Tr}(\underbrace{rr'}_{\text{nilpotent}}) = 0$ for all $r' \in R$. (The multiplication matrix of a nilpotent element is nilpotent.) Then the matrix $\mathrm{Tr}(r_i r_j)$ has a zero row, and its determinant is zero.

Case 2: there is no nonzero nilpotent element. Then $R = L_1 \times \ldots \times L_s$ where L_i are finite field extensions of k. On the HW you proved that if it's inseparable, the entire trace map is zero. So $D_{R/k} = D_{L_1/k} \cdot \cdots \cdot D_{L_s/k}$ is nonzero iff each L_i is separable over k. □

Corollary 13.11. *L/K is ramified (at some $\mathfrak{q} \mid \mathfrak{p}$) above $\mathfrak{p}$ iff $\mathfrak{p} \mid D_{B/A}$.*

Proof. $\mathfrak{p} \mid D_{B/A} = N_{L/K}\mathscr{D}_{B/A}$ iff there exists $\mathfrak{q} \mid \mathfrak{p}$ such that $\mathfrak{q} \mid \mathscr{D}_{B/A}$. □

Corollary 13.12. *There are only finitely many primes of B that ramify. There are only finitely many primes of A that ramify.*

Example 13.13. Let $L = \mathbb{Q}(\alpha)$ where α is a root of $x^3 - x - 1$. (This is irreducible, because if not, there is a linear factor, but there is no rational root by the rational root test; alternatively, it is irreducible over $\mathbb{F}_2$.) We want to compute the ring of integers $\mathcal{O}_L$.

We know $\mathbb{Z}[\alpha] \subset \mathcal{O}_L$. These are both rank-3 lattices, so it has to be finite index (say, index m).

$$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc}(1, \alpha, \alpha^2) = \operatorname{Disc}(x^3 - x - 1) = -4(-1)^3 - 27(-1)^2 = -23$$

Then $\operatorname{disc} \mathcal{O}_L = \frac{-23}{m^2} \in \mathbb{Z}$. That severely limits the possibilities for m...

The factorization of (p) in $\mathbb{Z}[\alpha]$ corresponds to the factorization of $x^3 - x - 1 \pmod p$. There is ramification at $p = 23$: there are two primes over this; one of them ramifies and one of them doesn't.

Lecture 14: October 21

14.1. Computing the different. Let L/K be a finite separable extension of degree n, and A and B as usual.

Proposition 14.1. *If $B = A[\alpha]$, and f is the minimal polynomial of α over K, then $\mathscr{D}_{B/A} = (f'(\alpha))$.*

Lemma 14.2 (Euler)**.**

$$\mathrm{Tr}\left(\frac{\alpha^i}{f'(a)}\right) = \begin{cases} 0 & \text{if } i = 0, 1, \ldots, n-2 \\ 1 & \text{if } i = n-1 \\ \text{something in } A & \text{if } i \geq n \end{cases}$$

PROOF. Use partial fractions! Factor $f(x) = \prod_{\beta \in R}(x - \beta)$ over $\overline{K}$. Then

$$\frac{1}{f(x)} = \sum_{\beta \in R} \frac{1}{f'(\beta)(x-\beta)}.$$

Write $\frac{1}{x-\beta} = \frac{1}{x(1-\frac{\beta}{x})} = \frac{1}{x} + \frac{\beta}{x^2} + \frac{\beta^2}{x^3} + \dots$. So:

$$\frac{1}{f(x)} = \frac{1}{x^n} - \frac{a_{n-1}}{x^{n+1}} + \dots.$$

Now equate coefficients of $\frac{1}{x^{i+1}}$:

$$LHS = \begin{cases} 0 & \text{if } i < n-1 \\ 1 & \text{if } i = n-1 \\ \text{something in } A & \text{if } i > n-1. \end{cases}$$

The coefficient on the RHS is $\sum_{\beta \in R} \frac{1}{f'(\beta)}\beta^i = \operatorname{Tr}\left(\frac{\alpha^i}{f'(\alpha)}\right)$. □

PROOF OF PROPOSITION 14.1. Let B be the A-span of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. Let $I = \left(\frac{1}{f'(\alpha)}\right)$ = the A-span of $\frac{1}{f'(\alpha)}, \frac{\alpha}{f'(\alpha)}, \dots, \frac{\alpha^{n-1}}{f'(\alpha)}$ (as a fractional ideal of B). Then $I \subset B^*$ since $\operatorname{Tr}\left(\alpha^i \cdot \frac{\alpha^j}{f'(\alpha)}\right) \in A$ by Lemma 14.2. Since these are free modules,

$$(B^* : I) = \det \operatorname{Tr}\left(\underbrace{\alpha^i}_{\substack{\text{basis} \\ \text{for } B}} \underbrace{\frac{\alpha^j}{f'(\alpha)}}_{\substack{\text{basis} \\ \text{for } I}} \right)_{0 \le i,j \le n-1}.$$

(You're expressing the basis for I in terms of the dual basis, by pairing it with the basis for B.) This matrix is easy to take a determinant of, because it has the form $\begin{pmatrix} & & 1 \\ & 1 & * \\ 1 & * & * \end{pmatrix}$ and the determinant of this is just 1. So $B^* = I$, and $\mathscr{D}_{B/A} = I^{-1} = (f'(\alpha))$. □

Proposition 14.3. *Let $M/L/K$ be a tower of finite separable extensions, and a corresponding tower of rings $C/B/A$. Then $\mathscr{D}_{C/A} = \mathscr{D}_{C/B}\mathscr{D}_{B/A}$. (Note that the first two are C-ideals, but the last is a B-ideal. But you can still multiply them.) Taking $N_{M/K}$ in two stages, you get $D_{C/A} = (N_{L/K}D_{C/B}) \cdot D_{B/A}^n$ (where n) is the degree of M/L.*

PROOF. Omitted. Just go back to the definition of the inverse different. □

Aside about algebraic geometry 14.4. Let k be a field, and let K be a finitely generated (*as a field*) algebraic field extension of k of transcendence degree 1. (That is, K is a finite extension of $k(t)$.) Algebraic geometry gives a unique regular projective curve X over k whose function field is K. Any nonempty open subset of X (in the Zariski topology) is $\operatorname{Spec} A$ for a Dedekind domain A. (E.g. you get the projective line by gluing together two affine lines, and those are $\operatorname{Spec} k[t]$ (a Dedekind domain).)

Suppose you have a finite separable extension L/K of degree n. Suppose K is the function field of K; then L is the function field of Y, and there is a dominant morphism $Y \to X$.

Choose a nonempty open affine $\operatorname{Spec} A \subset X$. Let $\operatorname{Spec} B$ be the inverse image of $\operatorname{Spec} A$; there is a corresponding inclusion $A \hookrightarrow B$. Then $\mathscr{D}_{B/A}$ is an ideal of B. Nonzero primes are the points of the curve; an ideal is a product of powers of primes, which corresponds to an integer combination of points. That is, $\mathscr{D}_{B/A}$ is an effective divisor (the coefficients are ≥ 0 since it's an actual ideal, not just a fractional ideal) on the affine curve $\operatorname{Spec} B$. If you vary A, you get an open cover of X, and the inverse image gives an open cover of Y. The different differents $\mathscr{D}_{B/A}$ glue together to get a divisor on Y, called the *ramification divisor* R *of* $Y \to X$ – it measures which points are ramified in this covering of curves.

You can use this to relate the genus of Y to the genus of X: there is a generalized Riemann-Hurwitz formula

$$2g_Y - 2 = n(2g_X - 2) + \deg R.$$

(You define the degree of the morphism $Y \to X$ to be the degree of the field extension L/K.)

What is the genus? If you're working over $\mathbb{C}$, then $X(\mathbb{C})$ is a 1-dimensional complex manifold (this relies on regular-ness), which can be viewed as a 2-dimensional real manifold. Since X is projective, this is a compact manifold. It also turns out to be an oriented surface. Then g_X is the topological genus of this surface.

14.2. Unramified extensions of a complete DVR.

Theorem 14.5. *Let A be a complete DVR, $K = \operatorname{Frac} A$, and $k =$ the residue field. There is an equivalence of categories*

$$\left\{\begin{array}{c}\textit{finite unramified extensions } K' \textit{ of } K \\ \textit{with } K\textit{-algebra homomorphisms}\end{array}\right\} \longrightarrow \left\{\begin{array}{l}\textit{finite separable extensions of } k \\ \textit{with } k\textit{-algebra homomorphisms}\end{array}\right\}$$

that takes K' to its residue field, and on morphisms takes $(K' \to K'')$ to the induced map on residue fields.

In particular,

- *there is a bijection between isomorphism classes of finite unramified extensions of K and finite separable extensions of k;*
- *if K', K'' have residue fields k', k'', then $\operatorname{Hom}_{K\text{-}alg}(K', K'') \to \operatorname{Hom}_{k\text{-}alg}(k', k'')$ is a bijection.*

So everything you'd ever want to know about a finite unramified extension over a complete DVR is preserved after passing to the residue field.

Proof. To check that a functor is an equivalence of categories, you need to show it is

- full and faithful (i.e. $\operatorname{Hom}_K(K', K'') \to \operatorname{Hom}_k(k', k'')$ is surjective and injective);
- essentially surjective (i.e. every k' is isomorphic to the residue field of some K').

Essentially surjective: Given k', use the primitive element theorem to write $k' \cong k[x]/(\overline{f}(x))$ where $\overline{f}$ is an irreducible, separable polynomial over k. Let $f \in A[x]$ be any lift of $\overline{f}$. Let $K' = K[x]/(f(x))$. We proved earlier that K'/K is an unramified extension with valuation ring $A' = A[x]/(f(x))$ and residue field k'.

Full and faithful: Let A', A'' be value rings corresponding to K', K''. Write $k' \cong k(\overline{\alpha})$ for some $\overline{\alpha} \in k'$ using the primitive element theorem. Lift $\overline{\alpha}$ to $\alpha \in A'$. Then $A' = A[\alpha]$ because it has the correct degree (since it's unramified, $[K' : K] = f = [k' : k]$). Let $f \in A[x]$ be the minimal polynomial of α over K. Then $\mathrm{Hom}_K(K', K'') \to \mathrm{Hom}_A(A', A'')$ given by restriction is a bijection (in the reverse direction, tensor with K). There is also a map $\mathrm{Hom}_A(A', A'') \to \mathrm{Hom}_k(k', k'')$; we need to show that this is a bijection.

$\mathrm{Hom}_A(A', A'') = \mathrm{Hom}_A(A[x]/f, A'')$ so specifying a homomorphism is the same as saying where x goes, and x must go to a root of f in A''. That is, $\mathrm{Hom}_A(A', A'') \leftrightarrow \{\text{roots of } f \text{ in } A''\}$. Similarly, $\mathrm{Hom}_k(k', k'') \cong \mathrm{Hom}_k(k[x]/\overline{f}, k'') \cong \{\text{roots of } \overline{f} \text{ in } k\}$. So it suffices to show that $\{\text{roots of } f \text{ in } A\} \to \{\text{roots of } \overline{f} \text{ in } k''\}$ is a bijection. This is exactly what Hensel's lemma says. □

Remark 14.6. We proved that $\mathrm{Hom}_K(K', K'') \to \mathrm{Hom}_k(k', k'')$ is a bijection even if only K' is unramified over K.

Example 14.7. Let $A = \mathbb{Z}_p$ and $K = \mathbb{Q}_p$; then $k = \mathbb{F}_p$. Fix $\overline{\mathbb{F}}_p, \overline{\mathbb{Q}}_p$. For each $n \geq 1$, $\mathbb{F}_p$ has a unique extension of degree n in $\overline{\mathbb{F}}_p$ (namely, $\mathbb{F}_{p^n}$). Therefore, $\mathbb{Q}_p$ has a unique unramified extension of degree n in $\overline{\mathbb{Q}}_p$ (this happens to be $\mathrm{Frac}\, W(\mathbb{F}_{p^n})$ where $W(\mathbb{F}_{p^n})$ is the ring of Witt vectors).

Definition 14.8. Fix a separable closure F^{sep}. Define K^{unr} to be the maximal unramified extension: i.e.

$$K^{unr} = \bigcup_{\substack{\text{finite unram.} \\ \text{ext. } \subset F^{sep}}} K'.$$

The reason I fixed F^{sep} is so that all of these things are contained in it; otherwise, you don't know how to take a union.

Example 14.9. $\mathbb{Q}_p^{unr}/\mathbb{Q}_p$ is the union of all the $\mathrm{Frac}\, W(\mathbb{F}_{p^n})$'s; this is an infinite extension and (by the equivalence of categories) $\mathrm{Gal}(\mathbb{Q}_p^{unr}/\mathbb{Q}_p) \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. This is $\varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$ (where the n are ordered by divisibility in the limit). This is called the *profinite completion* of $\mathbb{Z}$. You can also show that $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

So if you want to describe an automorphism of the big field, you just have to describe a compatible collection of automorphisms of the little fields.

$\mathbb{Q}_p^{unr}$ has value group $\mathbb{Z}$ and residue field $\overline{F}_p$ (the growth of the value group is controlled by e, which is 1 in the unramified case).

Lecture 15: October 23

Let A be a complete DVR, L/K a finite separable (*but not necessarily unramified*) extension where $K = \operatorname{Frac} A$. Also assume that the extension ℓ/k of residue fields is separable. We denote $e := e_{L/K}$ and $f = f_{L/K}$.

Theorem 15.1. *(1) Among subextensions of L/K unramified over K, there is one containing all the others; call it K'.*

(2) L/K' is totally ramified. $[L : K'] = e$ and $[K' : K] = f$. The extension of residue fields corresponding to $L/K'/K$ is $\ell/\ell/k$.

(3) If L/K is Galois, then $\mathrm{Gal}(L/K') = I_{L/K}$ (the inertia subgroup in $\mathrm{Gal}(L/K)$).

Proof. (1) Let K' be an unramified extension of K with residue field ℓ (you can do this by Theorem 14.5). The inclusion $\ell \hookrightarrow \ell$ induces an inclusion $K' \hookrightarrow L$. If $K \overset{\text{unram}}{\subset} F \subset L$, then the corresponding inclusion of residue fields $f \subset \ell \subset \ell$ induces a series of field homomorphisms $F \to K' \to L$. The composition is an inclusion, and $K' \hookrightarrow L$ is an inclusion, so $F \to K'$ is an inclusion as well.

(2) Now we have a tower $L/K'/K$ where K'/K is unramified. This corresponds to an extension of residue fields $\ell/\ell/k$. First note that $[K' : K] = f$ and $[L : K'] = e$. We showed above that $f_{K'/K} = 1$ (since the extension of residue fields is ℓ/k), so $f_{L/K'} = 1$, so $e_{L/K'} = [L : K'] = e_{L/K}$. Thus L/K' is totally ramified.

(3) $I_{L/K'} \subset I_{L/K}$ and $I_{L/K'} \subset \mathrm{Gal}(L/K')$. The groups $I_{L/K'}, I_{L/K}, \mathrm{Gal}(L/K')$ have cardinalities $e_{L/K'}, e$, and $[L : K']$, respectively. We showed in (2) that these are all the same. □

15.1. Tamely ramified extensions. Same setup as in the previous theorem; suppose $\operatorname{char} k = p$.

Definition 15.2. L/K is *tamely ramified* if $p \nmid e$ (this is always true when the characteristic zero.)

L/K is *wildly ramified* if $p \mid e$.

Example 15.3. $L = K(\pi^{1/e})$ (where π is the uniformizer of A) is totally ramified of degree e over K. This is tamely ramified iff $p \nmid e$.

Theorem 15.4. *Let A, K, L, B be as above. If L/K is totally tamely ramified of degree e, then $L = K(\pi^{1/e})$ for some uniformizer π of A.*

In general, if you have any tamely ramified extension, you can break it up as an unramified bottom part and a tamely totally ramified top part.

Proof. It turns out that you have to be careful with the choice of π. But start off by choosing arbitrary uniformizers π_K of K and π_L of L. If we normalize so that $v(\pi_K) = 1$,

then $v(\pi_L) = \frac{1}{e}$ (by one definition of the ramification index). Then $L = K(\pi_L)$ because $[L : K] \geq [K(\pi_L) : K] \geq e = [L : K]$ (and hence the inequalities are equalities).

$v(\pi_L^e) = v(\pi_K)$, but a priori $\pi_L^e = u \cdot \pi_K$ for some "unit" $u \in L$ (i.e. $v(u) = 0$). If u were 1, then $L = K(\pi_L) = K(\pi_k^{1/e})$ as desired. The goal is to choose π_K, π_L differently so as to make $u = 1$.

You can replace π_K with $t \cdot \pi_K$, where t is a unit (in A). That is, you can multiply u by an element $t \in A^\times$. A and B have the same residue field (L/K is totally ramified, so $f = 1$). You can multiply u by something that reduces to u^{-1} in the residue field; so assume that $u \equiv 1 \pmod{\mathfrak{m}}_B$ (maximal ideal of B).

You can change π_L by multiplying it by a unit in B; this multiplies $\pi_L^e = u\pi_K$ by unit^e. I claim that u is an e^{th} power; this is because $x^e = u$ has a solution in B by Hensel's lemma. So we can make $u = 1$. □

Let A be a complete DVR. Let $K = \operatorname{Frac} A$. You can extend the absolute value uniquely to any extension, and hence you get an absolute value on $\overline{K}$.

Definition 15.5. Let $\alpha, \beta \in \overline{K}$ with α separable over K. Let $\alpha = \alpha_1, \ldots, \alpha_n \in \overline{K}$ be the conjugates of α. Say that "β belongs to α" if $|\beta - \alpha| < |\beta - \alpha_j|$ for all $j \geq 2$ (it is closer to α than any of the other conjugates). Equivalently, $|\beta - \alpha| < |\alpha - \alpha_j|$ for all $j \geq 2$ (equivalence is by non-archimedeanness – every nonarchimedean triangle is isosceles).

