254A: Number Theory

Nir Elber

Fall 2021

Contents

Theme 1
Commutative Algebra

1.1 August 25

Ok, I guess we can start.

1.1.1 Logistics

We're usign Neukirch. The reading for Friday is §1.1. Office hours are Monday, Wednesday, Friday, 12PM–1PM and 3PM–4PM at 883 Evans. Email is `voyta@math.berkeley.edu`. There is a bcourses, but the course website is `math.berkeley.edu/~vojta/254a.html`.

There will be no final exam, but there will be weekly homeworks. We'll go over most of Chapter 1 (sans the last 2–3 sections), Chapter 2 (sans section 6 and some of 7, 9, 10), some of Chapter 3 (§1–3), some of Chapter 7[1] (a little bit), and some of Chapter 6 (parts of §1–2).

1.1.2 Overview

Here's our main character.

Definition 1.1 (Number Field)**.** A *number field* K is a finite field extension of $\mathbb{Q}$.

Example 1.2. For example, $\mathbb{Q}(\sqrt{2})$ is a number field.

We often work with the picture that $\mathbb{Z} \subseteq \mathbb{Q}$ and $\mathcal{O}_K \subseteq K$, where $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. (Namely, $\mathcal{O}_K$ consists of the roots of monic polynomials with integer coefficients in $\mathbb{Z}$ which live in K.) The trivial example is that $\mathbb{Z}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ by the Rational root theorem.

Warning 1.3. We might sloppily call the elements $\mathcal{O}_K$ "integers." To distinguish, we may often call $\mathbb{Z}$ the "rational integers."

[1] Analytic!

Chapter 1

In Chapter 1, we will interest ourselves in $\mathbb{A}$, which is the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$. The questions we ask here are what carries from $\mathbb{Z}$ to a particular $\mathcal{O}_K$.

$\mathbb{Z}$	$\mathcal{O}_K$
finite units	$\mathcal{O}_K^\times$ is finitely generated
PID	not a PID in general
UFD	iff a PID
	ideals have UPF

In Chapter 1, we will also talk a little about quadratic reciprocity.

Chapter 2

In Chapter 2, we localize. The idea is to focus on a single prime, say $\mathfrak{p} \subseteq \mathcal{O}_K$. For example, recall that we're interested in solving Diophantine equations in number theory. In the number field case, we are interested in solutions to equations which might extend to number fields and their rings of integers.

For example, the equation

$$x^2 + y^2 = -1$$

has no solutions in $\mathbb{Q}$ because it has local obstructions at the infinite place (namely, no solutions in $\mathbb{R}$). Similarly,

$$x^2 + y^2 = 7$$

has local obstructions in $\mathbb{Q}_2$ (check $\pmod 4$). The theory in Chapter 2 will let us generalize these arguments.

Chapter 3

In Chapter 3, we will study the different and discriminant. Very roughly, these are related to the question of how we might want to study ideal factorization via prime-splitting.

Chapter 7

In Chapter 7, we will do some analytic number theory. This is the study of the Riemann ζ function and friends.

Chapter 6

In Chapter 6, we will go over the statements of class field theory. Here we study abelian extension of number fields. If you want proofs, take 254B.

1.1.3 Philosophy

In number theory, we are interested in Diophantine equations and a few other things.

Example 1.4. We can solve $xy = 24$ with $x, y \in \mathbb{Z}$ by using the prime factorization of 24.

Example 1.5. We can solve $xy = 24$ with $x, y \in \mathbb{Q}$ by parameterization: $(x, y) = (t, 24/t)$ for $t \in \mathbb{Q}^\times$.

Example 1.6. We can solve $x^2 - 2y^2 = 1$ with $x, y \in \mathbb{Z}$ with more work.

1. We know that signs do not alter solutions. Further, the trick is that $(x, y) \mapsto (3x + 4y, 2x + 3y)$ and $(x, y) \mapsto (3x - 4y, -2x + 3y)$ also maps solutions. Then we can generate all solutions from $(1, 0)$ in this manner.

   In general, we can solve $x^2 - dy^2 = b$ for any $b \in \mathbb{Z}$ and $d \in \mathbb{Z} \setminus \mathbb{Q}^{\times 2}$ in this manner.

2. We factor this as $(x + y\sqrt{2})(x - y\sqrt{2}) = 1$ and decide to work in $\mathbb{Z}[\sqrt{2}]$. Namely, $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ (its multiplicative inverse is $x - y\sqrt{2}$), so we see we have to study the units of $\mathbb{Z}[\sqrt{2}]$. (We do have to be careful that $(1 - \sqrt{2})(1 + \sqrt{2}) = -1$ gives a unit with norm -1.)

   In fact, we have some sort of converse: if $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$, then let its multiplicative inverse by $x' + y'\sqrt{2}$. Multiplying their components, we see

   $$1 = (xx' + 2yy') + (xy' + x'y)\sqrt{2},$$

   forcing the individual components to be 1 and 0 respectively (note $\sqrt{2}$ is irrational). So $y/x = -y'/x'$, and they must both be reduced because $\gcd(x, y) = \gcd(x', y') = 1$ from $xx' + 2yy' = 1$. So $y = \pm y'$ and $x = \mp x'$. From this it follows

   $$x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2}) = \mp(x + y\sqrt{2})(\mp x \pm y\sqrt{2}) = \mp 1.$$

   So indeed, studying units in $\mathbb{Z}[\sqrt{2}]$ will at least get us somewhere because they are almost solutions to $x^2 - 2y^2 = 1$.

Here is something interesting about the second method here: we can let $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ by the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. This lets us define

$$\mathrm{N}_{\mathbb{Q}}^{K} : \mathbb{Q}(\sqrt{2})^\times \to \mathbb{Q}^\times$$

whose pre-image from $\{\pm 1\}$ consists of our units, and whose pre-image from 1 is actually our solutions. With some more pushing in this direction, we can recover $x + y\sqrt{2} = \pm(1 + \sqrt{2})^{2^\bullet}$ as our solutions set to the actual problem.

1.2 August 27

The reading for Monday is §1.1 and §1.2

1.2.1 Basic Definitions

In this course, our rings will always be rings with identity; ring homomorphisms will always send units to units. Our rings will almost always be commutative; we'll see if not. We take the following definitions.

Definition 1.7 (Entire/integral domain)**.** A ring R is *entire* or *an integral domain* if $1 \neq 0$ and has no zero divisors. In other words, $R \neq \{0\}$ and $ab = 0$ implies $a = 0$ or $b = 0$.

We note that R is an integral domain if and only if it can be embedded into a field (namely, its fraction field).

Definition 1.8 (Factorial/UFD)**.** A ring R is *factorial* if and only if it is an entire and all nonzero elements have a factorization into irreducible elements, up to permutation and associates.

Example 1.9. We have that $\mathbb{Z}$ is factorial by elementary number theory.

Definition 1.10 (Principal)**.** A ring R is *principal* if and only if $1 \neq 0$ and every ideal is principal.

Note we can have principal rings which are not entire, but PIDs are principal rings.

Definition 1.11. A polynomial $p(x) \in R[x]$ is monic if and only if $p \neq 0$ and its leading coefficient is 1.

1.2.2 Integral Rings

We start with Gauss's lemma (on polynomials).

Lemma 1.12 (Gauss)**.** Fix A a unique factorization domain with fraction field K. Fix $f \in A[x] \setminus \{0\}$. If $f = gh$ for $g, h \in K[x]$, then there is a $c \in K^\times$ such that $f = (cg)(h/c)$ with $cg, h/c \in A[x]$.

In other words, we can turn factorizations from $K[x]$ to $A[x]$.

Proof. This is an exercise but not in the homework; it's in Neukirch. ■

We want to define integral rings, so here is.

Definition 1.13 (Integral)**.** Let $A \subseteq B$ be rings.

(a) We have $b \in B$ is *integral* over A if b is the root of some monic polynomial $f \in A[x] \setminus \{0\}$. We will maybe call f an integral dependence relation of b.

(b) We have B is integral over A if each $b \in B$ are integral over A.

(c) The integral closure of A in B is the set of all $b \in B$ such that b is integral over A.

(d) If A is an integral domain, the integral closure of A is the integral closure of A in its fraction field.

We will show that the integral closure is a ring later. Note that the integral closure and the algebraic closure are potentially very different objects. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$. Here is an example.

Proposition 1.14. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.

Proof. In one direction, take $\alpha \in \mathbb{Z}[\sqrt{2}]$ and write $\alpha = a + b\sqrt{2}$ for $a, b \in \mathbb{Z}$. Then α is a root of the monic polynomial

$$(x - a)^2 - 2b^2 \in \mathbb{Z}[x].$$

So indeed, α is integral over $\mathbb{Z}$.

In the other direction, suppose $\alpha \in \mathbb{Q}(\sqrt{2})$ is integral over $\mathbb{Z}$. We are promised a monic polynomial $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. Additionally, α is algebraic, so we get $g \in \mathbb{Q}[x]$ the minimal (monic, irreducible) polynomial of α.

Then $g \mid f$, so we can use Lemma 1.12 to get $c \in K^\times$ such that $cg \in \mathbb{Z}[x]$ with $f/(cg) \in \mathbb{Z}[x]$. But now f and g are monic, so $c \in \mathbb{Z}$ and $1/c \in \mathbb{Z}$ as the leading coefficient of $f/(cg)$, from which it follows $c = \pm 1$, so in fact $g \in \mathbb{Z}[x]$ all along.

We now have two cases.

1. If $\alpha \in \mathbb{Q}$, then $g(x) = x - \alpha$, so $\alpha \in \mathbb{Z}$, and we are safe.
2. Otherwise $\alpha = a + b\sqrt{2}$ with $b \neq 0$. Here $g(x) = (x-a)^2 - 2b^2$ is our minimal polynomial, so expanding coefficients tells us $2a \in \mathbb{Z}$ and $a^2 - 2b^2 \in \mathbb{Z}$.

   We need to know $a, b \in \mathbb{Z}$, which requires some pushing. We have $a \in \frac{1}{2}\mathbb{Z}$, so we would like a similar condition on b. Note $8b^2 = (2a)^2 - 4\left(a^2 - 2b^2\right) \in \mathbb{Z}$, so $2b \in \mathbb{Z}$ by checking denominators.

Now things collapse: if $a \notin \mathbb{Z}$, then $2a$ is odd, so $4a^2$ is odd, so $4\left(a^2 - 2b^2\right) = 4a^2 - 2 \cdot (2b)^2$ is also odd, which is a contradiction because $a^2 - 2b^2 \in \mathbb{Z}$. Thus, $a \in \mathbb{Z}$, which forces $b \in \mathbb{Z}$, finishing. ■

Remark 1.15. Life is not always so good. In $\mathbb{Q}(\sqrt{5})$, our integral closure is not $\mathbb{Z}[\sqrt{5}]$ because $\frac{1+\sqrt{5}}{2}$ is a root of $x^2 - x - 1 \in \mathbb{Z}[x]$. However, it turns out that $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is our integral closure.

1.2.3 A Better Integrality

Here are some definitions.

Definition 1.16 (Algebraic number)**.** An *algebraic number* is an element of the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$.

Definition 1.17 (Algebraic integer)**.** An *algebraic integer* is an algebraic number which is integral over $\mathbb{Z}$.

Definition 1.18 (Rational integer)**.** A *rational integer* is an element of $\mathbb{Z}$.

We want to talk about integral ring extensions, so we take the following definitions.

Definition 1.19 (Finite)**.** With $A \subseteq B$ rings, we define B to be *finite* over A or is a *finite A-algebra* if B is a finitely generated A-module.

Example 1.20. We see $\mathbb{Q}[t]$ is a finitely generated $\mathbb{Q}$-algebra (namely, generated by t), but it is not a finitely generated $\mathbb{Q}$-module, so it is not finite over $\mathbb{Q}$.

Example 1.21. If $K \subseteq L$ are fields, then L is finite over K if and only if $[L : K]$ is finite.

We want to show that the integral closure is actually a ring.

Definition 1.22 (Faithful)**.** An A-module M is *faithful* if $aM = 0$ implies $a = 0$. In other words, the A-action does a good job.

Proposition 1.23. Fix $A \subseteq B$ rings with $b \in B$. These are equivalent.

(a) b is integral over A.

(b) $A[b]$ is finite over A.

(c) There is a faithful $A[b]$-module M which is finitely generated as an A-module.

The last condition is the weirdest and, sadly, the most useful.

Remark 1.24. In fact, all $A[b]$-modules M with $A[b] \subseteq M \subseteq B$ are faithful because $1 \in M$ has $a \cdot 1 = 0$ implies $a = 0$.

Proof. We go in sequence.

- We start with (a) implies (b). If b is a zero of a monic polynomial of degree n in $A[x]$, then $A[b]$ is generated as an A-module by $\{1, b, \dots, b^{n-1}\}$ because higher powers can be reduced via the monic polynomial.
- Next we show (b) implies (c). Here $A[b]$ works.
- Now we show (c) implies (a). We use the determinant trick. Suppose $\{m_1, \dots, m_n\}$ generate M over A. Then for eack k, we can write

$$bm_k = \sum_{\ell=1}^{n} c_{k,\ell} m_\ell$$

for some coefficients $c_{k,\ell} \in A$. These $c_{k,\ell}$ give a matrix, which we name C. Letting C^* be the adjoint matrix, we have $CC^* = (\det C) I_n$.

Now $f(x) = \det(xI_n - C) \in A[x]$ is monic, which we hope is our monic polynomial witnessing the integrality of b. Defining $D := bI_n - C$, we see

$$D \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} bm_1 - \sum_{\ell=1}^{n} c_{1,\ell} m_\ell \\ \vdots \\ bm_n - \sum_{\ell=1}^{n} c_{1,\ell} m_\ell \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

In particular, $D^*D\langle m_1, \dots, m_n\rangle = 0$, so $D^*D = (\det D) I_n$ implies $(\det D)\langle m_1, \dots, m_n\rangle = 0$. However, $\det D = f(b)$, so in fact $f(b)(m_k) = 0$ for all k. And now we are in the home stretch: M is generated by the m_k, so $f(b)M = 0$, so $f(b) = 0$ because M is faithful. ∎

1.3 August 30

Reading for Wednesday is §1.3. There's also a handout on the discriminant of $x^n + ax + b$.

1.3.1 Integral Closures

Last time we (barely) showed the following.

Proposition 1.25. Let $A \subseteq B$ be rings and let $b \in B$. Then the following are equivalent.

(a) b is integral over A.

(b) $A[b]$ is finite over A.

(c) There is a faithful $A[b]$-module M which is finitely generated as an A-module.

Let's begin to reap the rewards of this. We want to show that the integral closure of a ring in a larger ring is in fact a ring, so we move towards there.

Lemma 1.26. Let $A \subseteq B$ be rings with $b_1, b_2 \in B$. If b_1 and b_2 are both integral over A, then $b_1 + b_1$ and $b_1 - b_2$ and $b_1 b_2$ are also integral over A.

Proof. We imitate the proof of algebraic-ness for fields. Because b_2 is integral over A, it will remain integral over $A[b_1]$ (simply inherit the same polynomial: $A[x] \subseteq A[b_1][x]$). Then $A[b_1, b_2]$ is finite over $A[b_1]$ by Proposition 1.25. The point is that we get the following tower of rings which are finite over each other so

that $A[b_1, b_2]$ is finite over A. (We leave working out this last assertion an exercise, though not a hard one.)

$$\begin{array}{c} A[b_1, b_2] \\ \text{finite} \,\big|\, \\ A[b_1] \\ \text{finite} \,\big|\, \\ A \end{array}$$

In particular, all elements of $A[b_1, b_2]$ are finite over A, so all the listed objects in the conclusion of our lemma are in fact integral over A. (Here we are taking $M = A[b_1, b_2]$ in Proposition 1.25.) ■

So we get the following corollary for our efforts.