Lemma 15.6 (Krasner's lemma)**.** *A, B, K, L as before (in particular A is a complete DVR). If β belongs to α, then $K(\beta) \supset K(\alpha)$.*

Proof. If not, then $\alpha \notin K$. Then there is some $\sigma \in$ the Galois group that fixes β and moves α (i.e. $\beta \in \operatorname{Gal}(\overline{K}/K(\beta))$ but $\sigma\alpha \neq \alpha$). We know that $|\sigma x| = |x|$ for all $x \in \overline{K}$ by uniqueness of absolute values. Take $x = \beta - \alpha$; then this tells you $|\beta - \sigma\alpha| = |\beta - \alpha|$, contradicting the definition of "β belongs to α". □

Proposition 15.7. *Take A, B, K, L as before. Let $f \in K[x]$ be a separable polynomial, monic irreducible of degree n. If $g \in K[x]$ is sufficiently close to f (the coefficients are sufficiently close), then*

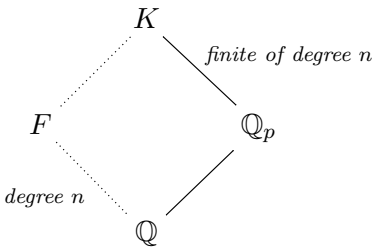
(1) each root β of g belongs to a root α of f;
(2) $K(\beta) = K(\alpha)$;
(3) g is separable and irreducible.

Proof. (1) Fix β. Then $f(\beta) \approx g(\beta) = 0$ (the coefficients are close, and β is not too big – the coefficients are bounded, and that bounds the roots). $f(\beta) = \prod_{\substack{\text{roots } \alpha \\ \text{of } f}} (\beta - \alpha)$. One of these factors $\beta - \alpha$ must be small, less than $|\alpha' - \alpha|$ for distinct roots α, α' of f if g is close enough to f.

(2) By Krasner's lemma, $K(\beta) \supset K(\alpha)$. But $K(\beta)$ has degree $\leq n$, and $K(\alpha)$ has degree n. So $K(\beta) = K(\alpha)$.

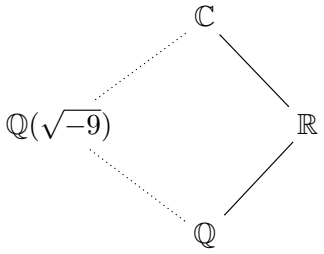
(3) $K(\beta) = K(\alpha)$ is a separable extension of degree n over K. So g is separable and irreducible. □

Corollary 15.8. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. (This is automatically separable because we're in characteristic 0.) Then there exists $F \subset K$ such that $[F : \mathbb{Q}] = n$ and $F \cdot \mathbb{Q}_p = K$.*

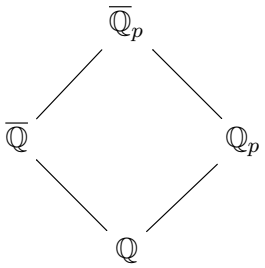


Proof. By the primitive element theorem, $K = \mathbb{Q}_p(\alpha)$. Let f be the minimal polynomial of α over $\mathbb{Q}_p$; this lives in $\mathbb{Q}_p[x]$. Approximate f by some $g \in \mathbb{Q}[x]$; you can do this since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ (everything in $\mathbb{Q}_p$ is a limit of things in $\mathbb{Q}$). By Proposition 15.7, g is irreducible over $\mathbb{Q}_p$ (it is irreducible over $\mathbb{Q}$), and has a root $\beta \in \overline{\mathbb{Q}}_p$ such that $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha)$. Let $F = \mathbb{Q}(\beta)$. Then $[F : \mathbb{Q}] = \deg g = n$ and $F \cdot \mathbb{Q}_p = \mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha) = K$. □

Example 15.9. This sort of works over $\mathbb{R}$ too. Suppose $f = x^2 + \pi^2$ over $\mathbb{R}$, and you approximate this by $g = x^2 + 9$. This leads to



Corollary 15.10. *Choose an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}_p$. Then $\overline{\mathbb{Q}} \cdot \mathbb{Q}_p = \overline{\mathbb{Q}}_p$.*



Corollary 15.11. *The homomorphism* $\mathrm{Gal}(\overline{Q}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *given by restriction of automorphisms is injective.*

Lecture 16: October 28

Definition 16.1. Let V be an n-dimensional real vector space. A *lattice* in V is a subgroup of the form

$$\Lambda := \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_m$$

where $e_1, \ldots, e_m \in V$ are linearly independent over $\mathbb{R}$.

A lattice is *full* if $m = n$.

Nonexample 16.2. $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ in $\mathbb{R}$ is not a lattice because the generators are not linearly independent.

Proposition 16.3. *Let* $\Lambda \subset V$ *be a subgroup. Then* Λ *is a lattice* $\iff$ Λ *is (topologically) discrete.*

Proof. ($\implies$) Extend $e_1, \ldots, e_m$ to a basis $e_1, \ldots, e_n$ of V. Then there is an isomorphism $V \cong \mathbb{R}^n$ where the e_i's correspond to the standard basis of $\mathbb{R}^n$. Then $\Lambda \cong \mathbb{Z}^m \times \{0\}^{n-m} \subset \mathbb{R}^n$ so Λ is discrete. ($\impliedby$) Assume Λ is discrete. Replace V by the $\mathbb{R}$-span of Λ. Change basis to assume that $V = \mathbb{R}^n$ and $\Lambda \supset \mathbb{Z}^n$.

Claim 16.4. $(\Lambda : \mathbb{Z}^n)$ *is finite.*

Proof. If not, the unit cube contains infinitely many elements of Λ. Break the unit cube into smaller cubes of side length $\frac{1}{q}$. By the pigeonhole principle, one of these cubes contains ≥ 2 elements of Λ. Their difference is an element of Λ of length $\leq \mathrm{diam}(\text{cube}) = \frac{1}{q}\sqrt{n}$. But q was arbitrary, so Λ contains arbitrarily short vectors. So 0 is not an isolated point in Λ. This contradicts the assumption that Λ was discrete. □

So Λ is finitely generated. So $\Lambda \cong \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n \oplus$ a finite abelian group, but the finite group is zero since $\Lambda \subset V$ (so there are no elements of finite order). $v_1, \ldots, v_n$ are independent since there are n of them and they span $\mathbb{R}^n$. So Λ is a lattice. □

We want to talk about volume, so from now on assume V is equipped with a positive definite inner product. So you get a notion of length and volume (i.e. Haar measure – if you identify V with $\mathbb{R}^n$ this will just be Lebesgue measure $\times$ a scalar). You can always reduce to the case $V \cong (\mathbb{R}^n$ with the usual inner product).

Example 16.5. Let $\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n \subset \mathbb{R}^n$ be a full lattice. Let $F = \{a_1e_1 + \cdots + a_ne_n : 0 \leq a_i < 1\}$. (E.g. if $n = 2$ then this is the parallelogram spanned by e_1, e_2, and $e_1 + e_2$. It is clear that the lattice gives a tiling of the plane by this parallelogram.) Then

$\mathbb{R}^n = \bigsqcup_{\lambda\in\Lambda}(F+\lambda)$. Also, $\mathrm{vol}(F) = |\det(e_1,\dots,e_n)|$ (this is the matrix whose i^{th} column is e_i).

Definition 16.6. A *fundamental domain* for Λ is a measurable subset $F \subset V$ such that $V = \bigsqcup_{\lambda\in\Lambda}(F+\lambda)$.

There are many possibilities for this: if F is a fundamental domain, then so is $F+e_1$, or you can cut it up into pieces and translate them by different elements of Λ. It turns out that this is basically all that can happen.

Proposition 16.7. *If F, G are two fundamental domains for $\Lambda \subset V$ then* $\mathrm{vol}(F) = \mathrm{vol}(G)$.

Proof. Translation by $-\lambda$ of $(F+\lambda)\cap G$ is $F\cap(G-\lambda)$. Since these are translates, they have the same volume. But $\bigsqcup_\lambda (F+\lambda)\cap G = G$ and $\bigsqcup F\cap(G-\lambda) = F$, so these also have the same volume. □

Definition 16.8. Define the *covolume* to be $\mathrm{covol}(\Lambda) := \mathrm{vol}(F)$ for a fundamental domain. This is $\mathrm{vol}(V/\Lambda)$. It measures how spread out the lattice is.

Proposition 16.9. *If $\Lambda \supset \Lambda'$ are lattices in V,* $\mathrm{covol}(\Lambda') = (\Lambda:\Lambda')\,\mathrm{covol}(\Lambda)$.

Proof. If F is a fundamental domain then $\bigsqcup_{\substack{\text{coset reps}\\ \lambda \text{ for } \Lambda'\subset\Lambda}} F+\lambda$ is a fundamental domain for Λ'. □

Lemma 16.10. *Let $S \subset \mathbb{R}^n$ be any measurable subset. If* $\mathrm{vol}(S) > 1$*, then there exist distinct $s, s' \in S$ such that $s - s' \in \mathbb{Z}^n$.*

Proof. Chop $\mathbb{R}^n$ into unit cubes, and translate the pieces of S into the "standard fundamental lattice" $[0,1)^n$. They overlap, because the volume is > 1. If s, s' are two overlapping points (after being translated), then $s - s' \in \mathbb{Z}^n$. □

Theorem 16.11 (Minkowski's lattice point theorem for $\mathbb{Z}^n \subset \mathbb{R}^n$)**.** *Let $S \subset \mathbb{R}^n$ be* symmetric *(i.e. if $x \in S$ then $-x \in S$) and* convex *(i.e. if $x, y \in S$, then the line segment joining x and y is completely contained in S). If* $\mathrm{vol}(S) > 2^n$*, then S contains a nonzero lattice point.*

It's kind of obvious that $0 \in S$: if $x \in S$, then $-x \in S$, and so the line between them – and in particular its midpoint 0 – is in S.

Proof. $\mathrm{vol}(\frac{1}{2}S) > 1$ (by $\frac{1}{2}S$ I mean scaling all the vectors in S by $\frac{1}{2}$) so by Lemma 16.10 there exist distinct $\frac{1}{2}s, \frac{1}{2}s' \in \frac{1}{2}S$ such that $\frac{1}{2}s - \frac{1}{2}s' \in \mathbb{Z}^n$. Write $\frac{1}{2}s - \frac{1}{2}s' = \frac{s+(-s')}{2}$, so this is the midpoint of the segment joining s and $-s'$. By convexity, it is in S. □

Theorem 16.12 (Minkowski's lattice point theorem)**.** *Let V be an $\mathbb{R}$-vector space with inner product, and Λ a full lattice in V. Let $S \subset V$ be a symmetric, convex subset. Suppose that* $\mathrm{vol}(S) > 2^n \,\mathrm{covol}(\Lambda)$*. Then S contains a nonzero element of Λ.*

Theorem 16.13. *If p is a prime and $p \equiv 1 \pmod 4$, then p is a sum of two integer squares.*

There's another standard proof of this using the fact that $\mathbb{Z}[i]$ is Euclidean (but proving *that* involves some geometry).

Proof. The group $\mathbb{F}_p^\times$ is cyclic of order $p-1$, so $\mathbb{F}_p^\times$ contains an element i of order 4. Then i^2 is of order 2; the only solutions to $x^2 - 1$ over a field are ± 1, so $i^2 = -1$. Let

$$\Lambda = \{\lambda \in \mathbb{Z}^2 \,:\, (\lambda \pmod p) \in \mathbb{F}_p \cdot (1, i)\}$$

(e.g. if $p = 5$ (so $i = 2$), then this includes $(n, 2n)$ for all n but also $(3, 1)$ because it is $\equiv (3, 6) = 3 \cdot (1, \underbrace{\text{“}i\text{”}}_{2}) \bmod 5$). We have $(p\mathbb{Z})^2 \subset \Lambda \subset \mathbb{Z}^2$. Since $\mathrm{covol}(\mathbb{Z}^2) = 1$ and $\mathrm{covol}((p\mathbb{Z})^2) = p^2$ and the inclusions are strict, the inclusions are both index p so $\mathrm{covol}(\Lambda) = p$. Let $S = \{v \in \mathbb{R}^2 \,:\, |v| < \sqrt{2p}\}$; the disk is obviously symmetric and convex. Then $\mathrm{vol}(S) = \pi \cdot 2p > 4p = 2^2 \cdot \mathrm{covol}(\Lambda)$. By Minkowski's theorem, S contains some nonzero $(a, b) \in \Lambda$. Then $a^2 + b^2 \equiv 0 \pmod p$ because $(a, b) \in \Lambda$, and also $0 < a^2 + b^2 < 2p$ since $(a, b) \in S$. So $a^2 + b^2 = p$. □

To prove that every integer is the sum of four squares, try generalizing this...

16.1. Places.

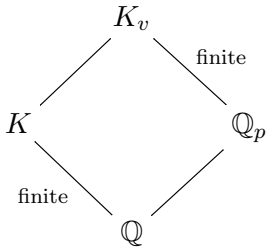
Definition 16.14. A *place* v of K is an equivalence class of nontrivial absolute values on K. Let M_K be the set of places of K.

Example 16.15. Ostrowski's theorem says that $M_\mathbb{Q} = \{|\ \ |_p \,:\, p \le \infty\}$, and that is in bijection with the set of primes, including the "infinite prime". The idea is that, in general, absolute values sort of correspond to primes, possibly infinite primes.

Every $v \in M_K$ is (the equivalence class of) an extension of some $|\ \ |_p$ for some $p \le \infty$. Write $v \mid p$.

v is *archimedean* if $v \mid \infty$, and *nonarchimedean* if $v \mid p$ for some finite prime p.

Definition 16.16. If $v \in M_k$, then let K_v be the completion of K w.r.t. v. Get



where $v \mid p$. (Note that "$\mathbb{Q}_p$" might mean $\mathbb{R}$ if $p = \infty$.)

Example 16.17. If v is archimedean, then K_v is a finite extension of $\mathbb{R}$; the only possibilities are $\mathbb{R}$ or $\mathbb{C}$. If v is nonarchimedean, then v is associated to a discrete valuation on K extending v_p on $\mathbb{Q}$.

Theorem 16.18. $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\cong} \prod_{v|p} K_v$ *(even if $p = \infty$).*

Proof. $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a separable algebra over $\mathbb{Q}_p$, so it is $\cong \prod L_i$, where each L_i is a finite separable extension of $\mathbb{Q}_p$; I need to argue that the factors L_i correspond to completions.

We know that $|\ \ |_p$ on $\mathbb{Q}_p$ extends to some $|\ \ |_i$ on L_i, and L_i is complete, and K is dense in L_i. Let $v_i = |\ \ |_i$ restricted to K. If you have a dense subfield of a complete field, then the completion of the subfield is the original complete field. So $L_i = K_{v_i}$.

We have a map $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \to K_v$ because both $K, \mathbb{Q}_p \subset K_v$. This is surjective because they're dense. So each K_v appears at least once as an L_i.

Now the only thing to rule out is having one K_v multiple times. This can't happen: K is dense in $K \otimes \mathbb{Q}_p \cong \prod L_i$. If two of the factors were the same, then K would be going in as the diagonal to the product of those two factors. □

Corollary 16.19. *There is a bijection*

$$\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}_p) \Big/ \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}) \longleftrightarrow \{\textit{places } v \mid p\}.$$

(The LHS is the set of embeddings of K into $\overline{\mathbb{Q}}_p$, up to Galois conjugacy.)

Proof.

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

Ways of embedding K_v are in bijection with ways of choosing a root. So the Galois group acts transitively on $\mathrm{Hom}_{\mathbb{Q}_p}(K_v, \overline{\mathbb{Q}}_p)$, so there's a single orbit here. □

Example 16.20. $\mathrm{Hom}(K, \mathbb{C})/$ complex conjugation is in bijection with {archimedean places}.

$\mathrm{Hom}(K, \mathbb{R})$ is in bijection with the set of size-1 orbits, which is in bijection with the real places. The number of these is called r_1. Homomorphisms $K \to \mathbb{C}$ not mapping into $\mathbb{R}$ mod complex conjugation correspond to the size-2 orbits; these are the complex places. The number of these is called r_2.

So the size of the whole set is $r_1 + 2r_2$, and that is the number of roots, i.e. $[K : \mathbb{Q}]$.

Lecture 17: October 30

If $\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n \subset \mathbb{R}^n$, then we showed last time that $\mathrm{covol}(\Lambda) = \mathrm{vol}(F) = |\det A|$, where $A = \begin{pmatrix} \vdots & & \vdots \\ e_1 & & e_n \\ \vdots & & \vdots \end{pmatrix}$. There is another formula that is useful: note that this is also equal to $\sqrt{\det(A^t A)} = \sqrt{\det(\langle e_i, e_j \rangle)}$.

Recall that *places* are equivalence classes of nontrivial absolute values on K; each v is above some $p \leq \infty$. We had

Theorem 17.1. $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{v|p} K_v$

The new information here is about $v \mid \infty$. We have

$$K_{\mathbb{R}} := K \otimes \mathbb{R} \cong \prod_{v|\infty} K_v \cong \mathbb{R}^r \times \mathbb{C}^s$$

where $r + 2s = n$ (r and s this time are the same as r_1 and r_2 last time). K embeds into this; $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ is a set of order n with an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Homomorphisms that are fixed by this Galois group are the ones that land entirely in $\mathbb{R}$. There is a correspondence

$$\{\text{places } v \mid \infty\} \leftrightarrows \mathrm{Hom}(K, \mathbb{C}) \big/ \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \leftrightarrows \{\text{factors of } K_{\mathbb{R}}\}$$

because there are r size-1 orbits (i.e. $|\mathrm{Hom}(K, \mathbb{R})| = r$) and s size-2 orbits (these correspond to nonreal embeddings $K \to \mathbb{C}$, modulo complex conjugation), and $r + 2s = n$.

Example 17.2. Let $K = \mathbb{Q}[x]/(x^3 - 2)$. There are three possible embeddings, sending x to $\sqrt[3]{2} \in \mathbb{R}$, or $\zeta_3 \sqrt[3]{2}$, or $\zeta_3^2 \sqrt[3]{2} \in \mathbb{C}$ where ζ_3 is a primitive cube root of 1. So in this case, $n = 3$, $r = 1$, and $s = 1$ (there are two places above ∞).

Definition 17.3. If $v \mid p$, the *normalized "absolute value"* on K_v is

$$|x|_v = \left| N_{K_v/\mathbb{Q}_p}(x) \right|_p$$

where $|p|_p = \frac{1}{p}$ for finite p and $|x|_\infty$ is what you think it is for $x \in \mathbb{R}$.

Warning 17.4. We will show below that this is not always an absolute value.

Example 17.5 (Nonarchimedean case)**.** Suppose that $v \mid p < \infty$. Let $\mathcal{O}_v$ be the DVR in K_v. If $x \in \mathcal{O}_v$, then I claim that

$$|x|_v = \left(\#\frac{\mathcal{O}_v}{x\mathcal{O}_v}\right)^{-1}.$$

Why?

$$\left(N_{K_v/\mathbb{Q}_p}(x)\right) = N(x\mathcal{O}_v)$$

where these are both fractional ideals for $\mathbb{Z}_p$, the norm on the LHS is the element norm, and the norm on the RHS is the ideal norm. This $= (\mathcal{O}_v : x\mathcal{O}_v)$, where $p^m = \#\mathcal{O}_v/x\mathcal{O}_v$. To get the result, just take $|\ \ |_p$.

Example 17.6 (Archimedean case)**.** If v is real, then $K_v = \mathbb{Q}_p = \mathbb{R}$, so $|\ \ |_v$ is the usual absolute value on $\mathbb{R}$.

If v is complex, $|\ \ |_v$ is the square of the absolute value on $\mathbb{C}$. But this isn't an absolute value: $|1+1|_v \not\leq |1|_v + |1|_v$ (the triangle inequality fails).

Another interpretation: choose a Haar measure on K_v. Then composing this with multiplication by x gives another Haar measure. There is only one Haar measure, up to scalar, and it turns out that in this case, the scalar multiple is $|x|_v$.

Theorem 17.7 (Product formula)**.** *If $x \in K^\times$ then*

$$\prod_{v \in M_K} |x|_v = 1.$$

Proof. $N_{K/\mathbb{Q}}(x) = N_{K\otimes\mathbb{Q}_p/\mathbb{Q}_p}(x)$ (because if you have a basis for $K/\mathbb{Q}$, after tensoring with $\mathbb{Q}_p$ you can use the same basis; the norm is the determinant of the multiplication-by-x map, and it's the same matrix in each case). Multiplication by an element on $K \otimes \mathbb{Q}_p \cong \prod_{v|p} K_v$ is the same as multiplying each factor, so the norm breaks up as a product: $N_{K\otimes\mathbb{Q}_p/\mathbb{Q}_p}(x) = \prod_{v|p} N_{K_v/\mathbb{Q}_p}(x)$. Now take $|\ \ |_p$ to get $|N_{K/\mathbb{Q}}(x)|_p = \prod_{v|p} |x|_v$. Take the product over all $p \leq \infty$:

$$1 = \prod_{\text{all } \mathfrak{p} \leq \infty} \left|N_{K/\mathbb{Q}}(x)\right|_p = \prod_{\text{all } p \leq \infty} \prod_{v|\infty} |x|_v = \prod_v |x|_v$$

where the first equality is using the product formula over $\mathbb{Q}$. □

There are analogies between number theory and curves:

number field object	function field analogue
$\mathbb{Z}$	$k[t]$ (regular functions on $\mathbb{A}^1$)
$\mathbb{Q}$	$k(t)$ (function field of $\mathbb{P}^1_k$)
$v_p \longleftrightarrow \lvert\ \rvert_p$	v_f for some monic irred. $f \in k[t]$
$\lvert\ \rvert_\infty$	v_∞ ("valuation at ∞": $v_\infty\left(\frac{g}{h}\right) = \deg h - \deg g$)
number field K	function field K of some regular projective integral curve (= finite extension of $k(t)$)
element of K	element of K = rational function on X
places of K	Zariski-closed points of X
product formula	degree of principal divisor is 0

If $f \in k[t]$, $v_f(\varphi)$ is the order of vanishing of φ at a.

Part of the reason for introducing $\lvert\ \rvert_\infty$ is because it's like compactifying $\operatorname{Spec}\mathbb{Z}$, analogously to $\mathbb{P}^1$ being better-behaved than $\mathbb{A}^1$. Just as v_p and $\lvert\ \rvert_\infty$ are all the absolute values on $\mathbb{Q}$ (up to equivalence), on the function field side v_f and v_∞ are all the nontrivial absolute values on $k(t)$ that are trivial on k (up to equivalence). The proof of this is basically the same as the proof of Ostrowski's theorem.

Think of $\mathbb{Z}$ as regular functions on $\operatorname{Spec}\mathbb{Z}$, where n is the function $p \mapsto n \pmod p$.

There are embeddings

$$\mathcal{O}_K \hookrightarrow K \hookrightarrow K_\mathbb{R} = K \otimes \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s \hookrightarrow K_\mathbb{C} := K \otimes \mathbb{C} \cong \mathbb{C}^{r+2s} = \mathbb{C}^n.$$

($K_\mathbb{C} = K_\mathbb{R} \otimes_\mathbb{R} \mathbb{C}$ so the $\mathbb{R}$'s in $K_\mathbb{R}$ become $\mathbb{C}$'s, and the $\mathbb{C}$'s become $\mathbb{C} \otimes_\mathbb{R} \mathbb{C} \cong \mathbb{R}[x]/(x^2+1) \otimes_\mathbb{R} \mathbb{C} = \mathbb{C}[x]/(x^2+1) \cong \mathbb{C} \times \mathbb{C}$ where the last isomorphism sends $x \mapsto (i, -i)$.) As topological abelian groups, this is

$$\mathbb{Z}^n \hookrightarrow \mathbb{Q}^n \hookrightarrow \mathbb{R}^n \hookrightarrow \mathbb{C}^n.$$

So $\mathcal{O}_K$ is a full lattice in $K_\mathbb{R}$.

Right now $K_\mathbb{R}$ just a vector space; we need to choose a measure so we can talk about Minkowski spaces. It suffices to define length, and for that it suffices to define an inner product. There is a canonical hermitian inner product on $\mathbb{C}^n$, defined as

$$\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n) \rangle = \sum_{i=1}^n a_i \overline{b_i} \in \mathbb{C}.$$

There is a *canonical* isomorphism $K \otimes \mathbb{C} \xrightarrow{\cong} \mathbb{C}^n$ arising from the injection $K \hookrightarrow \mathbb{C}^n$ given by taking $x \mapsto (\sigma(x))_{\sigma \in \operatorname{Hom}(K,\mathbb{C})}$. So we get a canonical inner product on $K_\mathbb{C}$. Now restrict

this to get a canonical inner product on $K_{\mathbb{R}}$. This is a usual inner product (bilinear, not hermitian).

If $x, y \in K \hookrightarrow K_{\mathbb{R}}$, then $\langle x, y\rangle = \sum_{\sigma: K\to\mathbb{C}} \sigma(x)\overline{\sigma(y)}$. I claim that this is in $\mathbb{R}$: either σ already maps into the real numbers, or it is part of a pair.

Example 17.8. Let $K = \mathbb{Q}(i)$. There are no real embeddings, and one pair of complex embeddings, $\sigma_1 : i \mapsto i$ and $\sigma_2 : i \mapsto -i$. $K_{\mathbb{R}} = \mathbb{C}$ and $r = 0$, $s = 1$. What is the length of $i \otimes 1 \in K_{\mathbb{R}}$?

$$\begin{aligned}\langle i\otimes 1, i\otimes 1\rangle &= \langle (i,-i),(i,-i)\rangle \\ &= i\cdot\bar{i} + (-i)\overline{(-i)} = 2\end{aligned}$$

so $\|i \otimes 1\| = \sqrt{2}$.

Warning 17.9. Although $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s \overset{\text{as } \mathbb{R}\text{-V.S.}}{\cong} \mathbb{R}^{r+2s}$, volume in $K_{\mathbb{R}}$ corresponds to $2^s\cdot$ Lebesgue measure on $\mathbb{R}^{r+2s}$. The intuition is that $\mathbb{C} \hookrightarrow \mathbb{C}\times\mathbb{C}$ embeds $\mathbb{C}$ anti-diagonally (i.e. $x \mapsto (x, \overline{x})$), so everything gets stretched by $\sqrt{2}$.

We have proved that $\mathcal{O}_K$ is a full lattice in $K_{\mathbb{R}}$. What is its covolume?

Proposition 17.10. $\operatorname{covol}(\mathcal{O}_K) = \sqrt{|\operatorname{disc}\mathcal{O}_K|}$

(We're thinking of K as an extension of $\mathbb{Q}$, and $\mathcal{O}_K$ as a $\mathbb{Z}$-module.)

Proof. Let $e_1, \dots, e_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Let $A = (\sigma(e_j))_{\sigma,j} \in M_n(\mathbb{C})$ where the rows are indexed by homomorphisms $\sigma : K \hookrightarrow \mathbb{C}$. We showed that $\operatorname{disc}\mathcal{O}_K = (\det A)^2$ by considering $A^T A$. By the fact at the beginning of this lecture,

$$\begin{aligned}\operatorname{covol}(\mathcal{O}_K)^2 &= \det\langle e_i\otimes 1, e_j\otimes 1\rangle_{i,j} \\ &= \det\left(\sum \sigma_{e_i}\overline{\sigma_{e_j}}\right) \\ &= \det(\overline{A}^T A) = \overline{\det A}\det A \\ &= |\det A|^2 .\end{aligned}$$

Thus $|\operatorname{disc}\mathcal{O}_K| = \operatorname{covol}(\mathcal{O}_K)^2$. □

Lecture 18: November 4

HW #9 due on Monday, November **17**.

Last time we talked about viewing $\mathcal{O}_K$ as a lattice in $\mathbb{C}^n$ via the inclusions

$$\mathcal{O}_K \hookrightarrow K \hookrightarrow K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s \hookrightarrow K_{\mathbb{C}} \cong \mathbb{C}^n$$

where $n = r + 2s = [K : \mathbb{Q}]$. We proved that $\operatorname{covol}(\mathcal{O}_K) = \sqrt{|\operatorname{disc}\mathcal{O}_K|}$.

Corollary 18.1. *Let I be a nonzero fractional ideal of $\mathcal{O}_K$. Then*

$$\operatorname{covol}(I) = \sqrt{|\operatorname{disc} \mathcal{O}_K|} \cdot N(I).$$

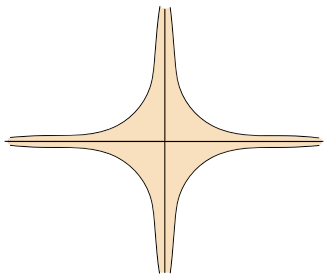
PROOF. Multiplying I by a positive integer b multiplies both sides by b^n. Without loss of generality $I \subset \mathcal{O}_K$. Then $\operatorname{covol}(I) = \operatorname{covol}(\mathcal{O}_K) \cdot (\mathcal{O}_K : I)$. □

If $0 \neq a \in I$, then $I \mid (a)$, so $N(I) \mid |N(a)| = \prod_{\sigma: K \to \mathbb{C}} |\sigma_a|$ (note that $N(I)$ is the ideal norm, and $N(a)$ is the element norm). (In fact, $I = (a) \iff N(I) = |N(a)|$ in $\mathbb{Z}$; this can be used as a test for principal-ness.)

Theorem 18.2 (Minkowski bound)**.** *Let K be a number field. Then there exists a constant $m = m_K \in \mathbb{R}_{>0}$ such that for any nonzero fractional ideal I of K, there exists a nonzero $a \in I$ such that $|N(a)| \leq m \cdot N(I)$. In fact, $m := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc} \mathcal{O}_K|}$ works, where s is the same as in $n = 2s + r$. This number is called the* Minkowski constant *of K.*

PROOF. We will apply the Minkowski lattice point theorem to the lattice I in $K_{\mathbb{R}}$, and a symmetric convex set $S \subset K_{\mathbb{R}}$ chosen so that $|N(a)|$ is small for every $a \in S$.

(For example, if $K = \mathbb{Q}(\sqrt{5})$, then $K_{\mathbb{R}} = \mathbb{R} \times \mathbb{R}$ (there are two real embeddings) and the norm map $K_{\mathbb{R}} = \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is given by $(x, y) \mapsto xy$. The region where the norm is $\leq$ a constant is



This is not convex, but you can set S to be the diamond $\{(x, y) : |x| + |y| \leq c\}$; choose c so this sits inside the original region but it is big enough to make the Minkowski lattice point theorem work.)

Lemma 18.3. *Let $S = \{z \in (z_\sigma)_{\sigma \in \operatorname{Hom}(K, \mathbb{C})} \in K_{\mathbb{R}} \subset K_{\mathbb{C}} : \sum |z_\sigma| \leq t\}$. Then* $\operatorname{vol}(S) = 2^r \pi^s \frac{t^n}{n!}$.

SKETCH OF PROOF. The isomorphisms $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s} = \mathbb{R}^n$ takes the canonical measure on $K_{\mathbb{R}}$ to $2^s \cdot$ the Lebesgue measure on $\mathbb{R}^n$. The condition $\sum |z_\sigma| \leq t$ in $K_{\mathbb{R}}$ corresponds to $|x_1| + \ldots |x_r| + 2\sqrt{u_1^2 + v_1^2} + \cdots + 2\sqrt{u_s^2 + v_s^2} \leq t$. This is basically an 18.02 problem. (E.g. convert the pairs of coordinates (u_i, v_i) to polar coordinates; you get an $r\, dr\, d\theta$ term, etc. . .). Remembering the extra 2^s, you eventually get the answer. □

Back to the proof of the theorem. Choose t so that $\operatorname{vol}(S) > 2^n \operatorname{covol}(I)$ (the LHS is a constant $\cdot t^n$ and the RHS is a constant $\cdot N(I)$). Then by Minkowski, there exists $a \in S$. Use:

Fact 18.4 (AM-GM (arithmetic mean – geometric mean))**.**

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \dots x_n}.$$

So

$$n \sqrt[n]{|N(a)|} = n \sqrt[n]{\prod |\sigma_a|} \leq \sum |\sigma_a| \leq t.$$

Then

$$|N(a)| \leq \text{const} \cdot t^n = \text{const}' N(I).$$

(You can be more precise about the constant to get the Minkowski constant.) □

Recall $\operatorname{Cl} K = \operatorname{Cl} \mathcal{O}_K = \operatorname{Pic} \mathcal{O}_K = \mathcal{I}_K /$ principal fractional ideals (where $\mathcal{I}_K$ is the group of fractional ideals for $\mathcal{O}_K$.)

Theorem 18.5. *Every ideal class contains an integral ideal (i.e. an actual ideal of $\mathcal{O}_K$) of norm $\leq m$ (where m is the Minkowski constant).*

Proof. Let $[I]$ be the *inverse* of the target ideal class. Theorem 18.2 gives a nonzero $a \in I$ such that $|N(a)| \leq m \cdot N(I)$. Then $(a)I^{-1}$, which is in the ideal class $[I]^{-1}$, is an integral ideal of norm $\leq m$. (Why integral? Since $a \in I$, $I \mid (a)$.) □

Lemma 18.6. $\{$*Ideals* $I \subset \mathcal{O}_K : N(I) \leq B\}$ *is finite for any* $B > 0$.

Proof. *Proof 1:* $\mathcal{O}_K \cong \mathbb{Z}^n$ has only finitely many subgroups I of prescribed index q; by Lagrange's theorem, $(q\mathbb{Z})^n \subset I \subset \mathbb{Z}^n$, and intermediate subgroups correspond to subgroups of $\mathbb{Z}^n/(q\mathbb{Z})^n$, which is finite.

Proof 2: Every such ideal I is $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_u$ (where $\mathfrak{p}_i$ are possibly non-distinct prime ideals). Then $B \geq N(I) = N(\mathfrak{p}_1) \dots N(\mathfrak{p}_u)$. Each prime has norm ≥ 2, so this is $\geq 2^u$; this bounds the number of primes. But there are also finitely many possible primes: each $\mathfrak{p}_i$ must lie above p for some prime $p \leq B$, and for each p there are at most n primes $\mathfrak{p} \mid p$. □

Theorem 18.7. *The class group is finite.*

Proof. Every element is represented by an ideal of norm $\leq m$, and there are finitely many of those. □

Corollary 18.8. $1 \leq m$

Proof. Apply Theorem 18.5 to the trivial ideal class; ideals have norm ≥ 1. □

Corollary 18.9. $\sqrt{|\operatorname{disc} \mathcal{O}_K|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}$

PROOF. Rewrite Theorem 18.5. □

By Sterling's formula, this grows exponentially with n.

Fact 18.10 (Sterling's formula)**.**

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n} \cdot e^{\theta/n}$$

where $0 < \theta < \frac{1}{12}$.

Corollary 18.11. *If $K \neq \mathbb{Q}$ then $|\operatorname{disc} \mathcal{O}_K| > 1$.*

PROOF. Estimate $a_n := \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}$. We have $a_2 = \frac{\pi}{2} > 1$, and $\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2}\left(1+\frac{1}{n}\right)^n > 1$. So all the a_n's are > 1, hence so is the discriminant. □

Corollary 18.12. *$\mathbb{Q}$ has no nontrivial unramified extension.*

Digression 18.13. The *class number* is $h_K = \#\operatorname{Pic} \mathcal{O}_K$. It is known that $h_{\mathbb{Q}(\sqrt{-d})} \to \infty$ as $d \to \infty$ (for squarefree d). But it is only conjectured that there are infinitely many squarefree $d > 0$ such that $h_{\mathbb{Q}(\sqrt{d})} = 1$. It was an open problem for a long time to find all the imaginary quadratic fields with class number 1; there were nine known ($d = -1, -3, \ldots, -163$), and it was eventually proved that there isn't a tenth.

Proposition 18.14. *$\{$Number fields K : $|\operatorname{disc} \mathcal{O}_K| < B\}$ is finite for every $B > 0$.*

PROOF. Bounding $|\operatorname{disc} \mathcal{O}_K|$ bounds $[K : \mathbb{Q}]$, so assume $[K : \mathbb{Q}] = n$ for a fixed n.

Case 1: K is totally real (i.e. all $v \mid \infty$ are real so $K_{\mathbb{R}} \cong \mathbb{R}^n$). Let

$$S := \left\{(x_1, \ldots, x_n) \in \mathbb{R}^n \,:\, |x_1| \leq 2B^{1/2} \text{ and } |x_i| < 1 \text{ for } i \geq 2\right\}.$$

Then $\operatorname{vol}(S) = 2^{n+1}B^{1/2} > 2^n |\operatorname{disc} \mathcal{O}_K|^{1/2} = 2^n \operatorname{covol}(\mathcal{O}_K)$. By Minkowski, S contains a nonzero element $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{O}_K \subset K_{\mathbb{R}} = \mathbb{R}^n$. Then $\prod_{i=1}^n |\alpha_i| = \left|N_{K/\mathbb{Q}}(a)\right| \in \mathbb{Z}_{\geq 1}$. Since $|a_i| < 1$ for $i \geq 2$, we need $|\alpha_1| > 1$.

I claim that $\mathbb{Q}(\alpha) = K$; if not, then each α_i would be repeated $[K : \mathbb{Q}(\alpha)]$ times. But $\alpha_1 \neq \alpha_2, \ldots, \alpha_n$ because their absolute values are different. So $[K : \mathbb{Q}(\alpha)] = 1$.