Theorem 1.27. Let $A \subseteq B$ be rings. Then the integral closure of A in B is a subring of B containing A.

Proof. The previous lemma shows that the integral closure is in fact closed under our operations. To show that the integral closure contains A, we know that any $a \in A$ is a root of the polynomial $x - a \in A[x]$. ■

Remark 1.28. It is not necessary for the integral closure of A in B to be finite over A. For example, $\overline{\mathbb{Z}}$, which is the integral closure of $\mathbb{Z}$ in $\mathbb{C}$, is not finite over $\mathbb{Z}$.

We now take the following definition.

Definition 1.29 (Integrally closed)**.** Let $A \subseteq B$ be rings.

(a) If the integral closure of A in B equals A, then we say that A is *integrally closed*.

(b) Take A entire. Then A is *integrally closed* if it is integrally closed in its fraction field.

Last time we defined integral closure, so here we are defining what it means for the lower ring to be integrally closed.

We hope that the integral closure is in fact integrally closed. Let's show this.

Lemma 1.30. Let $A \subseteq B \subseteq C$ be rings. If B is integral over A and C is integral over B, then C is integral over A.

Proof. Let $c \in C$, which we know is integral over B. Then we are promised a monic polynomial in $B[x]$ such that

$$c^n + \sum_{k=0}^{n-1} b_k c^k = 0.$$

By induction, we see that $A[b_1, \ldots, b_n]$ is finite over A (add the elements one at a time), and in fact $A[b_1, \ldots, b_n, c]$ is finite over A as well because of the above polynomial. So it follows that c is integral over A by Proposition 1.25. ■

And this gives us our result.

Proposition 1.31. Let $A \subseteq B$ be rings. Then the integral closure of A in B is integrally closed in B.

Proof. Rename B to C and set B to the integral closure of A in C. ■

Proposition 1.32. Let A be an entire rings. Then the integral closure of A is integrally closed.

Proof. Take $B = \operatorname{Frac}(A)$ in the previous proposition. ∎

In fact, we have the following.

Proposition 1.33. Any factorial, entire ring A is integrally closed.

Proof. This essentially follows from Lemma 1.12. Let K be the fraction field of A and $\alpha \in K$ such that α is integral over A so that we want to show $\alpha \in A$. Well, we are promised a monic polynomial $f \in A[x]$ such that $f(\alpha) = 0$.

Note that then $(x - \alpha) \mid f(x)$ in $K[x]$ and both f and $x - \alpha$ are monic, and $f \in A[x]$, so we are forced into having $x - \alpha \in A[x]$. So it follows $\alpha \in A$. ∎

1.3.2 The $AKLB$ Setup

We will have the following situation a lot.

$$\begin{array}{ccc} B & \subseteq & L \\ \vdots & & | \\ A & \subseteq & K \end{array}$$

Here, A is integrally closed, K is its fraction field, L is a finite field extension of K, and B is the integral closure of A in L. In this case, note that because A is integrally closed, $B \cap K = A$. (All elements of B are integral over A.)

Remark 1.34. We define L before B because there are potentially "lots" of base rings

We hope that the $B \subseteq L$ is actually a fraction field containment.

Proposition 1.35. We have that L is the fraction field of B.

Proof. Let $\alpha \in L$. Then we show stronger: we show that there is a nonzero $a \in A$ such that $a\alpha \in B$. (In other words, the denominator lives in A.) Fix $f(x) \in K[x]$ the monic irreducible polynomial promised for α over K. For concreteness,

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0x^0$$

for constants $a_0, \dots, a_{n-1} \in K$. The point is that we can choose $a \in A$ equal to the product of the denominators of the $a_\bullet$ so that $a^n \cdot f(x) = 0$ reads

$$(a\alpha)^n + (aa_{n-1}(a\alpha)^{n-1} + (a^2a_{n-2})(a\alpha)^{n-2} + \cdots + (a^na_0) = 0.$$

So this is a monic polynomial for $a\alpha$ that lives in $A[x]$, so $a\alpha \in B$ because B is the integral closure of B in L. ∎

We take the following.

Proposition 1.36. Take the $AKLB$ setup. Assume that A is factorial, and let $\alpha \in L$. Then $\alpha \in B$ if and only if the irreducible polynomial for α in K lies in $A[x]$.

Proof. The backwards direction has nothing to show; the forward direction is by Gauss's lemma. ∎

1.3.3 Norm and Trace

We like measuring sizes of things, but in this class we want our sizes to be Galois-invariant. Here is one way we do this.

Definition 1.37 (Norm and trace)**.** Fix L/K a finite field extension, and let $\alpha \in L$. Viewing L as a K-vector space of dimension $[L:K] < \infty$, we define $T_\alpha : x \mapsto \alpha x$ as a K-linear transformation $L \to L$. This lets us define

$$\mathrm{N}_L^K(\alpha) := \det T_\alpha \qquad \text{and} \qquad \mathrm{T}_L^K(\alpha) = \operatorname{trace} T_\alpha.$$

The function N_L^K is called the *norm*, and the function T_L^K is called the *trace*.

Remark 1.38. Importantly, we have the following properties.

- $\mathrm{N}_K^L(\alpha) \in \alpha$ and $\mathrm{T}_L^K(\alpha) \in K$ because we are viewing these as K-linear transformations.
- For $\alpha \neq 0$ is equivalent to T_α is invertible, so $\alpha \neq 0$ is equivalent to $\mathrm{N}_L^K(\alpha) = 0$.
- N_L^K is multiplicative because $T_{\alpha\beta} = T_\alpha \circ T_\beta$, and the determinant is multiplicative.
- T_L^K is additive because $T_{\alpha+\beta} = T_\alpha + T_\beta$, and the trace is additive.

We also have the following definition.

Proposition 1.39. Fix an algebraic closure $\overline{K}$ of K, and let $\sigma_1, \dots, \sigma_d$ be distinct embeddings of L into $\overline{K}$ which fix K. (Note $d = [L:K]^{\text{sep}}$.) Then we have

$$\mathrm{N}_K^L(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha)^{[L:K]^{\text{insep}}} \qquad \text{and} \qquad \mathrm{T}_K^L(\alpha) = [L:K]^{\text{insep}} \sum_{k=1}^{d} \sigma_j(\alpha).$$

Here, $[L:K]^{\text{insep}}$ is the inseparable degree.

Proof. This is Proposition 2.6 in Neukirch or Chapter IV, §5 in Lang's *Algebra*. ■

The point of this is that the norm and the trace can detect integrality, albeit weakly.

Proposition 1.40. Take the $AKLB$ setup. If $\alpha \in B$, then $\mathrm{N}_L^K(\alpha)$ and $\mathrm{T}_K^L(\alpha)$ are in A.

Proof. The point is that, for each embedding $\sigma : L \to \overline{K}$ fixing K, we have that $\sigma\alpha$ is integral over A. Then we use the above characterization. ■

Corollary 1.41. If $M/L/K$ are finite extensions of fields, then $\mathrm{N}_K^L \circ \mathrm{N}_L^M = \mathrm{N}_K^M$ and $\mathrm{T}_K^L \circ \mathrm{T}_L^M = \mathrm{T}_K^M$.

Proof. Compose embeddings of $M \to L$ and of $L \to K$ to get all the embeddings of $M \to K$. ■

Corollary 1.42. If $L = K(\alpha)$ for some α with monic irreducible polynomial given by

$$f(x) = x^n - a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + (-1)^n a_0,$$

then $f(x) = \prod_{k=1}^{d} (x - \sigma_k(\alpha))^{[K(\alpha):K]^{\text{insep}}}$ so that $\mathrm{N}_K^L \alpha = a_0$ and $\mathrm{T}_K^L \alpha = a_{n-1}$.

Proof. Given in the statement. ∎

The above corollary is especially nice for quadratics.

1.4 September 1

Let's have some fun today.

1.4.1 Quadratic Number Rings

Here is our situation.

Definition 1.43 (Quadratic extension)**.** Fix D a squarefree integer which is not 1, and we fix $K = \mathbb{Q}(\sqrt{D})$, which we call a *quadratic* extension of $\mathbb{Q}$ because its degree over $\mathbb{Z}$ is two.

We want to understand our number rings.

Proposition 1.44. Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in $K = \mathbb{Q}(\sqrt{D})$ a quadratic extension of $\mathbb{Q}$. The story so far is that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{D}] & \text{else.} \end{cases}$$

Proof. Fix a D. In one direction, we note that $\sqrt{D} \in \mathcal{O}_K$ always, so $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_K$. Additionally, $\frac{1+\sqrt{D}}{2} \in \mathcal{O}_K$ when $D \equiv 1 \pmod 4$ because of the polynomial $x^2 - x + \frac{1-D}{4} \in \mathbb{Z}[x]$.

We now show the reverse direction. We note that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ by, say, Gauss's lemma. Fix $\alpha \mathcal{O}_K \setminus \mathbb{Q}$ so that $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$ and $b \neq 0$. Our monic irreducible polynomial is now

$$x^2 - 2ax + \left(a^2 - Db^2\right) = 0,$$

so we are forced to have $2a \in \mathbb{Z}$ and $a^2 - Db^2 \in \mathbb{Z}$. We have cases.

- We note that $a \in \mathbb{Z}$ implies $-Db^2 \in \mathbb{Z}$, which implies $b \in \mathbb{Z}$ by elementary number theory, so $\alpha \in \mathbb{Z}[\sqrt{D}]$.
- Otherwise, $a = a' + 1/2$ with $a' \in \mathbb{Z}$, so

  $$(2a' + 1)^2 - 4Db^2 = 4\left(a^2 - Db^2\right) \in 4\mathbb{Z}.$$

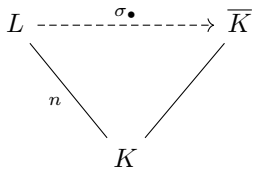
  It follows that $4Db^2$ is an integer, and in fact it is odd because $4a^2$ is odd. It follows that $2b$ is an odd integer, so we know $\alpha - \frac{1+\sqrt{D}}{2} \in \mathbb{Z}[\sqrt{D}]$. Thus, $\frac{1+\sqrt{D}}{2} \in \mathcal{O}_K$, and in fact $\mathcal{O}_K \subseteq \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$.

  However, this case only kicks in when $\frac{1-D}{4} \in \mathbb{Z}$ by taking the norm, so this case occurs if and only if $D \equiv 1 \pmod 4$.

So the statement follows. ∎

1.4.2 Discriminants

Let L/K be a finite, separable extension of fields of degree $n := [L : K]$. We fix a separable closure $\overline{K}/K$ and let $\sigma_1, \dots, \sigma_n$ be our (distinct) embeddings $L \to \overline{K}$. (Note that we do have n of these because L/K is separable.)



We have the following definition.

Definition 1.45 (Discriminant)**.** Let $\alpha_1, \dots, \alpha_n$ be a basis of L as a K-vector space. Then we define the *discriminant* of our basis as

$$\operatorname{disc}(\{\alpha_1, \dots, \alpha_n\}) := \det \begin{bmatrix} \sigma_1\alpha_1 & \cdots & \sigma_1\alpha_n \\ \vdots & \ddots & \vdots \\ \sigma_n\alpha_1 & \dots & \sigma_n\alpha_n \end{bmatrix}^2$$

Remark 1.46. The order of the basis doesn't matter: it will change the sign of the determinant at most, but we are squaring, so this doesn't have a real effect.

Example 1.47. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{D})$ a quadratic extension of K, and take the basis $\{1, \sqrt{D}\}$. Then we have

$$\operatorname{disc}(\{1, \sqrt{D}\}) = \det \begin{bmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{bmatrix}^2 = 4D.$$

Alternatively, we can take the basis $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$, which gives

$$\operatorname{disc}\left(\left\{1, \frac{1+\sqrt{D}}{2}\right\}\right) = \det \begin{bmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{bmatrix} = (-\sqrt{D})^2 = D.$$

Note that the example and definition doesn't care about integrality. But this is a number theory class, so we do.

Proposition 1.48. Fix everything as above. Then we claim

$$\operatorname{disc}(\{\alpha_1, \dots, \alpha_n\}) = \det \begin{bmatrix} \mathrm{T}_K^L(\alpha_1\alpha_1) & \cdots & \mathrm{T}_K^L(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{T}_K^L(\alpha_n\alpha_1) & \cdots & \mathrm{T}_K^L(\alpha_n\alpha_n) \end{bmatrix} \in K.$$

Proof. This follows by noting that

$$\begin{bmatrix} \sigma_1\alpha_1 & \cdots & \sigma_n\alpha_1 \\ \vdots & \ddots & \vdots \\ \sigma_1\alpha_n & \cdots & \sigma_n\alpha_n \end{bmatrix} \begin{bmatrix} \sigma_1\alpha_1 & \cdots & \sigma_1\alpha_n \\ \vdots & \ddots & \vdots \\ \sigma_n\alpha_1 & \cdots & \sigma_n\alpha_n \end{bmatrix} = \begin{bmatrix} \mathrm{T}_K^L(\alpha_1\alpha_1) & \cdots & \mathrm{T}_K^L(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{T}_K^L(\alpha_n\alpha_1) & \cdots & \mathrm{T}_K^L(\alpha_n\alpha_n) \end{bmatrix}$$

because the matrix multiplication at (k, ℓ) reads as

$$\sum_{k=1}^{n} \sigma_1(\alpha_k\alpha_\ell) = \mathrm{T}_K^L(\alpha_k\alpha_\ell).$$

Taking determinants of this equation finishes. ∎

Remark 1.49. Note that if we don't take the square in Definition 1.45, then we don't get an element of K as above. For concreteness, check the examples.

We would also like to show that the discriminant is nonzero.

Lemma 1.50. Fix everything as above. Suppose that $\{\alpha_k\}_{k=1}^n$ and $\{\beta_\ell\}_{\ell=1}^n$ both be bases for L over K. We define the matrix M to be our change of basis matrix: $\beta_k = \sum_\ell M_{k,\ell}\alpha_\ell$. Then we claim that

$$\operatorname{disc}(\{\beta_k\}_{k=1}^n) = (\det M)^2 \operatorname{disc}(\{\alpha_k\}_{k=1}^n).$$

Proof. Observe that

$$\begin{bmatrix} \sigma_1\beta_1 & \cdots & \sigma_n\beta_1 \\ \vdots & \ddots & \vdots \\ \sigma_1\beta_n & \cdots & \sigma_n\beta_n \end{bmatrix} = \begin{bmatrix} M_{11} & \cdots & M_{1n} \\ \vdots & \ddots & \vdots \\ M_{n1} & \cdots & M_{nn} \end{bmatrix} \begin{bmatrix} \sigma_1\alpha_1 & \cdots & \sigma_n\alpha_1 \\ \vdots & \ddots & \vdots \\ \sigma_1\alpha_n & \cdots & \sigma_n\alpha_n \end{bmatrix}$$

because

$$\sum_{\ell=1}^n M_{k,\ell}\sigma_k\alpha_\ell = \sigma_k \sum_{\ell=1}^n M_{k,\ell}\alpha_\ell = \sigma_k\beta_\ell.$$

Taking determinants and squaring finishes. ∎

We also have the following.

Lemma 1.51 (van der Monde)**.** Let A be a ring and let $\theta_1, \dots, \theta_n$ be in A. Then

$$\det \begin{bmatrix} \theta_1^0 & \cdots & \theta_n^0 \\ \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \cdots & \theta_n^{n-1} \end{bmatrix} = \prod_{k<\ell}(\theta_\ell - \theta_k).$$

Proof. We show that this is true in $\mathbb{Z}[x_1, \dots, x_n]$, which is enough because we have a map $\mathbb{Z}[x_1, \dots, x_n] \to A$ by $x_\bullet \mapsto \theta_\bullet$. However, we note that, for $k \neq \ell$, the determinant is a multiple of $(x_\ell - x_k)$ because $x_k = x_\ell$ sets two columns equal, making the determinant vanish. And in fact, the $(x_\ell - x_k)$ are distinct irreducibles.

So we use unique prime factorization to achieve

$$\prod_{k<\ell}(x_\ell - x_k) \;\Bigg|\; \det \begin{bmatrix} \theta_1^0 & \cdots & \theta_n^0 \\ \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \cdots & \theta_n^{n-1} \end{bmatrix}.$$

Comparing degrees, the degree of the left-hand side is $\frac{n(n-1)}{2}$, and the right-hand side has degree $0 + 1 + 2 \cdots + (n-1) = \frac{n}{n-1}2$, so we are off by at most a constant in $\mathbb{Q}$.

However, both sides have a $\theta_n^{n-1} \cdots \theta_2^1\theta_1^0$ term with coefficient 1: the determinant has coefficient here of $+1$ by multiplying along the diagonal, and the polynomial has coefficient here of $+1$ by taking all the positive terms of the product. ∎

This gives us the following corollary.

Corollary 1.52. Fix everything as above, and suppose that $L = K(\theta)$ so that $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ is a basis for L/K. Then

$$\operatorname{disc}\left(\{\theta^k\}_{k=1}^n\right) = \operatorname{disc} f(x),$$

where $f(x)$ is the irreducible polynomial for θ over K.

Proof. The point is that

$$\operatorname{disc}\left(\{\theta^k\}_{k=1}^n\right) = \det \begin{bmatrix} \sigma_1\theta^0 & \cdots & \sigma_n\theta^0 \\ \vdots & \ddots & \vdots \\ \sigma_1\theta^n & \cdots & \sigma_n\theta^n \end{bmatrix}^2 = \prod_{k<\ell}(\sigma_\ell\theta - \sigma_k\theta)^2 = \operatorname{disc} f(x),$$

where we have used the van der Monde determinant in the first equality. ■

In particular, we have the following.

Theorem 1.53. Because L/K is (finite) separable, we see that every basis has a nonzero discriminant. And in fact, the billinear form $\langle \alpha, \beta \rangle := \mathrm{T}_K^L(\alpha\beta)$ is non-degerenate. In other words, for each $\alpha \in L^\times$, the map $\beta \mapsto \langle \alpha, \beta \rangle$ and $\beta \mapsto \langle \beta, \alpha \rangle$ are nonzero.

Proof. Because L/K is a finite separable extension, it has a primitive element θ. Then we see that its irreducible polynomial $f(x) \in K[x]$ has no repeated roots (L/K is separable), so

$$\operatorname{disc}\left(\left\{\theta^k\right\}_{k=1}^n\right) = \operatorname{disc} f(x) \neq 0.$$

To talk about other bases, we simply use the change of basis matrix to go from another basis $\{\alpha_k\}_{k=1}^n$ to our power basis; the change of basis matrix is invertible and hence has nonzero determinant.

To show that the trace pairing is non-degenerate, it suffices to show that $\beta \mapsto \mathrm{T}_K^L(\alpha\beta)$ is a nonzero map for $\alpha \neq 0$; the other direction follows from commutativity of multiplication. Well, with $\alpha \neq 0$, we may extend $\alpha =: \alpha_1$ to a full basis $\{\alpha_k\}_{k=1}^n$. Then we see

$$0 \neq \operatorname{disc}\left(\{\alpha_k\}_{k=1}^n\right) = \det \begin{bmatrix} \mathrm{T}_K^L(\alpha_1\alpha_1) & \cdots & \mathrm{T}_K^L(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{T}_K^L(\alpha_n\alpha_1) & \cdots & \mathrm{T}_K^L(\alpha_n\alpha_n) \end{bmatrix}.$$

Because the determinant is nonzero, no particular row may be zero, and so in particular, the top row of $\mathrm{T}_K^L(\alpha_1\alpha_\bullet)$ must not be identically zero. So there is some $\beta := \alpha_k$ with $\mathrm{T}_K^L(\alpha\beta) \neq 0$. ■

1.5 September 3

1.5.1 The "Usual Picture"

We recall the following definition, but we revise it this time.

Definition 1.54 (Integrally closed)**.** A ring is *integrally closed* if and only if it is entire and integrally closed in its field of fractions.

The point here is that we are forcing our integrally closed rings to be entire.

Definition 1.55 (The "usual picture," or the $AKLB$ set-up)**.** Fix $\mathcal{O}_K$ an integrally closed ring and K its field of fractions. Further, fix L a finite extension of K, and we set $\mathcal{O}_L$ to be the integral closure of $\mathcal{O}_K$ in L. We also add the condition that $\mathcal{O}_K$ is Noetherian.

$$\begin{array}{ccc} \mathcal{O}_L & \subseteq & L \\ | & & | \\ \mathcal{O}_K & \subseteq & K \end{array}$$

We note that we showed on Monday that $L = \operatorname{Frac}(B)$.

Lots of fields we like satisfy the $AKLB$ set-up.

Example 1.56. Number fields satisfy the usual picture, where K/L is a finite field extension, and $\mathcal{O}_K$ and $\mathcal{O}_L$ are the integral closures of $\mathbb{Z}$ in K and L, respectively.

Example 1.57. Function fields K finite extensions $\mathbb{F}_p(t)$, where $\mathcal{O}_K$ is the integral closure of $\mathbb{F}_p[t]$ in K.

Example 1.58. We can also localize K and $\mathcal{O}_K$ by some multiplicative set and still satisfy the usual picture. Metric completions of these localizations also work.

We're goig to live in the $AKLB$ set-up for the rest of class.

1.5.2 Integral Bases

We would like to build an integral basis for $\mathcal{O}_L$ as an $\mathcal{O}_K$-module, which is an integral basis.

Lemma 1.59. There exists a basis of L/K contained in $\mathcal{O}_L$.

Proof. Let $\omega_1, \dots, \omega_n$ be some basis for L/K, where $n := [L : K]$. We showed on Monday that, for each $\omega_k \in L$, there is some $a_k \in \mathcal{O}_K$ such that $a_k\omega_k \in B$. So we can "multiply out" our denominators to get a basis $a_1\omega_1, \dots, a_n\omega_n \subseteq \mathcal{O}_L$. ∎

Now, for the rest of the class, we take A finite over $\mathbb{Z}$, or of finite type as an algebra over some field. We want to show that $\mathcal{O}_L$ is finite over $\mathcal{A}$, or is a localization.

Theorem 1.60. We show B is finite over A.

Proof. We do this case-by-case.

1. Fix K a number field with $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in K. We take $\omega_1, \dots, \omega_n$ a basis for L over K, and we fix $d := \operatorname{disc}(\{\omega_1, \dots, \omega_n\})$ so that $d \in \mathcal{O}_K \setminus \{0\}$.

   Because $d \neq 0$, we see that $\mathcal{O}_L \cong d\mathcal{O}_L$ as $\mathcal{O}_K$-modules and that $d\mathcal{O}_L \subseteq \mathcal{O}_L$. We claim that

   $$d\mathcal{O}_L \subseteq \bigoplus_{k=1}^{n} \mathcal{O}_K\omega_k.$$

   Take any $\alpha \in \mathcal{O}_L$ so that we may write

   $$\alpha = a_1\omega_1 + \cdots + a_n\omega_n, \qquad a_k \in K. \tag{$(*)$}$$

   Then we see that the $a_\bullet$ are the solution to the system of equations

   $$\sum_{\ell=1}^{n} \underbrace{\mathrm{T}_K^L(\omega_k\omega_\ell)}_{\in K} x_\ell = \mathrm{T}_K^L(\omega_k\alpha), \qquad k = 1, \dots, n$$

   wut

   by taking traces of $(*)$. So we use the determinant trick again. By Cramér's rule, this will have solutions which live in $d^{-1}\mathcal{O}_K$. So the claim follows because we can write

   $$d\alpha = \sum_{k=1}^{n} (da_k)\omega_k \in \bigoplus_{k=1}^{n} \mathcal{O}_K\omega_k.$$

   Now, because $\mathcal{O}_K$ is Noetherian, and the above shows that $d\mathcal{O}_L$ is a $\mathcal{O}_K$-submodule, it follows that $d\mathcal{O}_L$ is finitely generated over $\mathcal{O}_K$. So because $\mathcal{O}_K \cong d\mathcal{O}_K$, it follows that $\mathcal{O}_K$ is also finitely generated over $\mathcal{O}_K$.

2. Here $\mathcal{O}_K$ is finitely generated as an algebra over a field. This turns into "finiteness of the integral closure," for which we reference Eisenbud to kill.

3. If $\mathcal{O}_K$ is finitely generated as an algebra over $\mathbb{Z}$ with $p := \operatorname{char} K \neq 0$, then $\mathcal{O}_K$ is finitely generated as an algebra over $\mathbb{F}_p$, which goes to the previous case.

wut

4. If $\mathcal{O}_K$ is a localization of one of the rings we looked at earlier, then we are still done because integral closure commutes with localization, which is something we can check by hand.

There is some worry that we have not covered all cases where $\mathcal{O}_K$ is of finite type over $\mathbb{Z}$; positive characteristic for K was done in the third case, but $\operatorname{char} K = 0$ assumed we were a number field. This turns out to be okay when we assume that $\mathcal{O}_K$ is finite over $\mathbb{Z}$. ■

So we take the following definition.

Definition 1.61 (Full)**.** We say that a $\mathcal{O}_K$-submodule of L is *full* if it is not contained in any proper K-linear subspace of L. In other words, it spans L as a K-vector space.

So we have the following proposition.

Proposition 1.62. Fix M a nonzero finitely-generated $\mathcal{O}_L$-submodule of L. Then M is finitely generated as an $\mathcal{O}_K$-module and M is full.

Proof. Because M is finitely generated as an $\mathcal{O}_L$-module and $\mathcal{O}_L$ is finitely generated over $\mathcal{O}_K$, we see that M is finitely generated over $\mathcal{O}_K$.

For the other side, we note that $\mathcal{O}_L$ is full as a $\mathcal{O}_L$-module, so it follows that M is full; essentially, take an integral basis of L/K and multiply all elements by some $m \in M$. ■

So now when we continue with the class, we fix M to be a full, finitely generated $\mathcal{O}_K$-submodule of L.

Remark 1.63. This is more general the book because sometimes we will care about subrings of $\mathcal{O}_L$ and want integral bases for them too.

Anyways, we have the following definition.

Definition 1.64 (Integral basis)**.** An *integral basis* for $M \subseteq L$ over $\mathcal{O}_K$ is a set of elements $\{\omega_1, \dots, \omega_n\} \subseteq M$ such that the $\omega_\bullet$ are a basis for M as a free $\mathcal{O}_K$-module.

These don't always exist, but we like it when they do.

Proposition 1.65. The following are equivalent.

- M has an integral basis over $\mathcal{O}_K$.
- M is a free $\mathcal{O}_K$-module.
- M is a free $\mathcal{O}_K$-module of rank $n := [L : K]$.

Proof. This is in the handout. It is, in Vojta's words, "essentially trivial." ■

Proposition 1.66. If $\mathcal{O}_K$ is principal, then M has an integral basis.

wut

Proof. Note M has no torsion because $M \subseteq L$. Then we get our integral basis because M is a finitely generated module over a principal ideal domain. ■

In particular, if $\mathcal{O}_K = \mathbb{Z}$, then M has an integral basis, so rings of integers of number fields have an integral basis.

1.6 September 8

1.6.1 Integral Bases

We continue to work in the $AKLB$ set-up and that B is finite over A.

Definition 1.67 (Number field)**.** A *number field* is a finite field extension of $\mathbb{Q}$.

Definition 1.68 (Ring of integers)**.** The ring of integers $\mathcal{O}_K$ of a number field K is the integral closure of $\mathbb{Z}$ in K. It is finite over $\mathbb{Z}$ as we showed last time because integral basis of K is an integral bases of $\mathcal{O}_K$ over $\mathbb{Z}$.

Definition 1.69 (Discriminant)**.** The *discriminant* d_K of K is the discriminant of $\mathcal{O}_K$ over $\mathbb{Z}$. It is a well-defined nonzero rational integer.

Definition 1.70. Fix M a full, finitely generated A-submodule of L. If M has an integral basis (over A), then $\operatorname{disc} M$ is the discriminant of that integral basis.

Remark 1.71. By Lemma 1.50, this is well-defined up to multiplication by the square of a unit in A. In particular, when $A = \mathbb{Z}$, this is well-defined.

Proposition 1.72. Fix K a number field and $M \subseteq M'$ be full, finitely generated $\mathbb{Z}$-submodules of K. Then $[M' : M] < \infty$ and

$$d(M) = [M' : M]^2 d(M').$$

Proof. From Lemma 1.50, the point is that $[M' : M]$ is the determinant of a change-of-basis matrix from an integral basis of M to an integral basis of M'. Indeed, fix $\{\omega_k\}_{k=1}^n$ and $\{\omega_k\}_{k=1}^n$ be integral bases of M and M' respectively, where $n = [K : \mathbb{Q}]$. Fix N as the change-of-basis matrix satisfying

$$\begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix} = N \begin{bmatrix} \omega_1' \\ \vdots \\ \omega_n' \end{bmatrix}.$$

Then Lemma 1.50 implies that

$$d(M) = (\det N)^2 d(M').$$

So we need to show that $|\det N| = [M' : M]$. We can show this by integer Gaussian elimination on N, which makes N diagonal. ∎

blegh

Corollary 1.73. Fix $\theta \in \mathcal{O}_K$ such that the minimal polynomial of θ, which we name $f(x)$, over $\mathbb{Q}$ has squarefree discriminant. Then $\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$, and $d_{\mathbb{Q}(\theta)} = \operatorname{disc} f(x)$.

Remark 1.74. This is not always possible. For example, we cannot do this with any element of $\mathbb{Q}(\sqrt{2})$ because $d_{\mathbb{Q}(\sqrt{2})}$ is 8 and not squarefree.

Proof. Note that $\operatorname{disc} \mathbb{Z}[\theta] = \operatorname{disc} f(x)$ is squarefree, but

$$[\mathcal{O}_K : \mathbb{Z}[\theta]]^2 \mid \operatorname{disc} \mathbb{Z}[\theta],$$

so we are forced to have $[\mathcal{O}_K : \mathbb{Z}[\theta]] = 1$. So indeed, $\mathcal{O}_K = \mathbb{Z}[\theta]$. This works because $\mathbb{Z}[\theta]$ is full and lives in $\mathcal{O}_K$. ■

We can compute the ring of integers of a number field by looking for primitive integral elements whose minimal polynomial has squarefree discriminant. In general, we can try to find a chain of rings

$$\mathbb{Z}[\theta] = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_\ell = \mathcal{O}_K.$$

Example 1.75. We compute the ring of integers of $\mathbb{Q}(\sqrt{D})$ where D is squarefree and not 1. Fixing $\theta = \sqrt{D}$, we see that $\mathbb{Z}[\sqrt{D}]$ has discriminant $4D$, so the only square divisor to worry about is 4. It follows

$$[\mathcal{O}_K : \mathbb{Z}[\sqrt{D}]] \in \{1, 2\}.$$

Further, we see that $[\mathcal{O}_K : \mathbb{Z}[\sqrt{D}]] = 2$ if and only if $\mathcal{O}_K$ contains half of some element from $\mathbb{Z}[\sqrt{D}]$ (what else could we have?) if and only if one of $\frac{1}{2}, \frac{\sqrt{D}}{2}, \frac{1+\sqrt{D}}{2}$ lives in $\mathcal{O}_K$. Of course, $1/2, \sqrt{D}/2$ are not integral, so $[\mathcal{O}_K : \mathbb{Z}[\sqrt{D}]] = 2$ is equivalent to $\frac{1+\sqrt{D}}{2} \in \mathcal{O}_K$. This gives rise to the classification.