Look at the coefficients of the minimal polynomial of α: they are elementary symmetric functions of $\alpha_1, \ldots, \alpha_n$. But n is fixed and we have an upper bound on the size of each α_i. So the elementary symmetric functions are bounded as well. Since they are coefficients of the minimal polynomial of α, they are also integers. So there are finitely many possibilities for the coefficients, hence finitely many possibilities for the minimal polynomial, hence finitely many possibilities for α, hence finitely many possibilities for $K = \mathbb{Q}(\alpha)$.

Case 2: general case. Redefine S to be

$$S := \left\{(x_1, \dots, x_r, z_1, \dots, z_s) \in K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s \,:\, z_1 = a_1 + ib_1 \text{ satisfies } |a_1| < \frac{1}{2}, |b_1| < cB^{1/2}\right\}.$$

where c is a large constant depending on n. Now do something similar to the above. □

Lemma 18.15. *Given a prime p, $v_p(\operatorname{disc} \mathcal{O}_K)$ is bounded by some function of $n = [K : \mathbb{Q}]$.*

Proof.

$$v_p(\operatorname{disc} \mathcal{O}_K) = \sum_{v|p} v_p\left(D_{K_v}/\mathbb{Q}_p\right)$$

On the HW you proved that there are only finitely many possibilities for K_v since $[K_v : \mathbb{Q}_p] \leq n$, and there are $\leq n$ terms. □

Theorem 18.16 (Hermite's Theorem)**.** *Let S be a finite set of places, and $n \in \mathbb{Z}_{\geq 1}$. Then*

$$\{K/\mathbb{Q} \text{ of degree } n \,:\, K \text{ is unramified outside } S\}$$

is finite.

Proof. $v_p(\operatorname{disc} \mathcal{O}_K)$ is bounded for each $p \in S$, so $|\operatorname{disc} \mathcal{O}_K|$ is bounded. Now apply Proposition 18.14. □

Lecture 19: November 6

François Charles is lecturing next Thursday; no office hours next week.

There are two big theorems in basic algebraic number theory: if $[K : \mathbb{Q}] < \infty$ then

(1) $\operatorname{Pic} \mathcal{O}_K$ is finite;
(2) (Dirichlet unit theorem) $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r + s - 1$.

Last time we proved (1); this time we'll prove (2).

These are analogous to problems that are still open: finiteness of the class group is analogous to finiteness of the Shafarevitch group; (2) is analogous to the Birch and Swinnerton-Dyer conjecture.

Definition 19.1. An M_K-divisor is a function $c : M_K \to \mathbb{R}_{>0}$ sending $v \mapsto c_v$ such that:

- $c_v = 1$ for all but finitely many v;
- if v is nonarchimedean, then $c_v = |a_v|_v$ for some $a_v \in K$.

These are supposed to be values of an absolute value.

Definition 19.2. The size of c is $\|c\| := \prod c_v \in \mathbb{R}_{>0}$.

Definition 19.3. $L(c) := \{x \in K : |x|_v \le c_v \text{ for all } v\}$.

Compare with function field notation: if $D = \sum n_P P \in \operatorname{Div} X$, then $L(D) := \{f \in K : v_p(f) \ge -n_P \text{ for all } P \in X\}$.

Example 19.4. Let $K = \mathbb{Q}(i)$. Then

$$c = \begin{cases} c_{2+i} & = \frac{1}{5} \\ c_\infty & = 10 \\ c_v & = 1 \text{ for other } v \end{cases}$$

Then

$$L(c) = \{x \in (2+i) : |x|^2 \le 10\}$$

(where the $|\ |$ in the $|x|^2$ means the usual absolute value on $\mathbb{C}$). This gets lattice points on the lattice generated by $(2+i,\ i\cdot(2+i))$ inside the circle of radius $\sqrt{10}$; there are 9 points inside.

In general, there is a correspondence

$$c \longleftrightarrow \text{ fractional ideals } I \text{ together with } (c_v)_{v|\infty}.$$

Then $\|c\| = N(I)^{-1} \cdot \prod_{v|\infty} c_v$. For all $x \in K$, $x \in L(c)$ iff $x \in I$ and $|x|_v \le c_v$ for all $v \mid \infty$.

Corollary 19.5. *$L(c)$ is finite.*

Proof. I is a lattice in $K_{\mathbb{R}}$. □

Proposition 19.6. *If $B > \dfrac{\sqrt{\operatorname{disc} \mathcal{O}_K}}{2^r(2\pi)^s} \cdot 2^n$ and $\|c\| \ge B$ then $L(c)$ contains a nonzero value.*

Proof. Apply Minkowski's theorem to the lattice I and the region

$$S = \{x \in K_{\mathbb{R}} : |x|_v \le c_v \text{ for all } v \mid \infty\}$$

inside $K_{\mathbb{R}}$. Recall that $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$; the constraint puts a constraint on the absolute value of each piece.

$$\begin{aligned} \frac{\operatorname{vol} S}{\operatorname{covol} \Lambda} &= \frac{\prod_{v \text{ real}}(2c_v) \prod_{v \text{ complex}}(2\pi\sqrt{c_v}^2)}{\sqrt{|\operatorname{disc} \mathcal{O}_K|} \cdot N(I)} \\ &\ge \frac{2^r(2\pi)^s}{\sqrt{|\operatorname{disc} \mathcal{O}_K|}} \cdot B \qquad \text{using } \|c\| \ge B \end{aligned}$$

We need this to be $> 2^n$, which is what the condition says. □

In the function field case, the asymptotic version of the usual Riemann-Roch theorem says $\dim L(D) = 1 - g + \deg D$ if $\deg D$ is large. The analogous statement for number fields:

$$\#L(c) = \left(\frac{2^r(2\pi)^s}{\sqrt{|\operatorname{disc} \mathcal{O}_K|}} + o(1) \right) \cdot \|c\| \text{ as } \|c\| \to \infty.$$

PROOF. Skipped; more counting lattice points. □

I want to convert the multiplicative group structure of $\mathcal{O}_K^\times \hookrightarrow K_{\mathbb{R}}^\times$ to an additive structure; do this by taking the log. Define $\mathrm{Log} : (x_v)_{v|\infty} \mapsto (\log |x_v|)$. So now we're talking about $\mathbb{R}^{r+s}$. What does the unit group (i.e. $\mathcal{O}_K^\times$) correspond to?

Proposition 19.7. *Let* $\Lambda = \mathrm{Log}\mathcal{O}_K^\times \subset \mathbb{R}^{r+s}$.

(1) There is an exact sequence of abelian groups

$$0 \to (\mathcal{O}_K^\times)_{tors} \to \mathcal{O}_K^\times \overset{\mathrm{Log}}{\to} \Lambda \to 0.$$

(2) $(\mathcal{O}_K^\times)_{tors}$ *is finite.*
(3) Λ *is a lattice in* $\mathbb{R}^{r+s}$.

PROOF. Define ker to make

$$0 \to \ker \to \mathcal{O}_K^\times \overset{\mathrm{Log}}{\to} \Lambda \to 0$$

exact.

Claim 1: ker *is finite.* Let c correspond to $\mathcal{O}_K$, with $(2)_{v|\infty}$ (i.e. $c_v = 2$ for infinite places). Let $L(c) = \{x \in \mathcal{O}_K \,:\, |x|_v \le 2 \text{ for all } v \mid \infty\}$. For $x \in \mathcal{O}_K^\times$,

$$x \in L(c) \iff \mathrm{Log}x \in R := \{\mathbf{t} \in \mathbb{R}^{r+s} \,:\, \mathbf{t} \le (\log 2, \dots, \log 2)\}$$

(here the $\le$ is coordinate-wise) and

$$x \in \ker \iff \mathrm{Log}x = \mathbf{0}$$

Clearly, the second condition implies the first. Thus $\ker \subset L(c)$ (which is finite) so ker is finite.

Claim 2: Λ *is torsion-free.* This is because $\Lambda \subset \mathbb{R}^{r+s}$.

By Claim 2, $(\mathcal{O}_K^\times)_{tors} \subset \ker$. But by Claim 1, $\ker \subset (\mathcal{O}_K^\times)_{tors}$. This proves (1) and (2).

For (3), recall that R was made by taking the log of $L(c)$; more precisely, $\Lambda \in R = \mathrm{Log}(\mathcal{O}_K^\times \cap L(c))$, and $L(c)$ is finite, so $\Lambda \cap R$ is finite. This means that 9 is isolated in Λ, so Λ is discrete. We proved that discrete subgroups are lattices. □

Recapping the idea: look at how many units land in the rectangle R; see that finitely many land on 0, so the kernel is finite, and finitely many land in all of R, so it's discrete.

$(\mathcal{O}_K^\times)_{tors}$ is finite; it is the set of roots of unity in K (a.k.a. $\mu(K)$). The above exact sequence tells you that $\mathcal{O}_K^\times$ is a finitely generated abelian group. (Any group sandwiched between finitely generated abelian groups is a finitely generated abelian group. Actually, it turns out that the sequence splits, so you can write it as a direct sum.)

Let $H := \{\mathbf{t} \in \mathbb{R}^{r+s} \,:\, sum(\mathbf{t}) = 0\}$.

Lemma 19.8. $\Lambda \subset H$

PROOF. If $x \in \mathcal{O}_K$ and v is nonarchimedean, then $|x|_v \leq 1$. If $x \in \mathcal{O}_K^\times$ and v is nonarchimedean, then $|x|_v = 1$. Suppose $x \in \mathcal{O}_K^\times$. Then $\prod_{v|\infty} |x|_v = \prod_v |x|_v = 1$; take the log of this statement to get $sum(\mathrm{Log} x) = \sum_{v|\infty} \log |x|_v = 0$. □

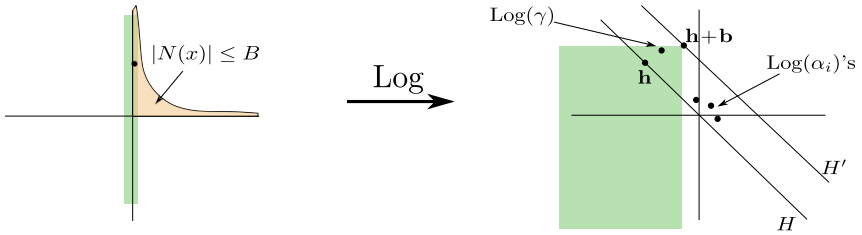
Theorem 19.9. *Λ is a full lattice in H.*

Corollary 19.10. $\Lambda \cong \mathbb{Z}^{r+s-1}$.

Corollary 19.11 (Dirichlet unit theorem)**.** *$\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r+s-1$.*

IDEA OF PROOF. You need to make units. If $x, y \in K^\times$ such that $(x) = (y)$, then $\frac{x}{y}$ is a unit. Find a lot of elements of small norm, and use the fact that the set of principal ideals of norm $\leq B$ is finite. Now use the pigeonhole principle to show that a bunch of them generate the same principal ideal. Call these principal ideals $(\alpha_1), \ldots, (\alpha_j)$, where the α_i's are elements of $\mathcal{O}_K$.

The region $\{x : |N(x)| \leq B\}$ looks like the area under a hyperbola.



If you choose a big enough box (whether it's tall and narrow or wide and short), it will contain a lattice point. Take the log of this: you get some hyperplane H' where the region below it satisfies $sum(\mathbf{t}) \leq \log B$. The boxes under the hyperbola turn into rectangles unbounded to the left under H'. Algebraic integers have norm ≥ 1, hence their logs are ≥ 0. Let H be the hyperplane $x_1 + x_2 + \cdots = 0$. We will show that, for every $\mathbf{h} \in H$, there is a lattice point nearby.

Fix $\mathbf{b}$ such that $sum(\mathbf{b}) = \log B$ (this is the same B as in Proposition 19.6). Given $\mathbf{h} \in H$, form the c corresponding to $\mathcal{O}_K$, with $e^{\mathbf{h}+\mathbf{b}}$. Then $\|c\| = B$. By Proposition 19.6, there is some nonzero $\gamma \in \mathcal{O}_K$ such that $\gamma \in L(c)$. Then $\mathrm{Log}\gamma \leq \mathbf{h} + \mathbf{b}$, so (taking the sum) $\log |N(\gamma)| \leq \log B$, so $|N(\gamma)| \leq B$. (γ) has to be some (α_i). So $\frac{\gamma}{\alpha_i} \in \mathcal{O}_K^\times$, and $\mathrm{Log}\frac{\gamma}{\alpha_i} = \mathrm{Log}\gamma - \mathrm{Log}\alpha_i \in \Lambda$, which is within a bounded amount of $\mathbf{h}$.

Conclusion: every $\mathbf{h} \in H$ is within a bounded distance of a vector in Λ. Thus Λ is a full lattice in H. □

Example 19.12. If $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ (where d is a nonsquare integer > 1), then $r = 2$, $s = 0$ (there are two ways to embed this in $\mathbb{R}$). Then $\operatorname{rank} \mathcal{O}_K^\times = 1$, $(\mathcal{O}_K^\times)_{tors} = \mu(K) = \{\pm 1\}$. So

$$\mathcal{O}_K^\times = \{\pm \varepsilon^n \,:\, n \in \mathbb{Z}\}.$$

By picking the right embedding into $\mathbb{R}$, without loss of generality $\varepsilon > 0$; also without loss of generality you can assume $\varepsilon > 1$. At this point, ε is uniquely determined. This is called the *fundamental unit*.

Lecture 20: November 13

Today we will talk about idèles and adèles, due to Chevalley.

You want to study $\mathbb{Z} \subset \mathbb{Q}$ at all the places. Temporarily forget about the infinite places. Recall $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n$; by the Chinese remainder theorem, this is $\prod_p \mathbb{Z}_p$. It is compact, since $\mathbb{Z}_p$ is compact and the product of compact sets is compact. Alternatively, a limit of finite groups is compact. But you also want to study $\mathbb{Q}$;

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \widehat{\mathbb{Z}} \\ \downarrow & & \downarrow \\ \mathbb{Q} & \hookrightarrow & \mathbb{A}_{\mathbb{Q}} \end{array}$$

The adèles $\mathbb{A}_{\mathbb{Q}}$ is the thing that fits in the bottom right.

You might want to put $\prod_p \mathbb{Q}_p$ there instead, but it is not locally compact (every point has a compact neighborhood). This is also intuitively the wrong object: any $x \in \mathbb{Z}$ is invertible except at finitely many primes. So you should be working with something smaller than $\prod_p \mathbb{Q}_p$; that is the adèles. Another reason the adèles are better than $\prod_p \mathbb{Q}_p$ is that you can do Fourier analysis on locally compact groups.

Recollections of point-set topology. A *basis* for a topology of X is a collection $(U_i)_{i \in I}$ of subsets of X such that

- for all $x \in X$ and $U_1, U_2 \ni x$, there exists U_3 with $x \in U_3 \subset U_1 \cap U_2$;
- $\bigcup_i U_i = X$.

There is a unique coarsest topology on X containing the U_i as open sets.

Product topology: Let $(X_i)_{i \in I}$ be topological spaces. The product topology on $\prod_{i \in I} X_i$ is the one with basis $\prod_{i \in I} U_i$ for opens $U_i \subset X_i$ such that $U_i = X_i$ for almost all $i \in I$ (i.e. for all but finitely many).

This is the coarsest topology such that the projections $\prod_{i \in I} X_i \xrightarrow{p_j} X_j$ are continuous. You need $p_j^{-1}(U_j) = \prod_{i \neq j} X_j \times U_j$ to be open; after taking finite intersections you get the product topology.

Theorem 20.1 (Tychonoff)**.** *The product of compact topological spaces is compact.*

(This would not work if you used the box topology!)

Warning 20.2. The product of locally compact spaces is *not* locally compact in general.

Exercise 20.3. $\prod_p \mathbb{Q}_p$ is not locally compact.

We fix this by using the *restricted product*.

Definition 20.4. Let $(X_i)_{i\in I}$ be a family of topological spaces, and for (almost) all $i \in I$ let $U_i \subset X_i$ be an open subset. (The model you should have in mind is $\mathbb{Z}_p \subset \mathbb{Q}_p$.) Define a topological space X:

- the points are $x = (x_i)_{i\in I} \in \prod X_i$ such that $x_i \in U_i$ for almost all $i \in I$
- a basis of open subsets is $\prod_{i\in I} V_i$ where $V_i \subset X_i$ is open for all i, and $V_i = U_i$ for almost all i.

We say that X is the *restricted product of the X_i's with respect to the U_i's*, and write $X = \prod_{i\in I} X_i$.

Example 20.5. The usual product is the restricted product with respect to the X_i's.

Remark 20.6. The restricted product does not depend on any single U_i, i.e. if $U_i' \subset X_i$ is open and $U_i' = U_i$ for almost all i, then the two restricted products are the same.

Corollary 20.7. *Let $S \subset I$ be a finite set. Define $X_S = \left(\prod_{i\in S} X_i\right) \times \left(\prod_{i\notin S} U_i\right) \subset X$ with the product topology. Then the inclusion $X_S \hookrightarrow X$ is continuous, the topology on X_S and the induced topology of the inclusion coincide, and X_S is open in X. Furthermore,*

$$X = \bigcup_{\substack{S\subset I \\ S \text{ finite}}} X_S.$$

Proof. Definition-chasing. □

You could have defined the restricted product using this corollary.

Proposition 20.8. *Assume that the X_i's are locally compact, and that the U_i's are compact for almost all i. Then X is locally compact.*

Proof. First I claim that X_S is locally compact for all finite S. Indeed, $X_S = \left(\prod_{i\in S} X_i\right) \times \left(\prod_{i\notin S} U_i\right)$. The first term is a finite product of locally compact spaces, hence locally compact; the second term is compact by Tychonoff's theorem.

Since the X_S's are open in X, and X_S is locally compact, $X = \bigcup X_S$ is locally compact. □

Adèles. Let k be a number field. For any (normalized) valuation v, consider the completion k_v. Let $\mathcal{O}_v \subset k_v$ be the ring of integers. There are only finitely many archimedean valuations, so we can assume that v is nonarchimedean.

Definition 20.9. Define the ring of adèles to be the restricted product of all the k_v's with respect to $\{\mathcal{O}_v : v \text{ is nonarchimedean}\}$:

$$\mathbb{A}_k = \prod_v k_v.$$

The ring structure on $\mathbb{A}_k$ is defined component-wise: elements look like $(a_v)_v$.

Exercise 20.10. Check that this is a topological ring.

Remark 20.11. $\mathbb{A}_{\mathbb{Q}}$ is the union of

$$\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p \times \prod_{\ell \notin S} \mathbb{Z}_\ell$$

as S runs through finite sets of primes.