1.6.2 Dedekind

Here is our notion of Noetherian.

Proposition 1.76. Fix A a commutative ring. The following are equivalent.

(a) All ideals are finitely generated.

(b) A has the ascending chain condition: all ascending chains $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ must stabilize.

(c) Every nonempty collection of ideals contains a maximal element.

Proof. This is in any book on algebraic number theory, commutative algebra, or maybe even ring theory, so we outline.

- (a) implies (b) because the union of all the ideals is finitely generated.
- (b) implies (c) by set theory: showing the contrapositive, we can build our infinite strictly ascending chain because at no point can we ever hit a maximal ideal.
- (c) implies (a) because any ideal I gives rise to a collection of its sub-ideals which are finitely generated. A maximal element in this partially ordered set must be I. ■

Definition 1.77 (Noetherian)**.** A ring A is *Noetherian* if it satisfies one of the above equivalent conditions.

Definition 1.78 (Dedekind)**.** A ring A is *Dedekind* if it integrally closed (and hence entire), Noetherian, and of Krull dimension ≤ 1 (i.e., every nonzero prime is maximal).

1.7 September 10

1.7.1 Dedekind Rings

Recall the definition.

Definition 1.79 (Dedekind)**.** A *Dedekind ring* is an entire, integrally closed, Noetherian ring of Krull dimension at most 1.

Warning 1.80. Some authors require Krull dimension equal to 1 in the above definition, preventing fields from being Dedekind.

Example 1.81. We know $\mathbb{Z}$ is Dedekind. Also $k[t]$ for fields k is Dedekind.

Example 1.82. The localization $\mathbb{Z}_{\mathfrak{p}}$ for a nonzero prime ideal $\mathfrak{p}$ is still Dedekind.

Non-Example 1.83. The ring $k[x,y]$ for k nor $\mathbb{Z}[x]$ are not Dedekind because they have Krull dimension 2. In general, $A[t]$ for any Dedekind ring A (which is not a field) is not Dedekind because its Krull dimension is too big.

Of course, we're really doing number theory in this class, so let's do some number theory.

Theorem 1.84. Fix K a number field. Then $\mathcal{O}_K$ is a Dedekind ring.

Proof. We check these one at a time.

- We see $\mathcal{O}_K$ is integrally closed because it is the integral closure of $\mathbb{Z}$, which must be integrally closed.
- We see $\mathcal{O}_K$ is Noetherian because $\mathcal{O}_K$ is finite over $\mathbb{Z}$ (shown earlier), so $\mathcal{O}_K$ is of finite type over $\mathbb{Z}$, so we are done because we can realize $\mathcal{O}_K$ is smaller than some polynomial ring over $\mathbb{Z}$, finishing by the Hilbert basis theorem.
- We lastly check that $\mathcal{O}_K$ has Krull dimension 1.

  Let $\mathfrak{p}$ be a nonzero prime ideal, which we want to show is maximal. We note that the index $[\mathcal{O}_K : \mathfrak{p}]$ is finite by Proposition 1.72[2], but $\mathcal{O}_K/\mathfrak{p}$ is at least an integral domain, so being finite forces $\mathcal{O}_K/\mathfrak{p}$ to be a field, implying that $\mathfrak{p}$ is a maximal ideal, finishing. ∎

Remark 1.85. In general, in the $ALKB$ set-up, if A is Dedekind, then B is also Dedekind. This is in Eisenbud.

We take the following definition.

[2] Both $\mathcal{O}_K$ and $\mathfrak{p}$ are finitely generated $\mathcal{O}_K$-modules, so they are full. It follows that the discriminant of these is well-defined and nonzero, from which Proposition 1.72 gives the finiteness.

Definition 1.86 (Ideal operations)**.** Fix A an entire ring with fraction field K. Further fix I and J be A-submodules of K. Then we define

$$I + J := \{a + b : a \in I, b \in J\}$$

and

$$IJ = \left\{ \sum_{k=1}^{n} a_k b_k : n \in \mathbb{Z}, \{a_k\}_{k=1}^n \subseteq I, \{b_k\}_{k=1}^n \subseteq J \right\}.$$

In other words, $I + J$ is the set of all sums, and IJ is the submodule generated by products.

Note that we have called the above definition "ideal operations" but have defined them more generally for A-submodules of K.

Lemma 1.87 (Prime avoidance)**.** Fix A a ring. Fix $I_1, \dots, I_r$ and $\mathfrak{p}$ be A-ideals with $\mathfrak{p}$ prime. If $I_1 \cdots I_r \subseteq \mathfrak{p}$, then there is an I_k with $I_k \subseteq \mathfrak{p}$.

Proof. The idea is to show the contrapositive: if $I_k \not\subseteq \mathfrak{p}$ for each k, then each I_k has some $x_k \in I_k \setminus \mathfrak{p}$. Then we see that $x_1 \cdots x_r \notin \mathfrak{p}$ (otherwise, there would be some $x_k \in \mathfrak{p}$), so $x_1 \cdots x_r \in I_1 \cdots I_r \setminus \mathfrak{p}$, finishing. ■

For the rest of class, we take A a Dedekind ring and K its fraction field.

Theorem 1.88 (Unique prime facotrization of ideals)**.** Every nonzero A-ideal I has a prime factorization

$$I = \prod_{k=1}^{r} \mathfrak{p}_k,$$

where the $\mathfrak{p}_\bullet$. The primes $\{\mathfrak{p}_k\}_{k=1}^n$ is unique up to permutation.

Remark 1.89. This proof is similar to the proof that all PIDs are UFDs.

We pick up the following lemma, which essentially sets up our "induction."

Lemma 1.90. Every nonzero A-ideal I contains a product of noonzero prime ideals.

Proof. Suppose for the sake of contradiction that this is false; then the set of coutnerexamples is nonempty collection of ideals and hence contains a maximal element because A is Dedekind and hence Noetherian. Let I be such a maximal element.

Certainly $I \neq A$ because then it contains the empty product of primes; also, I itself is not prime, for then I would contain itself. So I, being not prime, promises elements $a, b \in A \setminus I$ and $ab \in I$. However, we know set

$$\mathfrak{a} = I + (a) \qquad \text{and} \qquad \mathfrak{b} = I + (b).$$

By maximality, $\mathfrak{a}$ and $\mathfrak{b}$ each contain a product of primes. But I also contains $\mathfrak{ab} = I + aI + bI + (ab) \subseteq I$, so I contains the product inside of $\mathfrak{a}$ times the product inside of $\mathfrak{a}$. This finishes. ■

With this in mind, we would next like to be able to divide out by ideals.

Definition 1.91 (Inverse ideals)**.** Fix I a nonzero A-ideal. Then we define

$$I^{-1} = \{x \in K : xI \subseteq A\}.$$

We can check by hand that I^{-1} is an A-submodule of K, containing A.

This gives us the following lemma.

Lemma 1.92. Fix $\mathfrak{p}$ a a nonzero prime ideal and I a nonzero A-ideal. Then $I\mathfrak{p}^{-1} \supsetneq I$.

Proof. We start by showing that $\mathfrak{p}^{-1} \neq A$, which is equivalent to $\mathfrak{p}^{-1} \supsetneq A$. Indeed, pick up $a \in \mathfrak{p} \setminus \{0\}$, and use the previous lemma to find primes $\{\mathfrak{p}_k\}_{k=1}^r$ whose product is contained in a. In fact, by well-ordering, we may take r as small as possible. It follows that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p},$$

so we have that $\mathfrak{p}_k \subseteq \mathfrak{p}$ for one of the $\mathfrak{p}_k$; without loss of generality, take $\mathfrak{p}_r = \mathfrak{p}_1$, and we see that $\mathfrak{p}_r = \mathfrak{p}$ by maximality. Because r is minimal, we have that $\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} \not\subseteq (a)$, so we are promised $b \in (a) \setminus \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$. Now, $b^{-1}a \notin A$, but $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r = (a)$ implies that $a^{-1}b\mathfrak{p} \subseteq A$. So $a^{-1}b \in A \setminus \mathfrak{p}^{-1}$, finishing.

We now return to actually proving the lemma. We pick up our promised $x \in \mathfrak{p}^{-1} \setminus A$. Suppose for the sake of contradiction $I\mathfrak{p}^{-1} \subseteq I$. Then $xI \subseteq \mathfrak{p}^{-1}I \subseteq I$. Then we see that xI is a faithful $A[x]$-submodule over K and is finitely generated over A because I is faithful and finitely generated over A. It follows that x is integral over A (it's generating a finitely generated A-module), forcing $x \in A$, which is a contradiction. ■

Remark 1.93. We just used the fact that A is integrally closed above!

We'll continue with the proof of existence next class.

1.8 September 13

I'm using Visual Studio Code today. I've also done some upgrades to my preamble. Let's see how I like it.

1.8.1 Unique Prime Factorization, Continued

Today, we will have A be a Dedekind domain with K its fraction field. Recall that we were proving the following statement.

Theorem 1.94. Every nonzero ideal $I \subseteq A$ admits a factorization

$$I = \prod_{k=1}^{r} \mathfrak{p}_k$$

into prime ideals $\{\mathfrak{p}_k\}_{k=1}^r$, which is unique up to order.

We left off proving the existence. Last time we showed the following.

Lemma 1.95. If $\mathfrak{p}$ is a nonzero prime ideal and I a nonzero ideal, then $I\mathfrak{p}^{-1} \supsetneq I$.

As a corollary, we have the following.

Corollary 1.96. We have that $\mathfrak{p}^{-1}\mathfrak{p} = A$ for each $\mathfrak{p}$ a nonzero prime.

Proof. We see that $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq A$, where we have applied the previous lemma. However, $\mathfrak{p}$ is maximal, so we must have $\mathfrak{p}\mathfrak{p}^{-1} = A$. ■

We now jump into the proof.

Proof of Existence in Theorem 1.94. Suppose for the sake of contradiction not. Then we can consider the set of all nonzero prime ideals which do not have a prime factorization and note that this nonempty collection must have a maximal element $\mathfrak{m}$.

Note that $\mathfrak{m} \neq A$ because A has the empty factorization, so we can actually put $\mathfrak{m}$ inside of a maximal (prime) ideal $\mathfrak{p} \subseteq \mathfrak{m}$. In fact, $\mathfrak{m} \neq \mathfrak{p}$ because otherwise we would have the single-prime factorization. We note that

$$\mathfrak{m}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$$

while $\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{p}^{-1}$. So by maximality of $\mathfrak{m}$, we see that $\mathfrak{m}\mathfrak{p}^{-1}$ has a prime factorization, but then we can multiply both sides of the factorization by $\mathfrak{p}$ to get a factorization for $\mathfrak{m}$. This is a contradiction, finishing the proof. ■

Proof of Uniqueness in Theorem 1.94. This is as usual. Suppose that we have

$$\prod_{k=1}^{r} \mathfrak{p}_k = \prod_{\ell=1}^{s} \mathfrak{q}_\ell$$

for primes $\mathfrak{p}_\bullet$ and $\mathfrak{q}_\bullet$. Then we see that $\mathfrak{p}_1$ must contain one of the primes on the other side, say $\mathfrak{q}_1$, which forces $\mathfrak{p}_1 = \mathfrak{q}_1$, so we can cancel both sides by this prime and finish by induction. ■

Remark 1.97. This is roughly why we name ideals "ideals": they are giving us this lovely unique prime factorization.

This gives us the following corollary.

Corollary 1.98. The monoid of nonzero ideals of A is a free monoid generated by nonzero prime ideals.

Proof. This follows directly from Theorem 1.94. ■

We would like to turn this monoid into a group.

1.8.2 Fractional Ideals

We have the following definition.

Definition 1.99. A fractional ideal I of A is a nonzero, finitely generated A-submodule of K. (If K is a number field, we might say that a fractional ideal of K is a fractional ideal of $\mathcal{O}_K$.)

We have the following claim.

Proposition 1.100. Let I be an A-submodule of K. The following are equivalent.

(a) I is a fractional ideal of A.

(b) I is nonzero, and there is a nonzero $c \in A$ such that $cI \subseteq A$.

(c) I is nonzero, and there is a $c \in K^\times$ such that $cI \subseteq A$.

Proof. We take these one at a time. We see that (a) implies (b) by noting I is certainly nonzero, and in fact, I is finitely generated (as a fractional ideal) by, say, $\{x_k\}_{k=1}^m$. Then we can multiply I by the product of the denominators in x_k to get inside of A.

We see that (b) implies (c) with no work.

Lastly, we show that (c) implies (a). Well, fix our promised c. Because cI is an A-ideal, it follows that cI is finitely generated because A is Noetherian. Thus, I is finitely generated by dividing out each generator by c. ■

This gives the following corollary.

Corollary 1.101. All nonzero ideals of A are fractional ideals.

Proof. Take $c = 1$ in (b) of Proposition 1.100. ■

Remark 1.102. To avoid confusion, we might say "integral ideals" for A-ideals.

Carrying unique prime factorization over to fractional ideals, we have the following theorem.

Theorem 1.103 (Unique factorization of fractional ideals)**.** Fix $\{\mathfrak{p}_\alpha\}_{\alpha\in\lambda}$ be the prime ideals of A. Then every fractional ideal I of A has a unique factorization into primes

$$I = \prod_{\alpha\in\lambda} \mathfrak{p}_\alpha^{e_\alpha},$$

where the $e_\alpha \in \mathbb{Z}$ and all but finitely many of the e_α are zero. In fact, I is integral if and only if $e_\alpha \geq 0$ for each α.

Proof. We leave this as an exercise. ■

So we get our group after all.

Theorem 1.104. The set of fractional ideals of A forms an abelian group under multiplication, isomorphic to

$$\bigoplus_{\mathfrak{p}} \mathbb{Z}.$$

If $A = \mathcal{O}_K$ for a number field K, then we denote this group by J_K.

This gives the following definition.

Definition 1.105. Fix $\mathfrak{a}$ and $\mathfrak{b}$ fractional ideals of A. Then we write $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a}^{-1}\mathfrak{b} \subseteq A$.

In fact, we see that $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a}I = \mathfrak{b}$ for some integral ideal I. We even get the following.

Lemma 1.106. Fix $\mathfrak{a}$ and $\mathfrak{b}$ fractional ideals. We have that $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$.

Proof. By definition, we see that $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a}^{-1}\mathfrak{b} \subseteq A$ if and only if $\mathfrak{b} \subseteq A\mathfrak{a} = \mathfrak{a}$. ■

We are interested in the simplest fractional ideals, the principal ones.

Definition 1.107 (Principal)**.** Fix $x \in K^\times$. Then we define $(x) := xA$ to be the fractional ideal generated by x. We say that a fractional ideal is *principal*, if it takes this form, and denote P_A (or P_K if K is a number field) to be the set of fractional ideals.

This gives us the following definition.

Definition 1.108 (Class group)**.** We define the *ideal class group* $\mathrm{Cl}_K := J_K/P_K$ for a number field K.

Note that we are requiring K to be a number field here because it turns out to behave better in this case. Namely, we will show, soon, that it is finite.

Anyways, we have another definition.

Definition 1.109. Fix $\mathfrak{a}$ and $\mathfrak{b}$ fractional ideals of A. Then we define

$$(\mathfrak{b} : \mathfrak{a}) := \{x \in K : x\mathfrak{a} \subseteq \mathfrak{b}\}.$$

For example, $(A : \mathfrak{p}) = \mathfrak{p}^{-1}$ for all nonzero primes $\mathfrak{p}$.

Be careful: this notation does not mean index! This gives us the following.

Lemma 1.110. We have that $(\mathfrak{b} : \mathfrak{a}) = \mathfrak{b}\mathfrak{a}^{-1}$.

Proof. This computation is by force. Note that $x \in \mathfrak{b}\mathfrak{a}^{-1}$ if and only if $(x) \subseteq \mathfrak{b}\mathfrak{a}^{-1}$ if and only if $\mathfrak{b}\mathfrak{a}^{-1} \mid (x)$ if and only if $\mathfrak{b} \mid (x)\mathfrak{a}$ if and only if $x\mathfrak{a} \subseteq \mathfrak{b}$ if and only if $x \in (\mathfrak{b} : \mathfrak{a})$. ■

While we're here, we pick up the Chinese remainder theorem.

Theorem 1.111 (Chinese remainder)**.** Let A be any commutative ring with ideals $I_1, \dots, I_n$ such that $I_k + I_\ell = A$ for each $k \neq \ell$. Then

$$\frac{A}{I_1 I_2 \cdots I_n} = \prod_{k=1}^{n} A/I_k.$$

Proof. Omitted. ■

Note that $\prod$ is distinct from $\bigoplus$. This doesn't make much of a difference here because we are going to be projecting into this proof, not including.

Remark 1.112. If A is a Dedekind ring, then I and J are relatively prime ideals if and only if they are coprime in the sense of prime factorization. Indeed, $I + J \neq A$ if and only if there exists $\mathfrak{p} \supseteq I + J$ if and only if $\mathfrak{p} \supseteq I$ and $\mathfrak{p} \supseteq J$ if and only if $\mathfrak{p} \mid I$ and $\mathfrak{p} \mid J$.

Theme 2
Minkowski Theory

2.1 September 15

2.1.1 Lattices

Fix V a vector space over $\mathbb{R}$ of dimension n. We have the following definitions.

Definition 2.1 (Lattice)**.** A *lattice* $\Lambda \subseteq V$ is a free, finitely generated additive subgroup. In other words, we can write

$$\Lambda = \bigoplus_{k=1}^{m} \mathbb{Z} v_k$$

for $\{v_k\}_{k=1}^m$ linearly independent vectors in V. We call $\{v_k\}_{k=1}^m$ a *basis* for Λ.

Definition 2.2 (Complete)**.** A lattice $\Lambda \subseteq V$ is *complete* or *full* if its basis spans V.

There is also the following geometric definition of a lattice.

Proposition 2.3. Lattices are equivalent to discrete subgroups of V.

Proof. This is surprisingly technical, so we will omit it. ∎

We would like to talk geometrically about V/Λ for lattices Λ.

Definition 2.4 (Fundamental mesh)**.** Given a complete lattice Λ with basis $\{v_k\}_{k=1}^n$, we define the set

$$V/\Lambda := \left\{ \sum_{k=1}^{n} x_k v_k : x_k \in [0,1) \right\},$$

which is the *fundamental mesh* of Λ.

Note that the fundamental mesh is not defined independent of a basis.

We would like to talk about the relative size of V/Λ, so we fix an additive Haar measure μ on V; i.e., we require that μ be translation-invariant. Equivalently, for any isomorphism $\varphi : V \to \mathbb{R}^n$, there exists a constant c such that $\mu(S) = c \operatorname{Vol}(\varphi(S))$ for any measurable S. This gives the following definition.

Definition 2.5 (Covolume)**.** We define the *covolume* of Λ as $\mu(V/\Lambda)$.

Note that this is well-defined, even for different bases of Λ because there is a change of basis matrix between our bases, which has determinant 1 and hence yields the same $\mu(V/\Lambda)$.

2.1.2 Minkowski Theory

We take the following definitions.

Definition 2.6 (Convex)**.** We say that a subset X of V is *convex* if and only if X contains the full line segment $\overline{AB}$ for any $A, B \in X$.

Definition 2.7 (Centrally symmetric)**.** We say that a subset X of V is *centrally symmetric* if and only if $v \in X$ implies that $-v \in X$.

All of the best sets are convex and centrally symmetric: circles, ellipses squares, not pentagons for some reason, etc.

The point of these definitions is the following.

Theorem 2.8 (Minkowski)**.** Let Λ be a complete lattice of V, and let X be a convex, centrally symmetric subset of V. If one of the following is true, then X contains a nonzero lattice point of Λ.

(a) $\operatorname{vol} X > 2^n \operatorname{covol}(V/\Lambda)$

(b) $\operatorname{vol} X \geq 2^n \operatorname{covol}(V/\Lambda)$ and X is compact.

Proof. We show (a); (b)) follows from taking some arbitrary intersections.

(a) The key fact is that $\operatorname{vol} \frac{1}{2}X = \frac{1}{2^n} \operatorname{vol} X > \operatorname{covol} \Lambda$.

Fix D some fundamental mesh for Λ. By tiling the plane by D, we see that

$$\frac{1}{2}X \subseteq \bigcup_{v \in \Lambda} (x + D) = V$$

so that

$$\frac{1}{2}X = \bigcup_{v \in \Lambda} (v + D) \cap \frac{1}{2}X.$$

Taking measures, we see that

$$\operatorname{covol} \Lambda < \operatorname{vol} \frac{1}{2}X \leq \sum_{v \in \Lambda} \operatorname{vol} \left((v + D) \cap \frac{1}{2}X \right).$$

Our measure is translation-invariant, so we may slide each $(v + D) \cap \frac{1}{2}X$ back along v to $D \cap (\frac{1}{2}X - v)$, implying

$$\operatorname{covol} \Lambda < \sum_{v \in \Lambda} D \cap (\tfrac{1}{2}X - v).$$

Now, if these $D \cap (\frac{1}{2}X - v)$ are all disjoint, then their summed measure is less than or equal to $\operatorname{vol} D = \operatorname{covol} \Lambda$, which is false!

So we have that two translates $D \cap (\frac{1}{2}X - v_1)$ and $D \cap (\frac{1}{2}X - v_2)$ which intersect for two distinct vectors v_1, v_2. Say v is in the intersection so that $v + v_1, v + v_2 \in \frac{1}{2}X$, implying $2v + 2v_1, -2v - 2v_2 \in X$ because X is centrally symmetric (!), so

$$v_1 - v_2 = \frac{(2v + 2v_1) + (-2v - 2v_2)}{2} \in X$$

because X is convex (!). To finish, we see that $v_1 - v_2 \in \Lambda$ and is nonzero because $v_1 \neq v_2$.

(b) Homework. ■

Remark 2.9. Pay careful attention to where each condition on X was used. They did each show up.

2.1.3 Geometry of Numbers

Fix K a number field, $n := [K : \mathbb{Q}]$, and $\mathfrak{a}$ some fractional ideal of K. Note that $\mathfrak{a}$ has a $\mathbb{Z}$-basis of length n because $c\mathfrak{a}$ is an $\mathcal{O}_K$-ideal for some $c \in K^\times$, and integral ideals have integral bases.

The point of this is that $\mathfrak{a}$ corresponds to some complete lattice in $K \hookrightarrow \mathbb{R}^n$; note this induces isomorphisms $K \cong \mathbb{Q}^n$ and $\mathfrak{a} \cong \mathbb{Z}^n$. In a good algebraic world, we would be able to set $V := K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^n$ and show that $K \hookrightarrow V$ is a complete lattice of V. This is not easy to do.

The more concrete way to do this is to consider the n embeddings $\tau_1, \dots, \tau_n$ of $K \hookrightarrow \mathbb{C}$ which fix $\mathbb{Q}$. This gives us a map $K \hookrightarrow \mathbb{C}^n$

$$k \longmapsto (\tau_1 k, \dots, \tau_n k).$$

Of course, $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$ is too big, but we can refine this. We do two things.

- We start by taking $\rho_1, \dots, \rho_r$ to be the $\tau_\bullet$ for which $\operatorname{im} \rho_\bullet \subseteq \mathbb{R}$ (i.e., the "real" embeddings). This immediately kills a dimension for each $\rho_\bullet$.
- As for the "complex" embeddings, we note that each τ_k for which $\operatorname{im} \tau_k \not\subseteq \mathbb{R}$ has a pair embedding $\overline{\tau_k}$ for which $\operatorname{im} \overline{\tau_k} \not\subseteq \mathbb{R}$. So all of our complex embeddings comes in these pairs; we take only one of them. Explicitly, fix $\sigma_1, \dots, \sigma_s$ be one of the complex embeddings in each conjugate pair.

This gives us the map $j : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ by

$$j : k \longmapsto (\rho_1 k, \dots, \rho_r k, \sigma_1 k, \dots, \sigma_s k).$$

We can compute that the $\mathbb{R}$-dimension of $\mathbb{R}^r \times \mathbb{C}^s$ is $r + 2s = n$ by counting our embeddings. We might abuse notation and write $j : K \hookrightarrow \mathbb{R}^n$.

Definition 2.10 ($K_{\mathbb{C}}$ and $K_{\mathbb{R}}$)**.** Fix everything above. Then we write fix $K_{\mathbb{C}} = \mathbb{C}^n$ and $K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$, where the *canonical measure* on $K_{\mathbb{R}}$ is 2^s times the standard measure on $\mathbb{R}^n$ pulled back to $K_{\mathbb{R}}$.

It is not clear what this 2^s is doing, but it is very important.

2.2 September 17

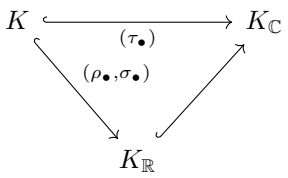
For today's lecture, K is a number field with $\mathcal{O}_K$ its ring of integers.

2.2.1 Motivating the Minkowski Measure

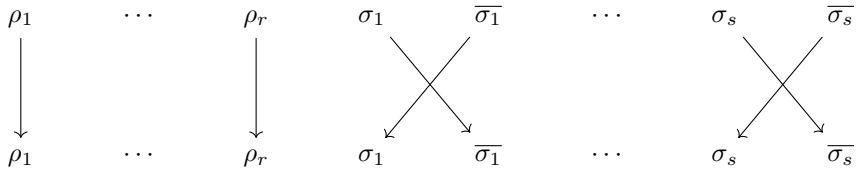
Recall that we have the map $K \hookrightarrow \mathbb{C}^n =: K_{\mathbb{C}}$ by $k \mapsto (\tau_1 k, \dots, \tau_n k)$ for each of our embeddings $\tau_\bullet$ as well as $j : K \hookrightarrow K_{\mathbb{R}}$ by

$$k \longmapsto (\rho_1 k, \dots, \rho_r k, \sigma_1 k, \dots, \sigma_s k).$$

By Galois theory, the points fixed by all the embeddings are those in K. Anyways, here is our diagram.



We recall that the canonical measure on $K_{\mathbb{R}}$ is the one obtained by pulling the measure on $\mathbb{R}^n$ back to $K_{\mathbb{R}}$ and multiplying by 2 on each complex coordinate. We also define $K_{\mathbb{C}} = \mathbb{C}^n$ with a "conjugation" symmetry $F : K_{\mathbb{C}} \to K_{\mathbb{C}}$ to do the following.



Each arrow here is complex conjugation; the point is that we want to swap the pairs of complex embeddings because they "should" be conjugate on K.

Let's try to motivate the multiplications by 2 in our canonical measure.

Lemma 2.11. Fix V a real vector space of dimension n with μ a Haar measure $\langle \cdot, \cdot \rangle$ a non-degenerate inner product. Further, fix $\alpha_1, \dots, \alpha_n$ a basis for $V/\mathbb{R}$ such that the measure of the "unit cube"

$$\mu\left(\left\{\sum_{k=1}^{n} t_k \alpha_k : t_\bullet \in [0,1]\right\}\right) = \left|\det \begin{bmatrix} \langle \alpha_1, \alpha_1 \rangle & \cdots & \langle \alpha_1, \alpha_n \rangle \\ \vdots & \ddots & \vdots \\ \langle \alpha_n, \alpha_1 \rangle & \cdots & \langle \alpha_n, \alpha_n \rangle \end{bmatrix}\right|^{1/2}. \tag{$*$}$$

Then $(*)$ holds for all $\alpha_1, \dots, \alpha_n$ whether or not these are a basis.

Proof. Let $\beta_1, \dots, \beta_n$ be arbitrary elements of V. If not a basis, then both sides of $(*)$ vanish. Otherwise, we fix B such that

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = B \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}.$$

Then, staring at $(*)$, we see that changing bases from the $\alpha_\bullet$ to $\beta_\bullet$ multiplies the right-hand side by $|\det B|$. On the other side, we see that

$$B \begin{bmatrix} \langle \alpha_1, \alpha_1 \rangle & \cdots & \langle \alpha_1, \alpha_n \rangle \\ \vdots & \ddots & \vdots \\ \langle \alpha_n, \alpha_1 \rangle & \cdots & \langle \alpha_n, \alpha_n \rangle \end{bmatrix} B^{\intercal} = \begin{bmatrix} \langle \beta_1, \beta_1 \rangle & \cdots & \langle \beta_1, \beta_n \rangle \\ \vdots & \ddots & \vdots \\ \langle \beta_n, \beta_1 \rangle & \cdots & \langle \beta_n, \beta_n \rangle \end{bmatrix},$$

so the right-hand side is also multiplied by $\sqrt{(\det B)^2}$. ∎

Example 2.12. Take $V = \mathbb{R}^n$ with μ the standard measure and $\alpha_1, \dots, \alpha_n$ our standard basis. Then both sides of $(*)$ are 1, so $(*)$ will always hold.

Lemma 2.11 justifies the multiplication by 2 in our canonical measure. Indeed, looking at the standard inner product

$$\langle (z_1, \dots, z_n), (w_1, \dots, w_n) \rangle = \sum_{k=1}^{n} z_k \overline{w_k}.$$

So now we embed $K_{\mathbb{R}}$ into $K_{\mathbb{C}}$, which is by

$$(x_1, \dots, x_r, z_1, \dots, z_s) \longmapsto (x_1, \dots, x_r, z_1, \overline{z_1}, \dots, z_s, \overline{z_s}).$$

For concreteness, we look at a single complex coordinate: here we take $\mathbb{C} \hookrightarrow \mathbb{C}^2$ by $z \mapsto (z, \overline{z})$. Then the inner product over at $\mathbb{C}^2$ looks like

$$\langle (z, \overline{z}), (w, \overline{w}) \rangle = z\overline{w} + \overline{z}w = 2\operatorname{Re}(z\overline{w}).$$

In particular, $z = x + iy$ and $w = u + iv$ gives $2\operatorname{Re}(z\overline{w}) = 2(xu + yv)$, which is twice the standard inner product we want when taking $x + iy \mapsto (x, y)$ as our embedding of $\mathbb{C} \to \mathbb{R}^2$.

In total, we see that the pull-back of the inner product on $K_{\mathbb{C}} \cong \mathbb{C}^n$ to $K_{\mathbb{R}}$ by defining $K_{\mathbb{R}}$ to be the F-invariants in $K_{\mathbb{C}}$, we get the standard inner product on $\mathbb{R}^n$ where each of the complex embeddings gets multiplied by 2. This is our canonical measure.

Remark 2.13. Note that we are using inner products as our interface with our measure instead of trying to pull back the measure from $K_{\mathbb{C}}$ directly. This is because the measure of $K_{\mathbb{R}}$ in $K_{\mathbb{C}}$ is zero.