We have a natural map $k \to \mathbb{A}_k$ induced by the maps $k \to k_v \to \prod k_v$. Why does this map into $\mathbb{A}_k$? If $x \in k$ then the set of valuations such that $v(x) < 0$ is finite (it's the set of primes that divide the denominator of x). ($\mathbb{A}_k$ is the smallest subset of $\prod k_v$ that receives a map like this.)

$\mathbb{Z} \subset \mathbb{R}$ is the setup for Fourier analysis: functions on $\mathbb{Z}$ are dual to functions on $\mathbb{R}/\mathbb{Z}$. This works because $\mathbb{Z} \subset \mathbb{Q}$ is discrete, and $\mathbb{Q}/\mathbb{Z}$ is compact. I will prove that $k \subset \mathbb{A}_k$ in a way that it is discrete, and $\mathbb{A}_k/k$ is compact. Then the Poisson summation formula, etc., works...

Definition 20.12. The principal adèles are the elements of $\mathbb{A}_k$ that lie in the image of k. We will identify these with k.

Lemma 20.13. *Let k be a number field, K/k a finite extension. Then we have a canonical homeomorphism*

$$\mathbb{A}_k \otimes_k K = \mathbb{A}_K.$$

Proof. Write $K = k\omega_1 \oplus \ldots \oplus k\omega_n$ as a k-vector space. Then

$$LHS = \prod_v k_v \otimes K \text{ with respect to } \mathcal{O}_v \otimes K.$$

Indeed, $k_v \otimes K = k_v\omega_1 \oplus \ldots \oplus k_v\omega_n$ and $\mathcal{O}_v \otimes K = \mathcal{O}_v\omega_1 \oplus \ldots \oplus \mathcal{O}_v\omega_n$. Furthermore, $k_v \otimes K = \bigoplus_i K_{V_i}$, where the V_i are the valuations of K lying over v. Then $\mathcal{O}_v \otimes K = \bigoplus \mathcal{O}_{V_i}$. As a consequence, LHS = RHS. □

Theorem 20.14. *k is discrete in $\mathbb{A}_k$, and the quotient of abelian groups $\mathbb{A}_k/k$ is compact.*

PROOF. k is a finite extension of $\mathbb{Q}$.

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathbb{A}_{\mathbb{Q}} \\ \downarrow & & \downarrow \\ k = k \otimes \mathbb{Q} & \hookrightarrow & \mathbb{A}_k = \mathbb{A}_{\mathbb{Q}} \otimes k \end{array}$$

By the lemma above, it suffices to prove this for the top row, i.e. we can assume that $k = \mathbb{Q}$.

Idea: the only non-compactness comes from the finite number of k factors; so once you mod out by k, it's compact.

By the lemma above, we can assume $k = \mathbb{Q}$. To show $\mathbb{Q}$ is discrete in $\mathbb{A}_{\mathbb{Q}}$, it suffices to prove that 0 is isolated. Consider the open set of $\mathbb{A}_{\mathbb{Q}}$ consisting of $(\alpha_v)_v$ such that $|\alpha_\infty| < 1$ and $|\alpha_p|_p \leq 1$ (this means that $\alpha_p \in \mathbb{Z}_p$). Let $x \in \mathbb{Q}$ satisfy these inequalities. Write $x = \frac{a}{b}$ for $b > 0$ and $(a, b) = 1$. Then for any p, $p \nmid b$ because $v_p(x) \geq 0$. So $b = 1$, and $x \in \mathbb{Z}$. Since $|x|_\infty < 1$, we have $x = 0$. (So 0 is the only element of $\mathbb{Q}$ in this neighborhood.)

Now we show that $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact. Define

$$W = \left\{(\alpha_v)_v \,:\, |\alpha_\infty| \leq \tfrac{1}{2},\ |\alpha_p|_p \leq 1\ \forall p\right\}.$$

This is open in $\mathbb{A}_{\mathbb{Q}}$.

Claim 20.15. *W is compact, and W surjects onto $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$.*

PROOF. W is the product of $[-\frac{1}{2}, \frac{1}{2}] \subset \mathbb{R}$ and $\prod_p \mathbb{Z}_p$. It is compact, because it is the product of compact spaces.

To show that W surjects onto $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$, for any $\beta \in \mathbb{A}_{\mathbb{Q}}$ we need to find $\alpha \in W$ and $b \in \mathbb{Q}$ such that $\beta = \alpha + b$. I have a bunch of p-adic numbers that are in $\mathbb{Z}_p$ for almost all p. For any p, choose $r_p = z_p/p^{n_p}$, where $z_p \in \mathbb{Z}$ and $|\beta_p - r_p|_p \leq 1$ (where β_p is the p-component of β). (Idea: I can translate β by $\mathbb{Q}$ so that it becomes a p-adic integer for a given p.) We can assume that $r_p = 0$ for almost all p, because β_p already satisfies the condition $|\beta_p|_p \leq 1$ for almost all p.

Let $r = \sum_p r_p$. Then, for all p, $|\beta_p - r|_p \leq 1$, and $|\beta_p - r|_p = \big|\beta_p - r_p + \underbrace{(r_p - \sum_q r_q)}_{\in \mathbb{Z}_p}\big|$. Now let s be such that $|\beta_\infty - r - s| \leq \frac{1}{2}$. Then $\beta - r - s \in W$. □

Thus $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact (it's the image of a compact set). □

LECTURE 21: NOVEMBER 18

Inside $\Lambda \subset \mathbb{R}^{r+s}$ is H, the space of sum zero. What is the metric on this? Choose any coordinate projection $\pi : \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$; restricting to H defines an isomorphism $H \cong$

$\mathbb{R}^{r+s-1}$, and this isomorphism gives a metric on H. The lattice in H turns into a lattice in $\mathbb{R}^{r+s-1}$ under this identification.

Definition 21.1. The *regulator* of K is $R := \mathrm{covol}(\pi(\Lambda))$; this is independent of the choice of π.

If $\varepsilon_1, \dots, \varepsilon_{r+s-1} \in \mathcal{O}_K^\times$ form a basis for $\mathcal{O}_K^\times/\text{torsion}$, consider

$$\begin{pmatrix} \vdots & \vdots \\ \mathrm{Log}\varepsilon_1 & \mathrm{Log}\varepsilon_n \\ \vdots & \vdots \end{pmatrix} \in M_{(r+s)\times(r+s-1)}(\mathbb{R});$$

then $R = |\text{any } (r+s-1)\times(r+s-1) \text{ minor}|$.

Proof of the strong approximation theorem using adèles. Last time, we had a global field K and defined the adèle ring $\mathbb{A} = \mathbb{A}_K$, which I will be writing as $\prod'(K_v, \mathcal{O}_v)$ instead of $\prod$. This is a topological ring. There is a natural inclusion $K \subset \mathbb{A}$, which makes K discrete and *cocompact* (i.e. $\mathbb{A}/K$ is compact). This is just like $\mathbb{Z} \subset \mathbb{R}$, or $\mathcal{O}_K \subset K_{\mathbb{R}}$. We showed that there is a compact set that surjects onto $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$, namely $W = [-\frac{1}{2}, \frac{1}{2}] \times \prod_p \mathbb{Z}_p$ (this is called an "adèlic box" – you're bounding every absolute value). Similarly, in general there is a surjection

$$W := \{(x_v)v \in \mathbb{A} : |x_v|_v \le c_v \ \forall v\} \twoheadrightarrow \mathbb{A}_K/K$$

for a suitable M_K-divisor c.

This all means that $\mathbb{A} = K + W$ (imagine a lattice in $\mathbb{R}^2$, and a sufficiently large box, such that if you translate the box by all lattice points, it covers $\mathbb{R}^2$).

We can finally give a proof of the strong approximation theorem:

Theorem 21.2 (Strong approximation theorem)**.** *Given a global field K. Choose a finite set S and a set T such that*

$$\{\textit{places of } K\} = S \sqcup \{w\} \sqcup T.$$

If $a_v \in K$ for $v \in S$ and $\varepsilon_v \in \mathbb{R}_{>0}$ for $v \in S$, then there exists $x \in K$ such that $|x - a_v|_v \le \varepsilon_v$ for all $v \in S$, and $|x|_v \le 1$ for all $v \in T$. (Note that there is no condition at w.)

Proof. Recall $W = \{(x_v) \in \mathbb{A} : |x_v|_v \le c_v \ \forall v\}$.

We have $\mathbb{A} = K + w$; multiply by some $u \in K^\times$ to get $\mathbb{A} = K + uW$; this changes the dimensions of W (without changing its volume) – it multiplies the v-component by $|u_v|$. Since there's no constraint at w, the idea is to make the w direction really long so that the other dimensions can be bounded.

We can choose $u \in K^\times$ so that $|u|_v \le \varepsilon_v c_v^{-1}$ and $|u|_v \le c_v^{-1}$ for all $v \in T$. Then make $|u|_w \le$ some really big number. This defines an adèlic box defined by an M_K-divisor of arbitrarily large size (gotten by making the big number really big).

Then

$$uW \subset \left\{ (y_v)_v \in \mathbb{A} \,:\, |y_v|_v \leq \begin{array}{l} \varepsilon_v \text{ for } v \in S \\ 1 \text{ for } v \in T \end{array} \right\}.$$

Now $\mathbb{A} = K + uW$; apply this to (a_v), extended to an adèle by defining $a_v = 0$ for $v \notin S$. Then $|x - a_v|_v = |y_v| \leq \begin{cases} \varepsilon_v & \text{if } v \in S \\ 1 & \text{if } v \in T. \end{cases}$ □

This is strong approximation for the additive group, but there are generalizations; see the survey of A. Rapinchuk, *On strong approximation for algebraic groups.*

Idèles. Historically, idèles came before adèles; it was a word that was supposed to sound like "ideal". Adèles were then "additive idèles".

Digression 21.3. If $\mathbb{Q}_p^{ab}$ denotes the maximum abelian extension, then $\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ is "approximately" $\mathbb{Q}_p^\times$ (you have to do some compactification). Analogously, $\mathrm{Gal}(K^{ab}/K)$ is approximately $\mathbb{A}^\times/K^\times$. This is the 1-dimensional case of the Langlands conjecture, which is about representations of the Galois group (1-dimensional representations are abelian).

Definition 21.4. The idèle group is $\mathbb{A}^\times = \prod'(K_v^\times, \mathcal{O}_v^\times)$.

What is the topology of $\mathbb{A}^\times$?

In general, suppose you have a topological ring R, and you want to make $R^\times$ into a topological ring. Naively, you might want to give it the subspace topology. But then, in general, you don't get a topological group (the inverse map might not be continuous).

Instead, view $R^\times$ as the subset defined by $xy = 1$ in $R \times R$, via $x \mapsto (x, x^{-1})$, and use the subspace topology of the product topology on $R \times R$. This forces the inverse map to be continuous, because it comes from swapping the coordinates on $R \times R$, which is continuous under the product topology.

So we now know how to define a topology on $\mathbb{A}^\times$. You could also give it the *restricted direct product topology*, where the basic open sets are $\prod_v U_v$ such that U_v is an open subset of $K_v^\times$ (it turns out the subspace topology is OK for K_v) and $U_v = \mathcal{O}_v^\times$ for all but finitely many v.

$\mathcal{O}_v^\times$ is closed in $\mathcal{O}_v$ for all $v \nmid \infty$, so $\mathcal{O}_v^\times$ is compact, so $\mathbb{A}^\times$ is locally compact.

Just as K embeds in $\mathbb{A}$, $K^\times$ embeds in $\mathbb{A}^\times$, sending $a \mapsto (\dots, a, a, a, \dots)$.

Proposition 21.5. *$K^\times$ is a discrete subgroup of $\mathbb{A}^\times$ (and it is a general topology fact that discrete subgroups of topological groups are closed).*

Proof. $K \times K$ is discrete inside of $\mathbb{A} \times \mathbb{A}$, and $K^\times$ is a subset of $K \times K$. □

Question 21.6. Is $K^\times$ a lattice in $\mathbb{A}^\times$? We just need the quotient to be compact. (This is asking whether you approximate any idèle by something in $K^\times$.)

Answer: no, for the same reason that $\mathbb{R}^{r+s}/\mathrm{Log}\mathcal{O}_K^\times$ is not compact: there is one infinite direction still left over. This is because of the product formula.

There is a map $\mathbb{A}^\times \to \mathbb{R}_{>0}^\times$ given by taking $a = (a_v) \mapsto \|a\| := \prod_v |a_v|_v$.

Definition 21.7. $(\mathbb{A}^\times)^1 = \{a \in \mathbb{A}^\times : \|a\| = 1\}$

The product formula is equivalent to saying $K^\times \subset (\mathbb{A}^\times)^1$.

Theorem 21.8. $(\mathbb{A}^\times)^1/K^\times$ *is compact.*

Modulo a lot of snake lemma, this is roughly equivalent to the unit theorem and the finiteness of the class group, together.

Proof. Let P_K be the group of principal fractional ideals. Clearly, the units are the kernel of the map $K^\times \to P_K$. Similarly, we have a map $(\mathbb{A}^\times)^1 \to \mathcal{I}_K$ given by taking $(a_v) \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$. This makes sense, because $a_v \in \mathcal{O}_v^\times$ for almost all v, and that means its valuation is zero. So this is actually a finite product. What is the kernel? This map doesn't even look at the infinite places, so there has to be a factor of $\prod_{v|\infty} K_v^\times$ in the kernel. But at the nonarchimedean places, the things in the kernel are $\mathcal{O}_v^\times$. I also need to put a "size 1" condition on the kernel; this is the same as imposing $(\prod_{v|\infty} K_v^\times)^1 \times \prod_{v\nmid\infty} \mathcal{O}_v^\times$.

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & P_K & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_{v|\infty} K_v^\times)^1 \times \prod_{v\nmid\infty} \mathcal{O}_v^\times & \longrightarrow & (\mathbb{A}^\times)^1 & \longrightarrow & \mathcal{I}_K & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathrm{coker} & \longrightarrow & (\mathbb{A}^\times)^1/K^\times & \longrightarrow & \mathrm{Pic}\,\mathcal{O}_K & \longrightarrow & 0
\end{array}$$

The snake lemma gives an exact sequence

$$0 \to \mathrm{coker} \to (\mathbb{A}^\times)^1/K^\times \to \mathrm{Pic}\,\mathcal{O}_K \to 0.$$

Since $\mathrm{Pic}\,\mathcal{O}_K$ is finite, it suffices to show that the thing labeled "coker" (by which I mean the cokernel of $\mathcal{O}_K^\times \to (\prod_{v|\infty} K_v^\times)^1 \times \prod_{v\nmid\infty} \mathcal{O}_v^\times$) is compact.

You can do Log to the archimedean places (and forget the other ones) of $(\prod_{v|\infty} K_v^\times)^1 \times \prod \mathcal{O}_v^\times \xrightarrow{\text{Log}} (\mathbb{R}^{r+s})^0 = H$.

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & \mu_K & \longrightarrow & \mathcal{O}_K^\times & \xrightarrow{\text{Log}} & \Lambda & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_{v|\infty}(K_v^\times)^1 \times \prod_{v\nmid\infty} \mathcal{O}_v^\times & \longrightarrow & (\prod_{v|\infty} K_v^\times)^1 \times \prod_{v\nmid\infty} \mathcal{O}_v^\times & \xrightarrow{\text{Log}} & (\mathbb{R}^{r+s})^0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & X & \longrightarrow & \text{coker} & \longrightarrow & H/\Lambda & \longrightarrow & 0
\end{array}$$

The resulting snake exact sequence is

$$0 \to X \to \text{coker} \to H/\Lambda \to 0. \tag{21.1}$$

Actually $\prod_{v|\infty}(K_v^\times)^1$ is easy to understand; each K_v is either $\mathbb{R}$ or $\mathbb{C}$, and $(K_v^\times)^1$ is $\{\pm 1\}$ in $\mathbb{R}$ or $\{z : |z| = 1\}$ in $\mathbb{C}$. These are compact, and so are $\mathcal{O}_v^\times$ (closed subsets of compact things). So the thing marked X is the image of something compact, hence it's compact.

The Dirichlet unit theorem says that H is a full lattice; so H/Λ is compact.

So (21.1) puts coker in a compact sandwich. □

Cyclotomic fields. Let k be any field, and $n \in \mathbb{Z}_{\geq 1}$ such that $\text{char}\, k \nmid n$. Then $x^n - 1$ is separable over k (the derivative of nx^{n-1}, and it's pretty easy to work out the roots of this, and check that they're not roots of $x^n - 1 \ldots$). So its splitting field L is Galois (= normal + separable) over k. $\mu_n = \{x \in L : x^n = 1\}$ is a group of order n. Finite subgroups of $L^\times$ for any field are cyclic, so μ_n is generated by some $\zeta \in L$ (a primitive n^{th} root of 1). Now $L = K(\zeta)$.

You get a homomorphism $\text{Gal}(L/k) \hookrightarrow \text{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ taking $\sigma \mapsto$ the a such that $\sigma(\zeta) = \zeta^a$. But this is not always surjective (e.g. if $k = \mathbb{C}$ and $n > 2$, because then $L = \mathbb{C}$ and $\text{Gal}(L/k) = 1$).

But as a corollary of this injectivity:

Corollary 21.9. *L/k is abelian (i.e. its Galois group is abelian).*

In $L[x]$:

$$x^n - 1 = \prod_{\alpha^n = 1} (x - \alpha) = \prod_{d|n} \prod_{\substack{\alpha \text{ of exact} \\ \text{order } d}} (x - \alpha).$$

Definition 21.10. $\Phi_d(x) = \prod_{\substack{\alpha \text{ of exact} \\ \text{order } d}} (x - \alpha)$ i called the d^{th} cyclotomic polynomial.

$$\begin{aligned}\deg \Phi_d(x) &= \text{the number of elements of order } d \text{ in a cyclic group of order } n \\ &= \#(\mathbb{Z}/n\mathbb{Z})^\times \\ &= \varphi(n) \qquad \text{(Euler phi function)}\end{aligned}$$

Example 21.11. Let's calculate $\Phi_{12}(x)$. Start by dividing by the things of order 4 and order 6: $\frac{x^{12}-1}{(x^6-1)(x^4-1)}$; but you've double-counted some things, so you have to multiply by x^2-1:

$$\Phi_{12}(x) = \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} = x^4 - x^2 + 1.$$

Lecture 22: November 20

Continuing from last time: we had a field k and an integer $n \geq 1$ where $\operatorname{char} k \nmid n$; we were talking about $L = k(\zeta)$ where ζ was a primitive n^{th} root of 1. We talked about the cyclotomic polynomial $\Phi_d(x) := \prod_{\substack{\alpha \in \overline{k} \text{ of exact} \\ \text{order } d}} (x - \alpha)$, and found that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

You can use this to solve for Φ_n inductively.