2.2.2 More Geometry of Numbers

Now let's do some theory.

Proposition 2.14. Fix $j : K \hookrightarrow K_{\mathbb{R}}$ as above. Further, let $\mathfrak{a}$ be a nonzero $\mathcal{O}_K$-ideal. Then $j(\mathfrak{a})$ is a complete lattice of $K_{\mathbb{R}}$ with covolume $\sqrt{|d_K|} \cdot [\mathcal{O}_K : \mathfrak{a}]$, with respect to the canonical measure of $K_{\mathbb{R}}$.

Proof. Fix $\alpha_1, \dots, \alpha_n$ an integral basis for $\mathfrak{a}$ over $\mathbb{Z}$. Then we fix M to be the matrix defining the discriminant of $\mathfrak{a}$; because the discriminant of $\mathfrak{a}$ is nonzero, this matrix M has nonzero determinant, so $j(\mathfrak{a})$ will be a full lattice of $K_{\mathbb{R}}$.

It follows

$$\begin{aligned}
\operatorname{covol} j(\mathfrak{a}) &= \mu\left\{\sum_{k=1}^{n} t_k j(\alpha_k) : t_\bullet \in [0,1]\right\} \\
&\overset{(*)}{=} \left|\det \begin{bmatrix} \langle j\alpha_1, j\alpha_1\rangle & \cdots & \langle j\alpha_1, j\alpha_n\rangle \\ \vdots & \ddots & \vdots \\ \langle j\alpha_n, j\alpha_1\rangle & \cdots & \langle j\alpha_n, j\alpha_n\rangle \end{bmatrix}\right|^{1/2} \\
&= \left|\det\left[\sum_{m=1}^{n} \tau_m\alpha_k \cdot \overline{\tau_m\alpha_\ell}\right]_{k,\ell}\right|^{1/2} \\
&= |\det(M^{\intercal}\overline{M})|^{1/2} \\
&= |d(\mathfrak{a})|^{1/2} \\
&= \sqrt{|d_k|} \cdot [\mathcal{O}_K : \mathfrak{a}].
\end{aligned}$$

There are lots of details to fill in here, but I can't be bothered to try to figure out what's going on. ∎

Remark 2.15. The above holds more generally: $\operatorname{covol} j(\mathfrak{a}) = |d(\mathfrak{a})|^{1/2}$ for any full $\mathbb{Z}$-submodule $\mathfrak{a}$ of $\mathcal{O}_K$ as well as any full $\mathbb{Z}$-submodule of K because any full $\mathbb{Z}$-submodule we can lift to a submodule of $\mathcal{O}_K$ by multiplying by some integer a first.

On Monday, we will use this to show finiteness of the class group.

2.3 September 20

For today's class, we take K to be a number field.

2.3.1 Small Elements of Ideals

Recall the following statement from last lecture.

Proposition 2.16. Fix $\mathfrak{a}$ an integral $\mathcal{O}_K$-ideal. Then $j(\mathfrak{a})$ is a full lattice of $K_{\mathbb{R}}$ with covolume $\sqrt{|d_K|} \cdot [\mathcal{O}_K : \mathfrak{a}]$.

This will give us the following theorem.

Theorem 2.17. Fix $\mathfrak{a}$ a nonzero $\mathcal{O}_K$-ideal. Then the following are true.

(a) Fix $\{c_\tau\}_{\tau \in \operatorname{Hom}(K,\mathbb{C})}$ be a collection of positive real numbers such that $c_\tau = c_{\overline{\tau}}$ for each τ. Further suppose their product is
$$\prod_\tau c_\tau > A[\mathcal{O}_K : \mathfrak{a}],$$
where $A = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then there is a nonzero $a \in \mathfrak{a} \setminus \{0\}$ such that $|\tau a| < c_\tau$ for each τ.

(b) The above remains true if we replace both inequalities above with non-strict ones.

Note that the $c_{\overline{\tau}} = c_\tau$ condition exists because this is how τa also behaves.

Proof. We show these one at a time.

(a) Fix
$$X := \{(z_\tau) \in K_{\mathbb{R}} : |z_\tau| < c_\tau \text{ for each } \tau\}.$$
We can check that X is convex and centrally symmetric, so we would like to throw Minkowski's theorem at it. Well, computing the volume of X as various boxes in $\mathbb{R}$ and various disks in $\mathbb{C}$, and then adding in the 2^s from the canonical measure, we get
$$\operatorname{vol} X = 2^r \cdot 2^s \cdot \pi^s \prod_\tau c_\tau.$$
Using our bounds, this is larger than
$$\operatorname{vol} X > 2^r \left(2\pi \cdot \frac{2}{\pi}\right)^s \sqrt{|d_K|} \cdot [\mathcal{O}_K : \mathfrak{a}]. = \underbrace{2^r \cdot 4^s}_{2^n} \cdot \operatorname{covol} j(\mathfrak{a}),$$
so Minkowski's theorem does the job.

(b) This is on the homework. Essentially X above becomes compact. ∎

And now we get the following major step to finiteness of the class group.

Corollary 2.18. Every nonzero $\mathcal{O}_K$-ideal $\mathfrak{a}$ contains a nonzero element $a \in \mathfrak{a} \setminus \{0\}$ such that
$$[|\operatorname{N}_{\mathbb{Q}}^K(a)| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \cdot [\mathcal{O}_K : \mathfrak{a}].$$

Proof. Use Theorem 2.17 part (b): choose any good c_τ with product equal to $A[\mathcal{O}_K : \mathfrak{a}]$ (where here we have $A := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$ as usual) so that the nonzero element $a \in \mathfrak{a} \setminus \{0\}$ we are promised has
$$|\operatorname{N}_{\mathbb{Q}}^K(a)| = \prod_\tau |\tau a| < \prod_\tau c_\tau = A[\mathcal{O}_K : \mathfrak{a}],$$
which is what we wanted. ∎

We remark that, for $a \in \mathfrak{a}$ from the above corollary, we have that $(a) \subseteq \mathfrak{a}$ so that $\mathfrak{a} \mid (a)$, making $a\mathfrak{a}^{-1}$ an $\mathcal{O}_K$-ideal. In order to get finiteness of the class group, we would like to bound $[\mathcal{O}_K : a\mathfrak{a}^{-1}]$ because this would place all ideal classes in a box.

For this, we need the following tool.

2.3.2 Norms of Ideals

We have the following lemma.

Lemma 2.19. For all nonzero $a \in \mathcal{O}_K \setminus \{0\}$, we have that

$$[\mathcal{O}_K : (a)] = \left|\mathrm{N}_{\mathbb{Q}}^K(a)\right|.$$

Proof. Fix $\omega_1, \dots, \omega_n$ be an integral $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then

$$\{a\omega_1, \dots, a\omega_n\}$$

is also an integral basis for (a). Comparing discriminants, we have that

$$d((a)) = \det \begin{bmatrix} \tau_1(a\omega_1) & \cdots & \tau_1(a\omega_n) \\ \vdots & \ddots & \vdots \\ \tau_n(a\omega_1) & \cdots & \tau_n(a\omega_n) \end{bmatrix}^2 = \left(\prod_\tau \tau(a)^2\right) \det \begin{bmatrix} \tau_1(\omega_1) & \cdots & \tau_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \tau_n(\omega_1) & \cdots & \tau_n(\omega_n) \end{bmatrix}^2,$$

by factoring out $\tau_\bullet(a)$ from each column. However, this right-hand side is $|\mathrm{N}_{\mathbb{Q}}^K(a)|^2 d(\mathcal{O}_K)$, so it suffices to recall that

$$d((a)) = [\mathcal{O}_K : (a)]^2 d(\mathcal{O}_K)$$

from much earlier, finishing. ∎

With this in mind, we generalize norms of elements to norms of ideals as follows.

Definition 2.20 (Absolute norm)**.** The *absolute norm* of a nonzero $\mathcal{O}_K$-ideal I is $\mathrm{N}(I) := [\mathcal{O}_K : I]$.

This norm turns out to behave as we want.

Proposition 2.21. Given nonzero $\mathcal{O}_K$-ideals $\mathfrak{a}$ and $\mathfrak{b}$, we have $\mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b}) = \mathrm{N}(\mathfrak{ab})$.

Proof. We use the Chinese remainder theorem; we have the following cases.

1. If $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime (i.e., $\mathfrak{a}+\mathfrak{b} = \mathcal{O}_K$), then $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{ab}$, and we finish by the Chinese remainder theorem:
$$\frac{\mathcal{O}_K}{\mathfrak{ab}} = \frac{\mathcal{O}_K}{\mathfrak{a}\cap\mathfrak{b}} \cong \frac{\mathcal{O}_K}{\mathfrak{a}} \times \frac{\mathcal{O}_K}{\mathfrak{b}},$$
which gives what we wanted.
2. By unique prime factorization, it remains to deal with prime-powers. Take $\mathfrak{a} = \mathfrak{p}^k$ and $\mathfrak{b} = \mathfrak{p}^\ell$ for some prime $\mathfrak{p}$. By induction, we may take $\ell = 1$ and then strip off powers of $\mathfrak{p}$ from $\mathfrak{b}$ one at a time.
So we have to show that
$$\mathrm{N}\left(\mathfrak{p}^{k+1}\right) = \mathrm{N}(\mathfrak{p}^K)\,\mathrm{N}(\mathfrak{p}).$$
However, $\mathcal{O}_K/\mathfrak{p}^{k+1}$ is principal (this was on the homework), so we can find $\pi \in \mathcal{O}_K$ (namely, $\pi \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$) such that $(\pi \mod \mathfrak{p}^{k+1}) = \mathfrak{p}^k/\mathfrak{p}^{k+1}$. It follows that the map
$$x \mapsto ax + \mathfrak{p}^{k+1}$$
is surjective because $\mathcal{O}_K/\mathfrak{p}^{k+1}$ is principal, with kernel containing $\mathfrak{p}$ (because $a \in \mathfrak{p}^k$) but not containing 1, so we have induced an isomorphism
$$\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^{k+1}/\mathfrak{p}^k.$$
So we can compute the indices
$$[\mathcal{O}_K : \mathfrak{p}] = \left[\mathfrak{p}^{k+1} : \mathfrak{p}^k\right] = \frac{\left[\mathcal{O}_K : \mathfrak{p}^{k+1}\right]}{\left[\mathcal{O}_K : \mathfrak{p}^k\right]},$$
which is what we wanted. ∎

2.3.3 Finiteness of the Class Group

Now we have the following corollary, finishing up.

Corollary 2.22. Every ideal class in K contains an integral ideal of index at most

$$A_K := \left(\frac{2}{\pi}\right)^2 \sqrt{|d_K|}.$$

Remark 2.23. We can improve the constant to $M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_k|}$ with some effort.

Proof. Fix an ideal class C with $\mathfrak{a} \in C^{-1}$ an integral ideal, and find some $a \in \mathfrak{a}$ such that

$$\left|\mathrm{N}_{\mathbb{Q}}^K(a)\right| \le A[\mathcal{O}_K : \mathfrak{a}].$$

Now, $a\mathfrak{a}^{-1} = (a)\mathfrak{a}^{-1}$ is an integral ideal in the original ideal class C because $a \in \mathfrak{a}$. We note that We can bound this norm by

$$\left[\mathcal{O}_K : a\mathfrak{a}^{-1}\right] = \mathrm{N}(a\mathfrak{a}^{-1}) = \frac{\mathrm{N}((a))}{\mathrm{N}(\mathfrak{a})} = \frac{\left|\mathrm{N}_{\mathbb{Q}}^K(a)\right|}{[\mathcal{O}_K : \mathfrak{a}]} \le A.$$

Note that we had to use multiplicativity of the ideal norm to write $\mathrm{N}(a\mathfrak{a}^{-1})\,\mathrm{N}(\mathfrak{a}^{-1}) = \mathrm{N}((a))$. ∎

We are almost at the finish line.

Lemma 2.24. Suppose we have a constant $B = B_K$ depending only K such that every ideal class of K contains an integral ideal of norm bounded by B. Then Cl_K is finite.

Proof. We have to show that there only finite many ideals of norm bounded by B so that there are only finitely many candidates for distinct ideal classes. For this, it suffices to show that there are finitely many ideals of a particular norm m with $0 < m \le B$.

excuse me?

Well, fix $\mathfrak{a}$ an integral domain of index m. Then it follows $\mathfrak{a} \supseteq m\mathcal{O}_K$, so $\mathfrak{a}$ is an additive subgroup of $\mathcal{O}_K/m\mathcal{O}_K \cong (\mathbb{Z}/m\mathbb{Z})^n$. But there are only finitely many elements of $(\mathbb{Z}/m\mathbb{Z})^n$, so only finitely many additive subgroups, so only finitely many options for $\mathfrak{a}$. ∎

And here we are.

Theorem 2.25. We have that Cl_K is finite.

Proof. This follows from the above discussion. ∎

This lets us have the following definition.

Definition 2.26 (Class number)**.** The *class number* of a number field K is $h_K := \#\,\mathrm{Cl}_K$.

Example 2.27. For $K = \mathbb{Q}(\sqrt{-7})$, we have that $h_K = 1$. Here we have $n = 2, = 0, s = 1$, and $d_K = -7$. It follows that every ideal class contains an integral ideal with norm at most

$$M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1 \sqrt{|-7|} = \frac{2}{\pi}\sqrt{7} < 2.$$

However, there is only ideal with index 1, so our only ideal class is the principal one.

2.4 September 22

The Minkowski grind continues. Fix K a number field, as usual.

2.4.1 Setting up the Diagram

We want to study $\mathcal{O}_K^\times$. We use the following commutative diagram.

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{C}}^\times & \xrightarrow{\ell} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle \mathrm{N}_{\mathbb{Q}}^K} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{C}^\times & \xrightarrow{z\mapsto -\log|z|} & \mathbb{R} \end{array}$$

Here, j is the restriction of $K \hookrightarrow K_{\mathcal{C}}$, by

$$h = (\tau_1, \dots, \tau_n) = (\rho_1, \dots, \rho_r, \sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_2}).$$

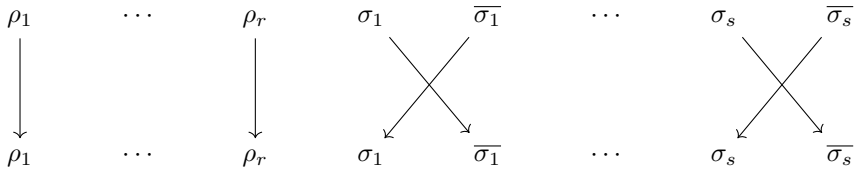
The new map here is ℓ, which takes $z \mapsto -\log|z|$ to each coordinate.

> **Remark 2.28.** As abuse of notation, given $f : A \to B$ and $g : C \to D$, we write $f \times g : A \times C \to B \times D$. Professor Vojta is making a pretty big deal of this.

Continuing, N takes a tuple in $K_{\mathbb{C}}^\times$ to the product of the coordinates, so that $K^\times \to \mathbb{Q}^\times \hookrightarrow \mathbb{C}^\times$ commutes. Lastly, the trace $\mathrm{Tr} : \prod_\tau \mathbb{R} \to \mathbb{R}$ takes the sum of coordinates.

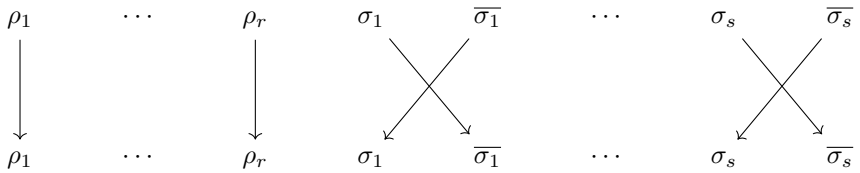
Lots of these groups turn out to have an involution, some of which are interesting. We name all of these F by abuse of notation.

- On $K^\times, \mathbb{Q}^\times$, and $\mathbb{R}$, we choose the identity map.
- On $\mathbb{C}^\times$, we choose conjugation $z \mapsto \overline{z}$.
- On $K_{\mathbb{C}}^\times$, we conjugate the ρ components and conjugate and swap the complex components. In other words, we take



  where each vertical line downwards is complex conjugation.

- On $\prod_\tau \mathbb{R}$, we do nothing on the ρ components and swap the σ components. In other words, we take



  where each vertical line downwards is the identity. (Technically, we could make this complex conjugation, which does nothing on $\mathbb{R}$.)

We can check that each arrow in our commutative diagram preserves the F-invariants; in fact, each of these maps commutes with F.

- The embedding $\mathbb{Q}^\times \hookrightarrow \mathbb{C}^\times$ does nothing.
- The map $\mathbb{C}^\times \to \mathbb{R}$, complex conjugation does nothing to $z \mapsto -\log|z|$.
- The map $K^\times \to K_{\mathbb{C}}^\times$, we see that F does nothing to the ρ coordinates, and the output of j has the $\sigma_\bullet$ and $\overline{\sigma_\bullet}$ coordinates conjugated.
- The map $K_{\mathbb{C}}^\times \to \prod_\tau \mathbb{R}$ doesn't care about the conjugation happening in $K_{\mathbb{C}}^\times$, but the swapping in $K_{\mathbb{C}}^\times$ is preserved in $\prod_\tau \mathbb{R}$ by construction of F on $\prod_\tau \mathbb{R}$.
- The vertical map $K^\times \to \mathbb{Q}^\times$ is okay because F acts trivially on both.
- The map $K_{\mathbb{C}}^\times \to \mathbb{C}^\times$ is okay because, when taking the product of all elements, we can conjugate before in $K_{\mathbb{C}}^\times$ or after in $\mathbb{C}^\times$. (The swapping does not matter because we are just taking the product of everything.)
- Lastly, the map $\prod_\tau \mathbb{R} \to \mathbb{R}$ we see that F merely permutes the coordinates of $\prod_\tau \mathbb{R}$, which Tr does not care about when taking the sum of everyone. So we are still safe.

2.4.2 Expanding the Diagram

So, taking the F invariants $X \mapsto X^F$ of our commutative diagram gives another commutative diagram, as follows.

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{\ell} & (\prod_\tau \mathbb{R})^F \\ \downarrow{\scriptstyle \mathrm{N}_{\mathbb{Q}}^K} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow{z\mapsto -\log|z|} & \mathbb{R} \end{array}$$

Namely, we recall that the F-invariants of $K_{\mathbb{C}}$ were in (natural) bijection with $K_{\mathbb{R}}$,[1] and the F-invariants of $\mathbb{C}$ are real numbers. We remark that

$$\left(\prod_\tau \mathbb{R}\right)^F = \{(t_1, \dots, t_r, u_1, u_1, \dots, u_s, u_s) : t_\bullet, u_\bullet \in \mathbb{R}\}$$

is isomorphic to $\mathbb{R}^{r+s}$ by

$$(t_1, \dots, t_r, u_1, u_1, \dots, u_s, u_s) \mapsto (t_1, \dots, t_r, 2u_1, \dots, 2u_s).$$

Note that we are doubling here so that the above map commutes with the trace (i.e., the sum of the coordinates is preserved). To be explicit, we write that the composite $K_{\mathbb{R}}^\times \to (\prod_\tau \mathbb{R})^F \to \mathbb{R}$ is

$$(x_{\rho_1}, \dots, x_{\rho_r}, x_{\sigma_1}, x_{\overline{\sigma_1}}, \dots, x_{\overline{\sigma_s}}, x_{\overline{\sigma_s}}) \mapsto \left(-\log|x_{\rho_1}|, \dots, -\log|x_{\rho_r}|, -\log|x_{\sigma_1}|^2, \dots, -\log|x_{\sigma_s}|^2\right).$$

Now, to focus on $\mathcal{O}_K$, we restrict $K^\times$ to $\mathcal{O}_K^\times$ as follows.

$$\begin{array}{ccccc} \mathcal{O}_K & \xrightarrow{\quad\lambda\quad} & S & \xrightarrow{\quad\quad} & H \\ \subseteq & & \subseteq & & \subseteq \\ K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{\ell} & (\prod_\tau \mathbb{R})^F \\ \downarrow{\scriptstyle \mathrm{N}_{\mathbb{Q}}^K} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow{z\mapsto -\log|z|} & \mathbb{R} \end{array}$$

[1] In fact, arguably we should define $K_{\mathbb{R}}$ as the F-invariants of $K_{\mathbb{C}}$.

Here, we define

$$S := \{y \in K_{\mathbb{R}}^{\times} : \mathrm{N}(y) = \pm 1\}.$$
$$H := \left\{(x_\tau) \in \left(\prod_\tau \mathbb{R}\right)^F : \mathrm{Tr}(x_\tau) = 0\right\}.$$

We might call S the "norm ± 1 hypersurface" and H the "trace 0 hyperplane." And indeed, $j : K^{\times} \to K_{\mathbb{R}}^{\times}$ does indeed take $\mathcal{O}_K^{\times}$ to the elements of norm 1 in $K_{\mathbb{R}}^{\times}$, so we can restrict j to $\mathcal{O}_K \to S$. Similarly, S upon taking logs will map straight to the origin.

2.4.3 Doing Number Theory

It will happen that $\mathcal{O}_K^{\times}$ maps into a lattice $\Gamma := \mathrm{im}\,\lambda$. So let's actually start doing some number theory.

Definition 2.29 (Roots of unity)**.** Fix μ_K to be the roots of unity in K. Note that $\mu_K \subseteq \mathcal{O}_K^{\times}$.

Lemma 2.30. We claim that $\ker \lambda = \mu_K$.

Proof. In one direction, suppose $\zeta \in \mu_K$. Then we as remark have $\zeta \in \mathcal{O}_K$ and in fact $\zeta^{-1} \in \mathcal{O}_K$. However, H is torsion-free, so we may write

$$\lambda(\zeta) = \frac{1}{m}\lambda(\zeta^m) = \frac{1}{m}\lambda(1) = 0.$$

(Here, $\lambda(1) = 0$ because surely the identity lives in the kernel.)

In the other direction, suppose $\zeta \in \ker \lambda$. Well, then we have that $|\tau\zeta| = 1$ for each $\tau \in \mathrm{Hom}(K, \mathbb{C})$, which turns out to be a problem. Indeed, we have the following.

Lemma 2.31. We claim that

$$\{\alpha \in \mathcal{O}_K : |\tau\alpha| \le c_\tau \text{ for all } \tau\}$$

is a finite set for any sequence $\{c_\tau\}$ of positive real numbers.

Proof. Note that $j(\mathcal{O}_K)$ is a discrete subgroup of $K_{\mathbb{R}}$ as when we studied additive Minkowski theory, so $j(\mathcal{O}_K)$ is a lattice and therefore contains only finitely many elements in the given bounded set. ∎

It follows that

$$\ker \lambda \subseteq \{\alpha \in \mathcal{O}_K : |\tau\alpha| \le 1 \text{ for all } \tau\}$$

is finite, so $\ker \lambda$ is finite, so all its elements have finite order. ∎

Remark 2.32. We note that the above proof also tells us that μ_K is finite, for free.

So now that we have the above, we get the following short exact sequence.

$$1 \to \mu_K \to \mathcal{O}_K \to \Gamma \to 1$$

Next time we will show that Γ is a complete lattice in H. For now, we'll show it's a lattice.

Lemma 2.33. We have that Γ is discrete in H.

Proof. Our lemma earlier showed that

$$\{\alpha \in \mathcal{O}_K : |\tau\alpha| \le c \text{ for all } \tau\}$$

is finite for any given $c > 0$. Transporting this through λ, we get that

$$\{(x_1, \dots, x_{r+s}) \in \mathbb{R}^{r+s} : |x_k| < c \text{ for all } k\}$$

is still finite because the kernel we just exhibited was finite. ■

Lemma 2.34. For any given $a \in \mathbb{Z}$, there are only finitely many $\alpha \in \mathcal{O}_K$ such that $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = a$, up to multiplication by a unit.

Here we need the last caveat because there might be infinitely many units.

Proof. We note that, given $\alpha, \beta \in \mathcal{O}_K^{\times}$, we see α/β is a unit if and only if $(\alpha) = (\beta)$, so we get the result by noting there are only finitely many ideals of $\mathcal{O}_K$ with norm $|a|$. In other words, we are counting α with $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = a$, up to unit, by checking the ideal they generate, of which we know there are finitely many. ■

2.5 September 24

From last time, we have K a number field, and we had the following diagram.

$$\begin{array}{ccccc}
\mathcal{O}_K & \xrightarrow{\quad} & S & \xrightarrow{\quad} & H \\
\subseteq & & \subseteq & & \subseteq \\
K^{\times} & \xrightarrow{j} & K_{\mathbb{R}}^{\times} & \xrightarrow{\ell} & (\textstyle\prod_{\tau} \mathbb{R})^{F} \\
\downarrow{\scriptstyle \mathrm{N}_{\mathbb{Q}}^{K}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\
\mathbb{Q}^{\times} & \hookrightarrow & \mathbb{R}^{\times} & \xrightarrow{z \mapsto -\log|z|} & \mathbb{R}
\end{array}$$

2.5.1 Talking Units

We also recall that we had the following lemma.

Lemma 2.35. For any given $a \in \mathbb{Z}$, there are only finitely many $\alpha \in \mathcal{O}_K$ such that $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = a$, up to multiplication by a unit.

In fact, from the proof we can take the slightly stronger version with the absolute value.

Lemma 2.36. For any given $a \in \mathbb{Z}$, there are only finitely many $\alpha \in \mathcal{O}_K$ such that $\left|\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)\right| = a$, up to multiplication by a unit.

Proof. Use the same proof as before. ■

Anyways, we continue with the lemmas.

Lemma 2.37. For every $\tau_0 : K \to \mathbb{C}$, there is a unit $\alpha \in \mathcal{O}_K^\times$ such that $|\tau u| < 1$ for each $\tau \notin \{\tau_0, \overline{\tau_0}\}$.

The idea here is that α must have large τ_0 and $\overline{\tau_0}$ component but small component at all other embeddings.

Proof. We construct an infinite sequence

$$\alpha_0, \alpha_1, \dots$$

with norm $\left|\mathrm{N}_{\mathbb{Q}}^K \alpha_\bullet\right| \le \left(\frac{2}{\pi}\right) \sqrt{|d_K|} =: A$ while $|\tau\alpha_{k+1}| < |\tau\alpha_k|$ for each $\tau \notin \{\tau_0, \overline{\tau_0}\}$.

Indeed, we do induction. We start with $\alpha_0 := 1 \le A$.[2] Then, given α_k, we choose any

$$c_\tau \in (0, |\tau\alpha_k|)$$

for each $\tau \notin \{\tau_0, \overline{\tau_0}\}$; we also force $c_\tau = c_{\overline{\tau}}$. It remains to choose

$$c_{\tau_0} = c_{\overline{\tau_0}} > 0,$$

wut

which we choose large enough so that $\prod_\tau c_\tau = A$. Then Minkowski theory provides us with an $\alpha_{k+1} \in \mathcal{O}_K \setminus \{0\}$ such that

$$|\tau\alpha_{k+1}| < c_\tau.$$

Now, to finish the proof, by the previous lemma, these $\alpha_\bullet$ lie in finitely many multiplicative cosets of $\mathcal{O}_K/\mathcal{O}_K^\times$ (they all have norm less than or equal to A), so there are $m > n \ge 0$ such that $\alpha_m/\alpha_n \in \mathcal{O}_K^\times$. This is what we wanted because

$$|\tau(\alpha_m/\alpha_n)| < 1$$

by construction of our sequence. ∎

Remark 2.38. There are some nice pictures associated with drawing the trace-zero hyperplane in $\mathbb{R}^{r+s}$. I won't TeX these because I cannot be bothered.

Now, when we look at the trace-0 hyperplane, our chosen elements above have one positive sign after taking $\log$ while the other ones are negative. Geometrically, these look like good candidates as a basis for our hyperplane.

Lemma 2.39. Fix m a positive integer with $A \in \mathbb{R}^{m \times m}$ an $m \times m$ matrix. We assume the following.

(i) All the row sums of A vanish.

(ii) All entries off the main diagonal are negative.

Then it follows that $\dim \operatorname{im} A = m - 1$.

Note that this mirrors what is going on with our previous lemma: one given coordinate of our α units is positive, and the rest are negative.

Example 2.40. With $m = 1$, A has to be the zero matrix by (i). This is fine.

Proof. Label A by

$$A = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n | \\ 1 & & | \end{bmatrix}$$

Note that $\langle 1, \dots, 1 \rangle \in \ker A$, so A is singular, so $\dim \operatorname{im} A \le m - 1$.

[2] $A \ge 1$ from the class number stuff; namely, A served as an upper bound for the ideal class number, and there is at least one ideal class.

Now suppose for the sake of contradiction $\dim \operatorname{im} A \le m-2$ so that there is an vector $\langle a_1, \dots, a_m \rangle \in \ker A \setminus \mathbb{R}\langle 1, \dots, 1\rangle$. Namely,

$$\sum_{k=1}^{m} a_k v_k = 0,$$

where not all the $a_\bullet$ are zero. Without loss of generality, take a_1 the smallest; otherwise, if $a_k > a_1$, then we can swap the kth row and column with the first row and column.

From this it follows that

$$0 = \sum_{k=1}^{m} a_k v_k - a_1 \sum_{k=1}^{m} v_k = \sum_{k=1}^{m} (a_k - a_1) v_k, \tag{$*$}$$

which is not a linear combination of the $v_\bullet$ where all the terms are nonnegative, and the v_1 term has vanished. However, not all the a_k are equal, so one of the $a_k - a_1$ will not vanish. It follows that $(*)$ has a negative term in it which doesn't vanish, and the entire sum will thus be negative. ■

We now get the following theorem.

Theorem 2.41. We have that Γ is a complete lattice in H.

Proof. Let $m = r+s$, and let A be the real $m \times m$ matrix, whose columns are populated by the negative embeddings of the units from Lemma 2.37 in sequence. (We are taking the negative because λ in our diagram has a $-\log$ involved.) Then A satisfies the conditions of Lemma 2.39, and we are done because the rank of H is also $r+s-1$. (The column sums are 0 because out units have norm ± 1, which go to 0 after logging.) ■

2.5.2 Dirichlet's Unit Theorem

We are now ready for the finish of all our hard work.

Theorem 2.42. We have that $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$ as an abstract group.

Remark 2.43. In fact, we have shown that $\mu(K)$ is finite, from which it follows $\mu(K)$ is cyclic because it is a finite multiplicative group of a field.

Proof. We use the fact that $\Gamma = \lambda(\mathcal{O}_K^\times)$ is a complete lattice, which implies from $H \cong \mathbb{R}^{r+s-1}$ that $\Gamma \cong \mathbb{Z}^{r+s-1}$. Then, using λ gives us a short exact sequence of abelian groups

$$1 \to \mu(K) \to \mathcal{O}_K^\times \to \mathbb{Z}^{r+s-1} \to 0.$$

This short exact sequence splits by tracking the basis of $\mathbb{Z}^{r+s-1}$ back into $\mathcal{O}_K^\times$, which is good enough because we live in the category of $\mathbb{Z}$-modules. ■

This gives the following definitions.