Here is a special case of the Möbius inversion formula:

$$\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)} \quad \text{where } \mu(d) := \begin{cases} (-1)^r & \text{if } d \text{ is a product of } r \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

μ is called the Möbius μ-function. This is a generalization of the computation of Φ_{12} last time.

Theorem 22.1. $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ *is an isomorphism.*

$\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n) = \deg \Phi_n(x)$ and $\#\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\text{minimal polynomial of } \zeta)$. The theorem is equivalent to saying that these orders are equal; since ζ is a root of Φ_n, the only way to get equality is if $\Phi_n =$ the minimal polynomial, and this only happens if $\Phi_n(x)$ is irreducible. Thus we have the equivalent formulation:

Theorem 22.2. Φ_n *is irreducible over* $\mathbb{Q}$.

Lemma 22.3. *If* $p \nmid n$, *then* $\mathbb{Q}(\zeta)/\mathbb{Q}$ *is unramified above* p, *and* $\operatorname{Frob}_p \in G := \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ *maps to* p *in* $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. $x^n - 1 \in \mathbb{F}_p[x]$ is separable (by checking the derivative), so $\mathbb{Q}(\zeta)/\mathbb{Q}$ is unramified above p. Let q be a prime of $\mathbb{Q}(\zeta)$ over $p \in \mathbb{Z}$. (We will show that the ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$ but that is not obvious.) Recall the decomposition group $D_q := \{\sigma \in G : \sigma(q) = q\}$

satisfies

$$1 \to I_q \to D_q \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \to 1$$

(where I_q is the inertia group). $|I_q| = e_q$ and $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = f_q$ by definition, so $|D_q| = e_q f_q$. We know that p is unramified, so $e_q = 1$ and $D_q \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is an isomorphism. (Since this is Galois, we could be writing e_p instead of $e_q \dots$) $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic, generated by Frobenius $x \mapsto x^p$, which has order f_q. Define Frob_q to be the unique element of D_q that maps to this.

In general, if you have two subgroups that are defined as stabilizers of a single point, they are conjugate. So $\{\mathrm{Frob}_q : q \mid p\}$ is a conjugacy class in G, but G is abelian, and any conjugacy class has just one element; call it Frob_p.

Frob_p is characterized by $\mathrm{Frob}_p(x) \equiv x^p \pmod{q}$ for all $x \in \mathcal{O}_{\mathbb{Q}(\zeta)}$. In particular, $\mathrm{Frob}_p(\zeta) \equiv \zeta^p \pmod{q}$.

On the other hand, Frob_p maps to some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, defined by $\mathrm{Frob}_p(\zeta) = \zeta^a$. Then $\zeta^a \equiv \zeta^p \pmod{q}$. Since $x^n - 1$ has distinct roots mod p, there is a bijection between roots in the residue field and roots in $\mathbb{Q}(\zeta)$, so we have $\zeta^a = \zeta^p$. □

Proof of Theorem 22.1. We're trying to show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is a surjection. The lemma tells us that we can hit every prime $p \nmid n$.

Start with some $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, and lift it to $a \in \mathbb{Z}_{>0}$. Then a is a product of primes $p \nmid n$. By the lemma, each p is in the image of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. □

Corollary 22.4. *If $p \nmid n$, then $f_p =$ order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Also, $e_p = 1$ and $g_p = \varphi(n)/f_p$.*

Proof.

$$\begin{aligned} f_p = [\mathbb{F}_q : \mathbb{F}_p] = &\text{ the order of the generator } (x \mapsto x^p) \text{ of } \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \\ = &\text{ the order of } \mathrm{Frob}_p \text{ in } D_p \subset G \\ = &\text{ the order of } p \text{ in } (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

□

Theorem 22.5. $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$

Proof. By induction on the number of prime factors of n.

Base case: no prime factors (i.e. $n = 1$). Duh.

Inductive step: suppose $n = mp^r$ where $p \nmid m$ and suppose that the result is true for m. Choose ζ_m and ζ_{p^r}, and take $\zeta_n = \zeta_m \zeta_{p^r}$. Consider the tower of extensions

$$\begin{array}{c} K(\zeta_{p^r}) = \mathbb{Q}(\zeta_n) \\ | \\ K = \mathbb{Q}(\zeta_m) \\ | \\ \mathbb{Q} \end{array}$$

By induction, $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.

Claim 22.6. *$\mathcal{O}_K[\zeta_{p^r}]$ is integrally closed.*

Proof. Check locally at each prime $\mathfrak{q}$ of $\mathcal{O}_K$.

Case 1: $\mathfrak{q} \mid p$. Consider $\Phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$ (baby case of Möbius inversion formula). As in one of the HW solutions, $\Phi_{p^r}(x+1)$ is Eisenstein over $\mathbb{Z}_{(p)}$, hence it's Eisenstein over $(\mathcal{O}_K)_{\mathfrak{q}}$ – since $\mathfrak{q}$ unramified in $K/\mathbb{Q}$, the valuation on $(\mathcal{O}_K)_{\mathfrak{q}}$ restricts to the valuation on $\mathbb{Q}_p$. Thus $\mathcal{O}_K[\zeta_{p^r}]_{\mathfrak{q}}$ is integrally closed for all $\mathfrak{q} \mid p$ (see the discussion after Corollary 7.11).

Case 2: λ is a prime of $\mathcal{O}_K$ above a prime $\ell \neq p$. Then $x^{p^r} - 1 \pmod{\ell}$ is a separable polynomial, hence $\Phi_{p^r}(x) \pmod{\ell}$ is separable, hence $\Phi_{p^r}(x) \pmod{\lambda}$ is separable, hence $\mathcal{O}_K[\zeta_{p^r}]_{\lambda}$ is integrally closed (again by after Corollary 7.11). □

Thus

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathcal{O}_{K(\zeta_{p^r})} \overset{\text{Claim}}{=} \mathcal{O}_K[\zeta_{p^r}] \overset{\text{ind. hyp.}}{=} \mathbb{Z}[\zeta_m][\zeta_{p^r}] = \mathbb{Z}[\zeta_n].$$

□

Zeta functions. References for analytic number theory:

- Davenport, *Multiplicative number theory* (more depth)
- Serre, *A course in arithmetic*

The Riemann zeta function is

$$\begin{aligned} \zeta(s) &= \prod_{\text{primes } p} \frac{1}{1-p^{-s}} \\ &= \prod_p (1 + p^{-s} + p^{-2s} + \dots) \\ &= \sum_{n \geq 1} n^{-s} \qquad \text{by unique factorization} \end{aligned}$$

for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ (in which case all of the above converges). It's like a "generating function for the primes". Things like $\prod \frac{1}{1-p^{-s}}$ are called Euler products.

There is a generalization to number fields K: the Dedekind zeta function is

$$\begin{aligned}\zeta_K(s) &= \prod_{\substack{\text{nonzero primes} \\ \mathfrak{p} \text{ of } \mathcal{O}_K}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \\ &= \sum_{\substack{\text{nonzero ideals} \\ I \subset \mathcal{O}_K}} N(I)^{-s}\end{aligned}$$

for $\operatorname{Re} s > 1$ (here N is the ideal norm; recall $N(\mathfrak{p}) = \#\mathcal{O}_K/\mathfrak{p}$).

Even more generally, suppose X is a scheme of finite type over $\operatorname{Spec} \mathbb{Z}$ (e.g. varieties over $\mathbb{F}_q$, since $\mathbb{F}_q$ is a finitely generated $\mathbb{Q}$-algebra) then define

$$\zeta_X(S) := \prod_{\substack{\text{closed points} \\ P \text{ of } X}} \frac{1}{1 - \#\kappa(P)^{-s}}.$$

for $\operatorname{Re} s > \dim X$. Here $\kappa(P)$ is the residue field; the arithmetic version of the Nullstellensatz says that this is finite.

Back to the Riemann zeta function. As $s \to 1^+$ (i.e. approaches along the positive real axis from the right), $\zeta(s) \to \sum \frac{1}{n} = \infty$ by the monotone convergence theorem. We also have $\log \zeta(s) = \sum_p -\log(1 - p^{-s}) \to +\infty$. Use the fact that $-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots = x + O(x^2)$ as $x \to 0$ to show that $\log \zeta(s) = \sum_p p^{-s} + \sum_p O(p^{-2s}) \le \sum_p p^{-s} + \sum_p O(p^{-2})$ so the error term converges: it's $O(1)$, bounded as $s \to 1$. So $\sum p^{-s} \to \infty$ as $s \to 1^+$.

(Aside about logs: we're just taking log on the positive real line, but in fact, log makes sense on all of the domain in question. It's easy to see that $\frac{1}{1-p^{-s}}$ is a nonzero complex function, and since the domain is simply connected, there is a well-defined branch of the logarithm.)

Corollary 22.7. *$\sum \frac{1}{p}$ diverges.*

Corollary 22.8. *There are infinitely many primes.*

The goal is to say something about the growth rate.

Eventually we will prove that $\zeta(s)$ extends to a meromorphic function on $\mathbb{C}$, with a simple pole at $s = 1$ and no other poles.

For now, we'll extend it up to the vertical line $s = 0$:

Proposition 22.9. *For $\operatorname{Re} s > 1$,*

$$\zeta(s) = \frac{1}{s-1} + \varphi(s),$$

where $\varphi(s)$ extends to a holomorphic function on the domain where $\operatorname{Re} s > 0$.

PROOF. I want to prove that $\zeta(s) - \frac{1}{s-1}$ extends to a holomorphic function. For $\operatorname{Re} s > 1$:

$$\begin{aligned}\zeta(s) - \frac{1}{s-1} &= \sum_{n\geq 1} n^{-s} - \int_1^\infty x^{-s}dx \\ &= \sum_{n\geq 1} n^{-s} - \sum_{n=1}^\infty \int_n^{n+1} x^{-s}dx \\ &= \sum_{n\geq 1} \underbrace{\int_n^{n+1} (n^{-s} - x^{-s})dx}_{\varphi_n(s)}\end{aligned}$$

I want $\sum_n \varphi_n(s)$ to extend to a holomorphic function. Each summand is clearly OK on its own.

Claim 22.10. $|\varphi_n(s)| \leq \frac{|s|}{n^{\operatorname{Re} s+1}}$

Out of time; finish later. □

LECTURE 23: NOVEMBER 25

Facts about $\zeta(s)$ (not all of these will be proven this term):

- there's a meromorphic continuation to $\mathbb{C}$ (next semester, or see Ahlfors' complex analysis book)
- and this has a simple pole at 1 and no other poles;
- there's a functional equation relating $\zeta(s)$ to $\zeta(1-s)$
- which shows that there are "trivial zeros" at -2, -4, -6, ...
- and that all other zeros lie in the "critical strip" $0 < \operatorname{Re} s < 1$.
- (Riemann hypothesis) All other zeros lie on the "critical line" $\operatorname{Re} s = \frac{1}{2}$.

If there was a nontrivial zero off the critical line, then there would be one nearby, across the critical line (using the functional equation and invariance of ζ by complex conjugation). So you can check this numerically by taking the contour integral in a box around part of the critical line and counting how many zeros are inside. If there's just one, then it has to be on the critical line.

Last time we were in the middle of proving

Proposition 23.1. *$\zeta(s) = \frac{1}{s-1} + \varphi(s)$ where $\varphi(s)$ extends to a holomorphic function for $\operatorname{Re} s > 0$.*

PROOF. For $\operatorname{Re} s > 1$, we showed that

$$\zeta(s) - \frac{1}{s-1} = \sum_{n\geq 1} \underbrace{\int_n^{n+1} (n^{-s} - x^{-s})dx}_{\varphi_n(s)}.$$

We're worried about convergence of the sum; so we need to estimate $|\varphi_n(s)|$:

Claim 23.2. $|\varphi_n(s)| \le \frac{|s|}{n^{\operatorname{Re} s+1}}$

Proof. By the fundamental theorem of calculus ("in reverse"),

$$n^{-s} - x^{-s} = \int_x^n -st^{-s-1}dt.$$

The absolute value of the integrand depends only on the real part of s. For $x \in [n, n+1]$,

$$|n^{-s} - x^{-s}| \le \int_n^x \frac{|s|}{n^{\operatorname{Re} s+1}}dt \le \frac{|s|}{n^{\operatorname{Re} s+1}}.$$

□

By the claim and the Weierstrass M-test, $\sum_{n\ge1} \varphi_n(s)$ converges uniformly in $\operatorname{Re} s \ge \varepsilon$ for any $\varepsilon > 0$ (you can't say that it converges for $\operatorname{Re} s > 0$, because you need to (temporarily) fix an upper bound $\varepsilon \ne 0$). A uniformly convergent sum of holomorphic functions is holomorphic, so $\sum_{n\ge1} \varphi_n(s) =: \varphi(s)$ is holomorphic for $\operatorname{Re} s > 0$. □

Recall from last lecture that $\log \zeta(s) = \sum_p p^{-s} + O(1)$ as $s \to 1^+$, and $\log \zeta(s) \to \infty$. (From this we deduced that there are infinitely many primes.)

Theorem 23.3 (Dirichlet's theorem on primes in arithmetic progressions)**.** *If* $\gcd(a, m) = 1$ *then there are infinitely many primes* $\equiv a \pmod m$*.*

As a warm up, let's try to find primes $\equiv 1 \pmod 4$. As a first try, consider

$$\prod_{p\equiv1 \pmod 4} \frac{1}{1-p^{-s}} = \sum_{\substack{n=p_1\cdots p_k \\ \text{s.t. } p_i\equiv1 \pmod 4}} n^{-s}.$$

But the RHS is hard to do analysis on. Instead, define the *Dirichlet character*

$$\chi(n) := \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{if } n \text{ is even} \end{cases}$$

and

$$L(s,\ \chi) := \prod_p \frac{1}{1-\ \chi(p)p^{-s}} = \sum_{n\ge1}\ \chi(n)n^{-s} = 1^{-s} - 3^{-s} + 5^{-s} - 7^{-s} + \dots.$$

This is much easier to analyze.

Then

$$\begin{aligned} \log L(s,\ \chi) &= \sum_p\ \chi(p)p^{-s} + O(1) && \text{as } s \to 1^+ \\ &= \sum_{p\equiv1 \pmod 4} p^{-s} - \sum_{p\equiv3 \pmod 4} p^{-s} + O(1) \end{aligned}$$

On the other hand,

$$\log \zeta(s) = \sum_{p \equiv 1 \pmod 4} p^{-s} + \sum_{p \equiv 3 \pmod 4} p^{-s} + O(1)$$

so

$$\frac{\log \zeta(s) + \log L(s, \chi)}{2} = \sum_{p \equiv 1 \pmod 4} p^{-s} + O(1)$$

We need the LHS to go to ∞ as $s \to 1^+$. We know that $\log \zeta(s) \to \infty$, but we're worried that these might cancel out. We will show that $\log L(\chi, s)$ remains bounded as $s \to 1^+$. (I.e. we need to show that $L(\chi, s)$ tends to something nonzero.) Eventually, we'll show that $L(s, \chi)$ extends to a holomorphic function near 1 (unlike $\zeta(s)$) and $L(1, \chi) \neq 0$. This is hard – it is basically the content of Dirichlet's theorem.

Let's do this more generally. χ above was a *mod 4 Dirichlet character*; a *mod m Dirichlet character* is a homomorphism

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Extend it to a function $\chi : \mathbb{Z}_{>0} \to \mathbb{C}$ by setting $\chi(n) = 0$ whenever n is not a unit mod m (i.e. whenever $\gcd(n, m) > 1$).

Characters of finite abelian groups. Let G be a finite abelian group. The *character group* is

$$\widehat{G} := \mathrm{Hom}(G, \mathbb{C}^\times).$$

(Since every element in G has finite order, these will all land in S^1.) This group is noncanonically isomorphic to G. (Why? This is true if G is cyclic – the n^{th} roots of unity is cyclic of order n, and the noncanonical-ness is because you have to choose a generator. This is compatible with products.)

Digression about Artin L-functions 23.4. If the group is not abelian, you need to look at all irreducible representations, not just the 1-dimensional ones. (For abelian groups, all irreducible representations are 1-dimensional.) But you can define Artin L-functions for higher-dimensional representations (the group in question is usually a Galois group). Consider $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(V)$ (in the abelian case case, this would be the composition $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$). The Artin L-function is $\prod_p \frac{1}{\det(1 - \rho(\mathrm{Frob}_p)|_{V^{I_p}} p^{-s})}$ (you have to restrict to the subspace fixed by the inertia subgroup I_p).

Let $\mathbb{1}$ denote the trivial character (the one that is 1 everywhere).

Proposition 23.5. *For $\chi \in \widehat{G}$,*

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G & \text{if } \chi = \mathbb{1} \\ 0 & \text{if } \chi \neq \mathbb{1}. \end{cases}$$

Proof. If $\chi \neq \mathbb{1}$, choose $a \in G$ such that $\chi(a) \neq 1$. Let $S = \sum_g \chi(g)$. Then $\chi(a)S = \sum_g \chi(ag) = \sum_{h \in G} \chi(h) = S$ (where the second equality is because $\{ag\}_{g \in G}$ also runs through all the elements of G). So $S = 0$. □

Proposition 23.6. *For $g \in G$,*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} \#G & \text{if } g = 1 \\ 0 & \text{otherwise.} \end{cases}$$

This is the same as the previous proposition, if you replace G by $\widehat{G}$.

Corollary 23.7.

$$\frac{1}{\#G} \sum_{\chi} \chi(g) = \begin{cases} 1 & \text{if } g = 1 \\ 0 & \text{otherwise.} \end{cases}$$

This gives a way to test whether a group element is trivial or not.

You can also use this to prove a Fourier inversion formula (this is on the HW).

In the following, χ will be a mod m Dirichlet character.

Definition 23.8. The Dirichlet L-function is

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

If $\chi = \mathbb{1}$, you don't quite get back the Riemann zeta function (because it's zero when $\gcd(m, p) \neq 1$); instead, $\zeta(s) = L(s, \mathbb{1}) \prod_{p|m} \frac{1}{1-p^{-s}}$. But if you're looking at the behavior as $s \to 1$, the extra factor tends to some nonzero constant, so it doesn't interfere with any of the asymptotics we'll be dealing with. You're supposed to think of $L(s, \mathbb{1})$ as "essentially the Riemann zeta function".

Proposition 23.9. *If $\chi \neq \mathbb{1}$, then $L(s, \chi)$ extends to a holomorphic function for $\operatorname{Re} s > 0$.*

Proof. By "summation by parts" (think of this as integration with delta functions). The idea is to take $L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s}$ and "integrate" $\chi(n)$ and "differentiate" n^{-s}. Let $T(x) = \sum_{n<x} \chi(n)$. Since $T(x)$ is periodic mod m, it is bounded. (E.g. for the mod 4 Dirichlet character considered above, we have $T(x) = 0$ for $x \in (4n-1, 4n+1]$ and 1 for $x \in (4n+1, 4n+3]$.)

I'm going to do something kind of sketchy: you can make this rigorous using Stieltjes integrals.

$$\begin{aligned} L(s,\ \chi) &= \sum_{n \geq 1} n^{-s}\ \chi(n) \\ &= \int_1^\infty x^{-s} dT(x) \qquad \text{(Stieltjes integral)} \\ &= x^{-s} T(x)\big|_1^\infty - \int_1^\infty T(x)(-sx^{-s-1}dx) \\ &= s \int_1^\infty T(x) x^{-s-1} dx \end{aligned}$$

This extends to a holomorphic function for $\operatorname{Re} s > 0$ since it converges uniformly on $\operatorname{Re} s \geq \varepsilon$ for any ε. $\square$

For $\operatorname{Re} s > 1$,

$$\sum_{p \equiv a \pmod m} p^{-s} = \sum_{\text{all } p} p^{-s} \cdot \begin{cases} 1 & \text{if } p \equiv a \pmod m \\ 0 & \text{otherwise} \end{cases}$$

$$= \sum_{\text{all } p} p^{-s} \frac{1}{\varphi(m)} \sum_{\chi} \chi(a^{-1}p) \qquad \text{Corollary 23.7 applied to } g = a^{-1}p$$

Note that $p \equiv a \pmod m \iff a^{-1}p \equiv 1 \pmod m$

$$= \sum_{\chi} \frac{\chi(a^{-1})}{\varphi(m)} \sum_{p} \chi(p) p^{-s}$$

Note that $\sum_p \chi(p)p^{-s}$ are the most important terms of the power series expansion of $\log L(s, \chi) = \sum -\log(1 - \chi(p)p^{-s})$.

$$= \sum_{\chi} \frac{\chi(a^{-1})}{\varphi(m)} \log L(s, \chi) + O(1)$$

$$= \frac{1}{\varphi(m)} \log \zeta(s) + \sum_{\chi \neq \mathbb{1}} \frac{\chi(a^{-1})}{\varphi(m)} \log L(s, \chi) + O(1) \qquad \text{as } s \to 1^+$$

Key claim 23.10. If $\chi \neq \mathbb{1}$ then $L(1, \chi) \neq 0$.

(We've already proved that it's holomorphic.) So $\log L(s, \chi) = O(1)$ as $s \to 1^+$. We've proven that $\zeta(s) = \frac{1}{s-1} +$ something holomorphic as $s \to 1$; so by the discussion above, the key claim implies $\sum_{p \equiv a \pmod m} p^{-s} = \frac{1}{\varphi(m)} \log \frac{1}{s-1} + O(1)$ as $s \to 1^+$. This also shows that primes are equally distributed in terms of classes mod m.

Lecture 24: December 2

Last time, we had reduced the proof of Dirichlet's theorem on primes in arithmetic progressions to the statement that

$$L(1, \chi) \neq 0 \text{ for all } \chi \neq \mathbb{1}.$$

To prove this, we need:

Theorem 24.1. *[Dirichlet analytic class number formula] Suppose that $[K : \mathbb{Q}] = n$. Then $\zeta_K(s)$ extends to a holomorphic function for $\operatorname{Re} s > 1 - \frac{1}{n}$ except for a simple pole at $s = 1$ with residue*

$$\frac{2^r (2\pi)^s h R}{w \cdot |\operatorname{disc} \mathcal{O}_K|^{1/2}}$$

where r, s (by abuse of notation) are the real and complex places, h is the class number $\# \operatorname{Pic} \mathcal{O}_K$, R is the regulator, and w is the number of roots of unity in K.

Example 24.2 (Evaluating the formula for the Riemann zeta function)**.** We're supposed to get residue = 1. By the formula:

$$res_{s=1}\zeta(s) = \frac{2^1(2\pi)^0 1 \cdot 1}{2 \cdot 1^{1/2}} = 1.$$

The regulator is the covolume of a zero-dimensional lattice, so it's the determinant of a 0×0 matrix; this is 1.

The proof is, unsurprisingly, rather involved. We need some preliminaries.

Definition 24.3. Let X, Y be metric spaces. Say that $f : X \to Y$ is Lipschitz iff there exists C such that for all $x, x' \in X$, $d(f(x), f(x')) \leq Cd(x, x')$. This is a bit stronger than continuity; it says your function doesn't stretch things too much. (E.g. it rules out space-filling curves.)

Say that $B \subset \mathbb{R}^n$ is d-Lipschitz parametrizable if there exist finitely many Lipschitz maps $f : [0, 1]^d \to B$ whose images cover B.

Lemma 24.4. *Let $S \subset \mathbb{R}^n$ be such that its boundary ∂S is $(n-1)$-Lipschitz parametrizable. Then $\#(tS \cap \mathbb{Z}^n) = \mathrm{vol}(S)t^n + O(t^{n-1})$ as $t \to \infty$.*

Why does the Lipschitz hypothesis matter? Imagine a finite-volume star-shaped region with infinite spikes, one hitting every integer point.

Proof. Idea: get a lower bound by counting the number of cubes that fit inside the shape, and get an upper bound by counting the cubes that intersect the shape. So

$$\#\text{boxes contained in } tS \leq \mathrm{vol}(tS) \leq \#\text{boxes intersecting } tS$$

but also I claim that

$$\#\text{boxes contained in } tS \leq \#(tS \cap \mathbb{Z}^n) \leq \#\text{boxes intersecting } tS.$$

(How to relate boxes and lattice points? For every lattice point, form the box that has that point as its lower left corner.) We want to bound the difference between the upper and lower bounds, i.e. the number of boxes that touch tS but aren't completely contained in it. This is $\leq$ #boxes within $O(1)$ of $\partial(tS)$. By hypothesis, we know that ∂S is covered by finitely many images of the unit cube; subdivide this into $\tau := \lfloor t \rfloor$ pieces. By the Lipschitz hypothesis, each point of ∂S is within $O(\frac{1}{\tau})$ of one of the points $f_i(\frac{a_1}{\tau}, \dots)$ with $0 \leq a_i < \tau$. If you scale this up by a factor of t, each point of $\partial(tS)$ is within $O(1)$ of one of the points $t \cdot f_i(\frac{a_1}{\tau}, \dots)$. There are $O(\tau^{n-1})$ points $f_i(\frac{a_1}{\tau}, \dots)$. □

Open problem 24.5. If S is the unit disc, how many lattice points are inside tS? The lemma says that it's $\pi t^2 + O(t)$, but it turns out that the error is a lot smaller than this...

Generalization 24.6. Let Λ be a full lattice in $\mathbb{R}^n$. Then

$$\#(tS \cap \Lambda) = \frac{\mathrm{vol}(S)}{\mathrm{covol}(\Lambda)} t^n + O(t^{n-1}).$$

Let K be a number field with $[K:\mathbb{Q}] = n$; recall

$$\mathcal{O}_K^\times = U \times \mu(K)$$

where $\mu(K)$ is the set of roots of unity, and U is free of rank $r+s-1$ (μ is canonically defined, but U is not canonical – you can always change a generator of U by an element of μ.) Set $w := \#\mu(K)$.

To understand $\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{N(I)^s}$ as $s \to 1^+$, we need to understand the rate of growth of this series; equivalently, we need to estimate $\#\{I : N(I) \leq t\}$ as $t \to \infty$. (We know this is finite: I must be composed of primes whose norms are $\leq t$, and the exponents are also bounded.)

First consider the set of nonzero principal ideals I such that $N(I) \leq t$. Equivalently, we want to count generators – nonzero $\alpha \in \mathcal{O}_K$ such that $|N(\alpha)| \leq t$. But two α's will generate the same ideal if they differ by a unit; so we want to consider

$$\{\text{nonzero } \alpha \in \mathcal{O}_K : |N(\alpha)| \leq t\}/\mathcal{O}_K^\times.$$

Recall $\mathcal{O}_K$ is a full lattice in $K_\mathbb{R}$. So we are just counting lattice points in a bounded region.

Rewrite this set as

$$(K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/\mathcal{O}_K^\times$$

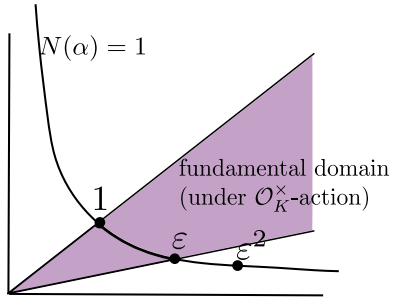
(where $K_{\mathbb{R},\leq t}^\times$ is the set of units in $K_\mathbb{R}$ whose norms are $\leq t$).

There is a w-to-1 map

$$\begin{aligned}(K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/U &\to (K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/\mathcal{O}_K^\times \\ &\cong F_{\leq t} \cap \mathcal{O}_K\end{aligned}$$

where F is a fundamental domain for the action of U on $K_\mathbb{R}^\times$.

Example 24.7. If K is a real quadratic field, $K_\mathbb{R} \cong \mathbb{R} \times \mathbb{R}$. The norm is just the product of the coordinates. So the set where $N(\alpha) = 1$ is a hyperbola. The lattice is not $\mathbb{Z} \times \mathbb{Z}$, though. You actually end up with infinitely many points below the hyperbola in the first quadrant – e.g. take any lattice point and multiply it by a unit to get another one. But we want to count orbits, so just concentrate on a fundamental domain:

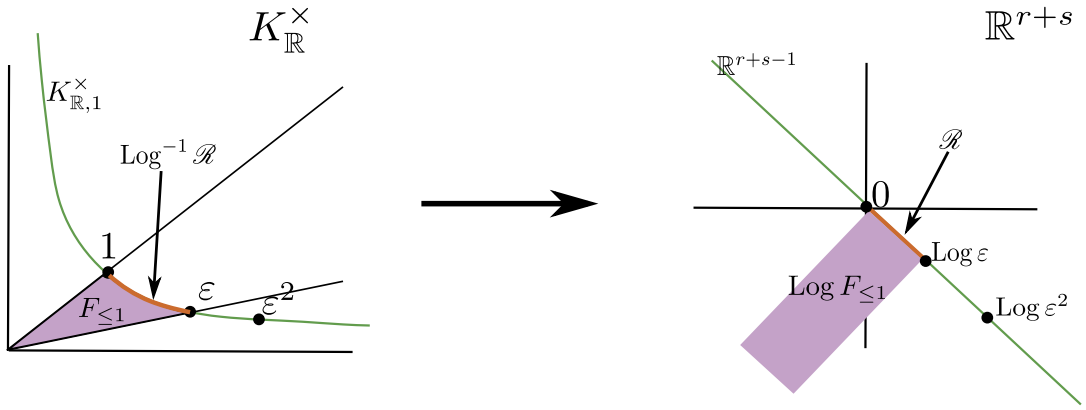


Look at the map

$$K_{\mathbb{R},1}^\times \overset{\text{Log}}{\to} \mathbb{R}_0^{r+s}$$

where the LHS is the norm-1 elements and the RHS is the sum-0 elements. This restricts to $U \to \mathrm{Log}U = \mathrm{Log}\mathcal{O}_K^\times$; this is the lattice we used in proving the rank of $\mathcal{O}_K^\times$. Let $\mathscr{R}$ be a fundamental domain for the lattice $\mathrm{Log}U$ in $\mathbb{R}_0^{r+s}$.

(So in our example, the image of the hyperbola $N(\alpha) = 1$ is the line $x + y = 0$, and the units $1, \varepsilon, \varepsilon^2, \ldots$ map to a lattice on this 1-dimensional subspace. $\mathscr{R}$ is a fundamental domain of this lattice, and its volume is the regulator.)



Then $\mathrm{Log}^{-1}\mathscr{R}$ is a fundamental domain for U acting on $K_{\mathbb{R},1}^\times$. (E.g. the part of the hyperbola between 1 and ε.) But I wanted a fundamental domain for the action on all of $K_{\mathbb{R}}^\times$, not just the norm-1 things. So consider the map $K_{\mathbb{R}}^\times \xrightarrow{\sigma} K_{\mathbb{R},1}^\times$ taking $x \mapsto \frac{x}{N(x)^{1/n}}$, and define the fundamental domain to $F := \sigma^{-1}\mathrm{Log}^{-1}\mathscr{R}$. Then:

(1) $F_{\leq t} = t^{1/n} F_{\leq 1}$;
(2) $\partial F_{\leq 1}$ is $(n-1)$-Lipschitz parametrizable.

So we can apply Generalization 24.6; this gives

$$\#(F_{\leq t} \cap \mathcal{O}_K) = \frac{\mathrm{vol}(F_{\leq 1})(t^{1/n})^n}{\mathrm{covol}(\mathcal{O}_K)} + O((t^{1/n})^{n-1}).$$

Lemma 24.8. $\mathrm{vol}(F_{\leq 1}) = 2^r(2\pi)^s R$ *where* R *is the regulator.*

This is basically a calculus problem. (In the example, we're computing the volume below the hyperbola, in the wedge.)

Proof. Let's change coordinates by taking the log:

$$\begin{aligned} \mathbb{R}^\times &\to \mathbb{R} \times \{\pm 1\} \\ x &\mapsto (\log|x|, sgn(x)) \\ \varepsilon e^\ell &\leftarrow\!\shortmid (\ell, \varepsilon) \\ dx &\mapsto e^\ell d\ell \times (\text{counting measure}) \end{aligned}$$

Do this to $\mathbb{C}^\times$ as well:

$$\mathbb{C}^\times \to \mathbb{R} \times [0, 2\pi)$$

$$\begin{aligned} z &\mapsto (2\log|z|, \arg z) \\ e^{\ell/2}e^{i\theta} &\leftarrow\!\shortmid (\ell, \theta) \\ 2dA &\mapsto 2e^{\ell/2}d(e^{\ell/2})d\theta = e^{\ell}d\ell d\theta \end{aligned}$$

Under the isomorphism

$$K_{\mathbb{R}}^{\times} = (\mathbb{R}^{\times})^r \times (\mathbb{C}^{\times})^s \cong \mathbb{R}^{r+s} \times \{\pm 1\}^r \times [0, 2\pi)^s,$$

the canonical measure on $K_{\mathbb{R}}^{\times}$ corresponds to $e^{\text{sum}}\cdot$ Lebesgue measure on $\mathbb{R}^{r+s}$; so $F_{\leq 1}$ corresponds to $\left(\mathscr{R} + (-\infty, 0](\frac{1}{n}, \ldots, \frac{2}{n})\right) \times \{\pm 1\} \times [0, 2\pi)^s$. (What's with the first term? Multiplying by an element of norm $\nu \leq 1$ corresponds to shifting by $\log \nu < 0$. What's with the $\frac{2}{n}$'s? The Log map sends $(x_1, \ldots, x_r, z_1, \ldots, z_s) \mapsto (\log|x_1|, \ldots, \log|x_r|, 2\log|z_1|, \ldots, 2\log|z_s|)$, so there are 2's for each copy of $\mathbb{C}$.)

To be continued... □

Lecture 25: December 4

We were in the middle of proving the Dirichlet analytic class number formula; to this end we were trying to prove:

Theorem 25.1.

$$\#\{I \subset \mathcal{O}_K \,:\, N(I) \leq t\} = \frac{2^r(2\pi)^s hR}{w|\operatorname{disc}\mathcal{O}_K|^{1/2}}t + O(t^{1-1/n})$$

Proof. Recall we had a w-to-1 map

$$F_{\leq t} \cap \mathcal{O}_K \to \{\text{nonzero principal ideals } I \text{ with } N(I) \leq t\}.$$

Let F be a fundamental domain for $K_{\mathbb{R}}^{\times}/U$. (Remember $\mathcal{O}_K^{\times} = \mu_k \times U$ where U is free.) Last time we explained why $\operatorname{Log}(F_{\leq 1}) = \left(\mathscr{R} + (-\infty, 0](\frac{1}{n}, \ldots, \frac{2}{n})\right) \times \{\pm 1\} \times [0, 2\pi)^s$. Last time we showed how taking Log takes the canonical measure on $K_{\mathbb{R}}^{\times} = (\mathbb{R}^{\times})^r \times (\mathbb{C}^{\times})^s$ to the measure e^{sum}(Lebesgue measure) on $\mathbb{R}^{r+s} \times \{\pm 1\}^r \times [0, 2\pi)^s$.

We want to do another coordinate change: take $\mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1} \times \mathbb{R}$ by $(x_1, \ldots, x_{r+s}) \mapsto (x_1, \ldots, x_{r+s-1}, \underbrace{x_1 + \cdots + x_{r+s}}_{y})$. How does this affect the measure? It sends e^{sum}(Lebesgue) to e^y(Lebesgue). This is essentially because $\det \begin{pmatrix} 1 & & & 1 \\ & 1 & & 1 \\ & & \ddots & \\ & & & 1 \end{pmatrix} = 1$.

Now actually do the integral!

$$\int_{\mathscr{R} + (-\infty, 0](\frac{1}{n}, \ldots, \frac{2}{n})} e^{\text{sum}}\text{Lebesgue} = \int_{y=-\infty}^{0} \operatorname{vol}(\mathscr{R} + y(\frac{1}{n}, \ldots, \frac{2}{n}))e^y dy$$

$$= \int_{y=-\infty}^{0} Re^y dy = R$$

Thus

$$\operatorname{vol}(F_{\le 1}) = R \cdot 2^r (2\pi)^s$$
$$\#F_{\le t} \cap \mathcal{O}_K = 2^r (2\pi)^s Rt + O((t^{1/n})^{n-1})$$

The denominator is $\operatorname{covol}(\mathcal{O}_K)$; we proved this a while ago. Dividing by w, we get

$$\#\left\{\begin{array}{c}\text{nonzero principal ideals } I \\ \text{with } N(I) \le t\end{array}\right\} = \frac{1}{w}\left(2^r(2\pi)^s Rt + O((t^{1/n})^{n-1})\right)$$

But we're not done – this only counts the principal ideal classes; we have to redo it for all the other ideal classes.

For any fractional ideal c, there is a correspondence

$$\left\{\begin{array}{c}\text{ideals } I \subset \mathcal{O}_K \text{ in the class of } c^{-1} \\ \text{such that } N(I) \le t\end{array}\right\} \overset{\text{mult. by } c}{\longrightarrow} \left\{\begin{array}{c}\text{nonzero principal ideals } J \\ \text{divisible by } c \text{ s.t. } N(J) \le tN(c)\end{array}\right\}.$$

But the latter set is the same as $\{\text{nonzero } \alpha \in c \ : \ |N(\alpha)| \le tN(c)\} \Big/ \mathcal{O}_K^\times$. I claim there are

$$\frac{2^r(2\pi)^s R}{w|\operatorname{disc}\mathcal{O}_K|^{1/2}N(c)} tN(c) + O(t^{1-1/n})$$

of these, because the new covolume is $|\operatorname{disc}\mathcal{O}_K|^{1/2}N(c)$ instead of just $|\operatorname{disc}\mathcal{O}_K|^{1/2}$.

But $N(c)$ cancels (this says that ideals are equidistributed over ideal classes); summing over the h ideal classes gets what we want. □

Lemma 25.2. *Let $a_1, a_2, \cdots \in \mathbb{C}$ and $\sigma \in \mathbb{R}$. Suppose $|a_1 + \cdots + a_t| = O(t^\sigma)$ as $t \to \infty$. Then $\sum_{n\ge 1} a_m m^{-s}$ converges to a holomorphic function for $\operatorname{Re} s > \sigma$.*

Instead of a radius of convergence, Dirichlet series have an x-coordinate ("abscissa") of convergence.

Proof. For $x \in \mathbb{R}_{\ge 0}$, let $A(x) = \sum_{m \le x} a_m$. Then for $\operatorname{Re} s > \sigma$, using integration by parts using Stieltjes integrals,

$$\sum a_m m^{-s} = x^{-s}A(x)|_{1^-}^{\infty} - \int_1^\infty A(x)(-sx^{s-1}dx)$$
$$= (0-0) + s\int_1^\infty$$

By the assumption on $A(x)$, this converges uniformly on the region $\operatorname{Re} s \ge \sigma + \varepsilon$ for any fixed ε. So it is holomorphic on all of these regions, hence holomorphic on the region $\operatorname{Re} s > \sigma$. □

Lemma 25.3. *Let $a_1, a_2, \cdots \in \mathbb{C}$, $0 \le \sigma < 1$, and $\rho \in \mathbb{C}$. If $a_1 + \cdots + a_t = \rho t + O(t^\sigma)$ as $t \to \infty$, then $\sum_{m\ge 1} a_m m^{-s}$ converges for $\operatorname{Re} s > 1$ and has an analytic continuation to $\operatorname{Re} s > \sigma$ except for a simple pole at $s = 1$ with residue ρ.*

Note that if all the a_i's are 1, then you get the Riemann zeta function!

PROOF. Let $b_m = a_m - \rho \in \mathbb{C}$. Then $b_1 + \cdots + b_t = O(t^\sigma)$.

$$\sum a_m m^{-s} = \rho \sum m^{-s} + \sum b_m m^{-s}.$$

The first term on the RHS is the Riemann zeta function; we proved before that it is holomorphic fr $\operatorname{Re} s > 1$ and has an analytic continuation to $\operatorname{Re} s > 0$ except for a pole at 1 with residue 1. By Lemma 25.2, the second term on the RHS is holomorphic for $\operatorname{Re} s > \sigma$. Since $\sigma < 1$, this piece is holomorphic at $s = 1$, so the residue is just the coefficient ρ of the Riemann zeta function. □

PROOF OF THE DIRICHLET ANALYTIC CLASS NUMBER FORMULA 24.1. We have

$$\begin{aligned}
\zeta_K(s) &= \sum_{I \subset \mathcal{O}_K} N(I)^{-s} \\
&= \sum_{m \geq 1} a_m m^{-s} \qquad \text{where } a_m := \#\{I : N(I) = m\} \\
a_1 + \cdots + a_t &= \#\{I \subset \mathcal{O}_K : N(I) \leq t\} \\
&\overset{25.1}{=} \frac{2^r (2\pi)^s h R}{w |\operatorname{disc} \mathcal{O}_K|^{1/2}} t + O(t^{1-1/n})
\end{aligned}$$

Lemma 25.3 says:

- $\zeta_K(s)$ converges for $\operatorname{Re} s > 1$
- there is an analytic continuation to $\operatorname{Re} s > 1 - \frac{1}{n}$ except for a simple pole at $s = 1$ with residue

$$\frac{2^r (2\pi)^s h R}{w |\operatorname{disc} \mathcal{O}_K|^{1/2}}.$$

□

There is also a Riemann hypothesis for general number fields K; the hypothesized zeros are the same, plus some more trivial zeros.

Theorem 25.4.

$$\zeta_{\mathbb{Q}(\zeta_m)}(s) \quad \text{“=”} \prod_{\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times} L(s, \chi), \qquad \textit{ignoring Euler factors corresponding to primes } p \mid m.$$

If $\mathbb{1}$ temporarily denotes the trivial character *mod* m, then $L(s, \mathbb{1}) = \prod_{p \nmid m} (1 - p^{-s})^{-1} \approx \zeta(s)$.

PROOF. Let $p \nmid m$. Look at the Euler factors on each side corresponding to p. On the LHS, you get $\prod_{\mathfrak{p} | p} (1 - N(\mathfrak{p})^{-s})^{-1}$. $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is a Galois extension, so we can talk about e, f, g corresponding to p; recall we proved that $e = 1$, $f =$ the order of Frobenius $=$ the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Since $efg = n = \varphi(m)$, we have $g = \frac{\varphi(m)}{f}$. So

$$\begin{aligned}
\prod_{\mathfrak{p} | p} (1 - N(\mathfrak{p})^{-s})^{-1} &= (1 - (p^f)^{-s})^{-g} \\
&= (1 - (p^{-s})^f)^{-g}
\end{aligned}$$

On the RHS, the factors coming from p are $\prod_\chi (1-\chi(p)p^{-s})^{-1}$. We need to show this is the same thing as $(1-(p^{-s})^f)^{-g}$. Do a change of variables $T := p^{-s}$; it suffices to prove:

Lemma 25.5. $(1-T^f)^g = \prod_\chi (1-\chi(p)T)$

PROOF. If p has order f, then $\chi(p)$ will be a f^{th} root of unity. That is, there is a surjective homomorphism

$$\widehat{(\mathbb{Z}/m\mathbb{Z})}^\times \to \mu_f \text{ sending } \chi \mapsto \chi(p)$$

with fibers of size $\varphi(m)/f = g$. So the RHS is $(\prod_{\alpha^f=1}(1-\alpha T))^g$. You can see that this = LHS. □

Key claim 25.6. If $\chi \neq \mathbb{1}$, then $L(1,\chi) \neq 0$.

PROOF. Compute $\operatorname{ord}_{s=1}$ in Theorem 25.4. Any individual factor $1-p^{-s}$ is nonzero at $s=1$ (because primes $\neq 1\ldots$). So if you throw away finitely many factors, it doesn't affect the order of vanishing. So you might as well replace with the Riemann zeta function, which has order of vanishing -1 at $s=1$. Then

$$-1 = \underbrace{-1}_{\text{from } \mathbb{1}} + \sum_{\chi\neq\mathbb{1}} \operatorname{ord}_{s=1} L(s,\chi)$$

but we proved that all of the terms $\operatorname{ord}_{s=1} L(s,\chi)$ are ≥ 0; so they must all be zero. □

Definition 25.7. If P is a set of primes, then the *Dirichlet density* of P is

$$\delta(P) := \log_{s\to 1^+} \frac{\sum_{p\in P} p^{-s}}{\log \frac{1}{s-1}}.$$

Example 25.8. $\delta(\{\text{all primes}\}) = 1$.

If P is the set of primes $p \equiv a \pmod m$, then the Key Claim shows that $\delta(P) = \frac{1}{\varphi(m)}$.

LECTURE 26: DECEMBER 9

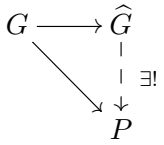
Today we'll talk about class field theory.

Profinite completion. Let G be a topological group. If $G \twoheadrightarrow F$ is a continuous surjection onto F then $F \cong G/U$ for some finite-index open finite subgroup $U \leq G$.

Definition 26.1.

$$\widehat{G} = \lim_{\substack{\text{fin.index} \\ \text{open subgroups} U \leq G}} G/U$$

It has the universal property that for every continuous homomorphism $G \to P$ to a profinite group P, there is a unique continuous dotted homomorphism.



We've already encountered $\widehat{\mathbb{Z}}$; on the other hand, $\widehat{\mathbb{Q}} = 0$.

There is a bijection between the set of finite-index open subgroups of G and those of $\widehat{G}$.

Profinite groups are always compact.

Local fields. There are two kinds of local fields: archimedean ones ($\mathbb{R}$ or $\mathbb{C}$) and nonarchimedean ones. Start with a complete DVR $\mathcal{O}$; assume the residue field k is finite. Embed $\mathcal{O}$ in its fraction field K (K is the local field). The maximal abelian extension K^{ab} (the compositum of all extensions with abelian Galois group) sits in a tower

$$K \subset K^{unr} \subset K^{ab} \subset K^s.$$

Why does it contain K^{unr}? Unramified fields are in bijection with finite separable extensions of the residue field, which is finite, and Galois groups of extensions of a finite field are all abelian.

Local nonarchimedean fields are defined to be either finite extensions of $\mathbb{Q}_p$, if the characteristic is 0, or $\mathbb{F}_q((t))$, if char $= p > 0$.

There is a homomorphism

$$\theta : K^\times \to \mathrm{Gal}(K^{ab}/K)$$

inducing an isomorphism $\widehat{K^\times} \xrightarrow{\cong} \mathrm{Gal}(K^{ab}/K)$. θ is called the local Artin homomorphism. If K is archimedean, then θ is surjective and $\ker\theta$ is the connected component of 1 in $K^\times$.

If K is nonarchimedean, then θ is injective. There are isomorphisms

$$K^\times \cong \mathcal{O}^\times \cdot \pi^{\mathbb{Z}} \cong \mathcal{O}^\times \mathbb{Z}$$

which induces an isomorphism $\widehat{K^\times} \cong \mathcal{O}^\times \times \widehat{\mathbb{Z}}$. This is not canonical, but

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}^\times & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\
\downarrow & & & & \downarrow{\scriptstyle\theta} & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Gal}(K^{ab}/K^{unr}) & \longrightarrow & \mathrm{Gal}(K^{ab}/K) & \longrightarrow & \mathrm{Gal}(K^{unr}/K) & \longrightarrow & 0
\end{array}$$

is, and I claim that the first vertical map is an isomorphism, and the third is after completion. What is this last map? By the bijection involving unramified extensions, $\mathrm{Gal}(K^{unr}/K) \cong \mathrm{Gal}(k^s/k)$, and I claim this is $= \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$ (the generator of each $\mathbb{Z}/n\mathbb{Z}$ corresponds to Frobenius).

$\mathrm{Gal}(K^{ab}/K^{unr})$ is the inertia group of K^{ab}/K. The bottom row is profinite completion of the top row. On elements,

$$\begin{array}{ccc} \pi & \longrightarrow & 1 \\ \downarrow & & \downarrow \\ Frob & \longrightarrow & Frob \end{array}$$

Recall we have a sequence of subgroups $\mathcal{O}^x \supset 1+\mathfrak{p} \supset 1+\mathfrak{p}^2 \supset$. These correspond to a sequence of subgroups in the inertia group called *ramification subgroups*. An element of the inertia group is, by definition, an automorphism that acts as the identity on the residue field $B/\mathfrak{q}$. The n^{th} ramification subgroup contains the ones that act as the identity on $B/\mathfrak{q}^n$. (But this is the wrong numbering...) If an automorphism acts as the identity on all of the $B/\mathfrak{q}^n$'s, then it is the identity.

Functoriality. Let L/K be a finite extension of local fields. I claim the diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{\theta_L} & \mathrm{Gal}(L^{ab}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \text{restriction}} \\ K^\times & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

is commutative. (Inclusion $K^\times \subset L^\times$ corresponds to the *transfer homomorphism* on Galois groups.)

There are bijections

$$\{\text{finite index open subgroups}\} \longleftrightarrow \{\text{finite index subgroups of } \mathrm{Gal}(K^{ab}/K)\}$$
$$\overset{\text{Galois theory}}{\longleftrightarrow} \{\text{finite abelian extensions of } K \text{ inside } K^s\}$$

The first thing is easy; the last thing is something you want to know about. More explicitly, an extension L/K corresponds to the open subgroup $N_{L/K}L^\times$.

If L/K is a finite abelian extension, I claim there is a surjection

$$K^\times \to \mathrm{Gal}(K^{ab}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$$

with kernel $N_{L/K}L^\times$. I said the inertia group in $\mathrm{Gal}(K^{ab}/K)$ is the image of $\mathcal{O}^\times$; the inertia subgroup in $\mathrm{Gal}(L/K)$ is also the image of $\mathcal{O}^\times$. A uniformizer $\pi \in \mathcal{O}^\times$ maps to Frobenius.

Example. Let $p > 2$. Suppose we want to describe all the extensions of $\mathbb{Q}_p$ with Galois group $\mathbb{Z}/p\mathbb{Z}$. This is the same as understanding the quotients $\mathbb{Q}_p^\times \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$, or equivalently understanding the surjections $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$. But $\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times p^{\mathbb{Z}} = (1+p\mathbb{Z}_p)\times\mathbb{F}_p^\times \times p^{\mathbb{Z}} \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}$. Take quotients of each piece by the p^{th} power; the middle piece goes away to get

$$\mathbb{Q}_\mathfrak{p}^\times/(\mathbb{Q}_\mathfrak{p}^\times)^p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Answer: there are $p+1$ such extensions.

Global fields. If the characteristic is 0, global fields are number fields (finite extensions of $\mathbb{Q}$); in characteristic p, global fields are global function fields (finite extensions of $\mathbb{F}_p((t))$).

If you choose the right constant field, these are function fields of a geometrically integral curve X over a finite field k.

Let K be a global field, and K_v be the completion of K at v (this is a local field). Let $\mathcal{O}_v$ be a valuation ring (if v is archimedean, set $\mathcal{O}_v = K_v$). You can define the adèle ring $\mathbb{A}_K = \prod'(K_v, \mathcal{O}_v)$ and the idèle group $\mathbb{A}_K^\times$, which comes with a map $\mathbb{A}_K^\times \to \mathcal{I}_K$ (the ideal group) in the number field case: for each element, take $v_\mathfrak{p}$ to get the exponent of $\mathfrak{p}$ in the ideal.

The *idèle class group* is $C_K := \mathbb{A}_K^\times / K^\times$.

Global CFT. Recall that local CFT said that there is an "almost isomorphism" $K^\times \to \mathrm{Gal}(K^{ab}/K)$. Global CFT says that there is a homomorphism

$$\theta : C_K \to \mathrm{Gal}(K^{ab}/K)$$

inducing an isomorphism $\widehat{C_K} \xrightarrow{\cong} \mathrm{Gal}(K^{ab}/K)$. This is called the *global Artin homomorphism*.

If K is a number field, θ is surjective, and $\ker\theta$ is the connected component of the identity. If K is a global function field, then θ is injective and the image consists of automorphisms $\sigma \in \mathrm{Gal}(K^{ab}/K)$ restricting to an integer multiple of Frobenius in $\mathrm{Gal}(k^s/k)$ (here k is the residue field, the largest finite field contained in K). Note that $\mathrm{Gal}(k^s/k) \cong \widehat{\mathbb{Z}}$ is topologically generated by Frobenius; things in the image are the elements corresponding to $\mathbb{Z} \subset \widehat{\mathbb{Z}}$.

Functoriality. Let L/K be a finite extension of global fields. Recall $\mathbb{A}_L \cong \mathbb{A}_K \otimes_K L$; this is a free $\mathbb{A}_K$-module with rank $[L : K]$. So you can define the norm map on adèles $N_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$ (take the determinant of the multiplication-by-α matrix wrt some basis). The claim is that there is a commutative diagram

$$\begin{array}{ccc} C_L & \xrightarrow{\theta_L} & \mathrm{Gal}(L^{ab}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ C_K & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

There are correspondences

$$\begin{aligned} \{\text{finite-index open subgroups of } C_K\} &\longleftrightarrow \{\text{finite-index open subgroups of } \mathrm{Gal}(K^{ab}/K)\} \\ &\longleftrightarrow \{\text{finite abelian extensions of } K \text{ inside } K^s\} \end{aligned}$$

More explicitly, an extension L/K corresponds to the subgroup $N_{L/K}C_L$.

If L/K is a finite abelian extension, by Galois theory there is a map $C_K \to \mathrm{Gal}(K^{ab}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$ coming from the tower $K^{ab}/L/K$; I claim that this is a surjection with kernel $N_{L/K}C_L$.

Local-global compatibility. Suppose we know the global θ. Let v be a place of K. You get a map $K_v^\times \hookrightarrow \mathbb{A}_K^\times$ taking $\alpha \mapsto (\cdots, 1, 1, 1, \alpha, 1, \cdots)$ (where α is in the v^{th} position). Compose this with $\mathbb{A}_K^\times$ to get a map $K_v^\times \to C_K$. I claim there is a unique θ_v making the

following diagram commute:

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\theta_v} & \mathrm{Gal}(K_v) \\ \downarrow & & \downarrow \\ C_K & \xrightarrow{\theta} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

where the right vertical arrow is res, and it is the local Artin homomorphism for K_v. (Injectivity is essentially Krasner's lemma.)

Conversely, if we know the local Artin homomorphism θ_v for every v and L is a finite abelian extension of K, define

$$\mathbb{A}_K^\times \to \mathrm{Gal}(L/K) \text{ sending } (a_v), t \prod_v \theta_v(a_v).$$

This is an infinite product; why does it make sense? For all but finitely many v, L/K is unramified at v and $a_v \in \mathcal{O}_v^\times$. The image of this under the local Artin map is the inertia group; since it's unramified, $\theta_v(a_v) \in I_v = \{1\}$. You can check that these are all compatible as you vary L; so you get a map to the inverse limit of all of these:

$$\mathbb{A}_K^\times \to \mathrm{Gal}(K^{ab}/K).$$

I claim that this factors through C_K; this claim is *Artin reciprocity* (i.e. that $K^\times$ is in the kernel). This is hard.

If you apply this to a quadratic extension, quadratic reciprocity comes out. If you want to read more about Artin reciprocity, read Bjorn's essay "A brief summary of the statements of CFT" on his website.

The End.