Definition 2.44 (Fundamental units)**.** A *system of fundamental units* of K is a sequence of units we name $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{r+s-1}$ whose image in Γ are a basis for Γ.

Definition 2.45 (Regulator)**.** The regulator R_K of K is the absolute value of the determinant of any $(r+s-1) \times (r+s-1)$ minor of the $(r+s-1) \times (r+s)$ matrix

$$\begin{bmatrix} -\log|\rho_1\varepsilon_1| & \cdots & -\log|\rho_r\varepsilon_1| & -\log|\sigma_1\varepsilon_1|^2 & \cdots & -\log|\sigma_s\varepsilon_1|^2 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -\log|\rho_1\varepsilon_{r+s}| & \cdots & -\log|\rho_r\varepsilon_{r+s}| & -\log|\sigma_1\varepsilon_{r+s}|^2 & \cdots & -\log|\sigma_s\varepsilon_{r+s}|^2 \end{bmatrix}$$

Note that the regulator is well-defined because (1) multiplying by a root of unity does change the magnitude of the units, and (2) the basis doesn't matter by doing some row operations, and (3) the minor doesn't matter because the sum of the column vectors is 0.[3]

We end with one more result.

Proposition 2.46. The covolume of Γ in H is $\sqrt{r+s}R$.

Proof. Project Γ onto any particular coordinate plane, which give covolume R. Then we notice that doing the same for H causes the volume to shrink by $\sqrt{r+s}$ because, for example,

$$(r+s-1,1,\dots,1) \in H$$

will shrink to a length of $\sqrt{(r+s-1)^2+(r+s-1)}$ while being projected to a length of $\sqrt{r+s-1}$ upon killing the first coordinate. Namely, our shrinking factor from this vector is $\sqrt{r+s}$, which dictates the shrinking of the entire hyperplane for some reason. ■

[3] For (3), the explicit way to see this is to add a column of 1s on the left matrix and do expansion by minors after adding all rows to the top row, effectively killing; this column is orthogonal to the rest of the vectors, so the next proposition follows by projecting.

Theme 3
Ramification Theory

3.1 September 27

Today we localize.

3.1.1 Setting Up Localization

Throughout today's class, we take A a (commutative) ring (with identity) where S is a multiplicative subset. What does multiplicative mean?

Definition 3.1 (Multiplicative)**.** A subset $S \subseteq A$ is *multiplicative* if and only if $1 \in S$ and $x, y \in S$ implies $xy \in S$. In other words, S is a submonoid of $(A, \times)$.

We have the following.

Proposition 3.2. Let $\sim$ be a relation on $A \times S$ defined by

$$(a_1, s_1) \sim (a_2, s_2) \iff \exists s' : s'(s_1 a_2 - s_2 a_2) = 0.$$

Then we have the following.

(a) $\sim$ is an equivalence relation on $A \times S$.

(b) $\sim$ is the smallest equivalence relation on $A \times S$ such that for which all $(a, s) \in A \times S$ have $(a, s) \sim (s_0 a, s_0 s)$ for any $s_0 \in S$.

Proof. The proof of (a) is annoying and will be omitted.

We now do (b). Suppose $\approx$ is the smallest equivalence relation satisfying the condition of (b). We can check by hand that

$$(a, s) \approx (s'a, s's)$$

so that $\approx \subseteq \sim$. Conversely, if $(a_1, s_1) \sim (a_2, s_2)$, then there exists some s' such that $s's_1a_2 = s's_2a_1$. It follows

$$(a_1, s_1) \approx (s's_2a_1, s's_2s_1) = (s's_1a_2, s's_1s_2) \approx (a_2, s_2),$$

so $\sim \subseteq \approx$. ∎

Remark 3.3. The extra s' in the equivalence relation exists because general rings might have zero-divisors, and this is needed to make our relation transitive.

So we have the following definition.

Definition 3.4 (Localized ring)**.** Define $S^{-1}A$ to be $(A \times S)/\sim$.

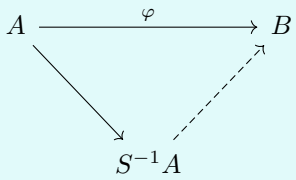
Then we have the following.

Proposition 3.5. The usual addition and multiplication rules for fractions on $S^{-1}A$ make $S^{-1}A$ into a commutative ring such that $A \to S^{-1}A$ by $a \mapsto a/1$ is a ring homomorphism.

Proof. We omit this because it is boring. The main point is that (b) from the above proposition gives us a more direct way to check the addition and multiplication rules are well-defined. ■

We also have the following universal property.

Proposition 3.6. Any homomorphism $\varphi : A \to B$ for which $\varphi(S) \subseteq B$ factors uniquely through $A \to S^{-1}A$. Namely, the induced arrow in the following diagram exists and is unique.



Proof. Check by hand. ■

There is also a notion of a localized module.

Definition 3.7. If M is an A-module, then essentially the same relation on $M \times S$ lets us define $S^{-1}M$.

And we have the following.

Proposition 3.8. The module $S^{-1}M$ is an $S^{-1}A$-module, and $S^{-1}M \cong M \otimes_A S^{-1}A$. In fact, $M \mapsto S^{-1}M$ is an exact functor: if

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

is an exact sequence of A-modules, then

$$0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$$

is an exact sequence of $S^{-1}A$-modules.

Proof. We leave this as an exercise because, as usual, it is not very interesting. ■

Let's do some examples.

Example 3.9. If A is entire, then $S = A \setminus \{0\}$ is multiplicative, so we have $A \to S^{-1}A$ is really just A mapping into its fraction field.

Example 3.10. We have that $S^{-1}A = 0$ if and only if $0 \in S$. In one direction, if $1/1 = 0/1$, then we see there is $s' \in S$ such that $s'(1-0) = 0$, so $s' = 0 \in S$. In the other direction, if $0 \in S$, then $a/s = 0/1$ because $0 \cdot (1a - 0s) = 0$.

Example 3.11. If A is entire with fraction field K, then $0 \notin S$ has $A \hookrightarrow S^{-1}A$ an injective map, and in fact $S^{-1}A$ is a subring of K.

3.1.2 Some Theory

We have the following proposition.

Proposition 3.12. Fix $\varphi : A \to S^{-1}A$ the canonical map. Then we have the following.

(a) $\ker \varphi = \{a \in A : \operatorname{Ann}(a) \cap S \neq \varnothing\}$.

(b) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of A. Then $S^{-1}\mathfrak{a}$ and $S^{-1}\mathfrak{b}$ (defined as $S^{-1}A$-modules because $\mathfrak{a}$ and $\mathfrak{b}$ are A-modules) are $S^{-1}A$-ideals. Further,

$$S^{-1}(\mathfrak{ab}) = S^{-1}\mathfrak{a}S^{-1}\mathfrak{b}.$$

(c) If $\mathfrak{a}$ is an A-ideal, then $\varphi^{-1}\left(S^{-1}\mathfrak{a}\right) = \{a \in A : aS \cap \mathfrak{a} \neq \varnothing\}$. Expanding, this is equivalent to $a/s \in S^{-1}\mathfrak{a}$ if and only if $s'a \in \mathfrak{a}$ for some $s' \in S$.

(d) If $\mathfrak{a}'$ is an $S^{-1}A$-ideal, then $S^{-1}\left(\varphi^{-1}\mathfrak{a}'\right) = \mathfrak{a}'$.

(e) if $\mathfrak{a}$ is an A-ideal, then $S^{-1}A/S^{-1}\mathfrak{a} \cong (A/\mathfrak{a}) \otimes_A S^{-1}A \cong \overline{S}^{-1}\mathfrak{a}$, where $\overline{S}$ is the image of S under $A \twoheadrightarrow A/\mathfrak{a}$.

Proof. This is omitted because it's too long. ∎

This gives the following corollaries.

Corollary 3.13. Given $\mathfrak{a}$ an A-ideal, the canonical map $\mathfrak{a} \to S^{-1}\mathfrak{a}$ is surjective.

Proof. This essentially follows from (d) above. ∎

Corollary 3.14. Given $\mathfrak{a}'$ an $S^{-1}A$-ideal, the canonical map $\mathfrak{a}' \to \varphi^{-1}\mathfrak{a}'$ is injective and preserves inclusions and therefore strict inclusions. It follows $\mathfrak{a}' \subseteq \mathfrak{b}'$ if and only if $\varphi^{-1}\mathfrak{a} \subseteq \mathfrak{b}$.

Proof. Omitted because what even is mathematics. ∎

So we have the following.

Proposition 3.15. If A is Noetherian, then $S^{-1}A$ is Noetherian.

Proof. This is because the pull-back φ^{-1} preserves strict inclusions, so $S^{-1}A$ may have no non-stabilizing infinite ascending chains. ∎

And let's talk briefly about being integrally closed.

Proposition 3.16. Fix $A \subseteq B \subseteq C$ entire rings with $0 \notin S$. Then we have the following.

1. If $\alpha \in B$ is integral over A, then it is integral over $S^{-1}A$.
2. If $\alpha \in B$ is integral over $S^{-1}A$, then there is some $s \in S$ such that $s\alpha$ is integral over A.
3. If B is the integral closure of A in C, then $S^{-1}B$ is the integral closure of $S^{-1}A$ in $S^{-1}C$.
4. If A is integrally closed, then $S^{-1}A$ is also integrally closed.

Proof. As usual, the proof is omitted. ■

Remark 3.17. This more or less generalizes the story of what happened with $\mathbb{Z}$ and $\mathbb{Q}$ way back

3.1.3 Spec Smack

We have the following definition.

Definition 3.18 (Spectrum)**.** We define the *spectrum* of A, notated $\operatorname{Spec} A$, to be the set of primes in A, including 0.

Example 3.19. In $\mathbb{Z}$, we have $\operatorname{Spec} A = \{(p) : p \text{ prime}\}$.

One of the nice things about the spectrum is that a ring homomorphism $\varphi : A \to B$ will take a prime $\mathfrak{p} \in \operatorname{Spec} B$ to another prime $\varphi^{-1}\mathfrak{p} \in \operatorname{Spec} A$. This means we have an induced map

$$\varphi^* : \operatorname{Spec} B \to \operatorname{Spec} A.$$

In our case, we have the following.

Proposition 3.20. The canonical map $\varphi : A \to S^{-1}A$ has the induced φ^* injective. We will often sloppily identify $\operatorname{Spec} S^{-1}A$ with its image under φ^* in $\operatorname{Spec} A$.

Remark 3.21. If $0 \in S$, then this actually works because $\operatorname{Spec} S^{-1}A = \operatorname{Spec} 0 = \varnothing$.

Proof. As usual, omitted. ■

We continue.

Proposition 3.22. Fix $\mathfrak{p} \in \operatorname{Spec} A$. Then we have the following.

(a) We have that $S^{-1}\mathfrak{p} = (1)$ if and only if $\mathfrak{p} \cap S \neq \varnothing$.

(b) If $\mathfrak{p} \cap S = \varnothing$, then $a/s \in S^{-1}\mathfrak{p}$ if and only if $a \in \mathfrak{p}$.

(c) If $\mathfrak{p} \cap S = \varnothing$, then $S^{-1}\mathfrak{p}$ is prime. It follows $\operatorname{Spec} S^{-1}A = \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \cap S = \varnothing\}$.

Proof. We outline in sequence.

(a) This follows because $1/1 \in S^{-1}\mathfrak{p}$ if and only if $s/s \in S^{-1}\mathfrak{p}$ so that $s \in \mathfrak{p}$ and $s \in S$.

(b) This follows because $a/s \in S^{-1}\mathfrak{p}$ if and only if $a \in \varphi^{-1}(S^{-1}\mathfrak{p})$, which is equivalent to there existing $s' \in S$ such that $s'a \in \mathfrak{p}$, which is equivalent to $a \in \mathfrak{p}$ because $S \cap \mathfrak{p} = \varnothing$. ■

So we have the following.

Proposition 3.23. Fix A a Dedekind ring and $0 \notin S$. Then $S^{-1}A$ is also Dedekind.

Proof. We can see that $S^{-1}A$ is entire by hand; we already checked that it is Noetherian and integrally closed given that A is.

Lastly, $S^{-1}A$ has dimension 1 because of the classification of its primes. In particular, if $S^{-1}A$ has non-maximal primes, then we could pull these back to non-maximal primes of A by φ^{-1} because φ^{-1} preserves strict inclusion. ■

3.2 September 29

We continue with out story on localization.

3.2.1 More Localization

From last time, we recall the following.

Proposition 3.24. Fix A a Dedekind domain and $S \subseteq A$ a multiplicative subset not containing 0. Then $S^{-1}A$ is a Dedekind domain.

So we have the following.

Corollary 3.25. Fix S and A as above with $\mathfrak{a}$ a nonzero A-ideal. Then if

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_{\mathfrak{p}}},$$

we have

$$S^{-1}\mathfrak{a} = \prod_{\mathfrak{p} \cap S = \varnothing} \left(S^{-1}\mathfrak{p}\right)^{\alpha_{\mathfrak{p}}}.$$

Proof. Because localization commutes with products,

$$S^{-1}\mathfrak{a} = S^{-1}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_{\mathfrak{p}}}\right) = \prod_{\mathfrak{p}} \left(S^{-1}\mathfrak{p}\right)^{\alpha_{\mathfrak{p}}}.$$

If $S \cap \mathfrak{p} \neq \varnothing$, then $\mathfrak{p}$ contains a unit of $S^{-1}A$, so $\mathfrak{p}$ dies. Otherwise, $S \cap \mathfrak{p} = \varnothing$ retains primality, so we get the factorization

$$S^{-1}\mathfrak{a} = \prod_{\mathfrak{p} \cap S = \varnothing} \left(S^{-1}\mathfrak{p}\right)^{\alpha_{\mathfrak{p}}}.$$

We can also check that the factors are distinct by checking how localization behaves with the spectrum. ■

3.2.2 Local Rings

We have the following definition.

Definition 3.26 (Local)**.** A ring R is *local* if it has a unique maximal ideal. We might say $(A, \mathfrak{m})$ is a local ring, where $\mathfrak{m}$ is the unique maximal ideal of A. We might also include the data of the residue field $k := A/\mathfrak{m}$.

We remark that the units of a local ring $(A, \mathfrak{m})$ are the elements of $A \setminus \mathfrak{m}$. Certainly no element of a proper ideal can be a unit (multiplying by an element of A would stay in the proper ideal); conversely, if $u \in A \setminus \mathfrak{m}$, then (u) cannot be placed inside of a maximal ideal, so (u) must not be proper, so $(u) = R$, so u is a unit.

Note that some care is needed for our definitions: localizing does not make one a local ring.

Non-Example 3.27. We see $A = \mathbb{Z}$ and $S = \{1\}$ or $S = \langle 2 \rangle$ do not give local rings.

Regardless, here are some examples.

Example 3.28. Take $A = \mathbb{Z}$ and $S = 2\mathbb{Z} + 1$. Then $S^{-1}A$ consists of all fractions with odd denominator; here (2) is the only nonzero prime ideal.

Example 3.29. More generally, fix A a ring wth $\mathfrak{p}$ prime. Then $S = A \setminus \mathfrak{p}$ is multiplicative, and we can define

$$A_{\mathfrak{p}} := S^{-1}A.$$

Here $\mathfrak{p}$ is the only prime of $S^{-1}A$.

We note that, in the notation of uor second example, the first example is $\mathbb{Z}_{(2)}$.

Anyways, we have the following.

Proposition 3.30. Fix A a Dedekind domain with only finitely many primes; then A is principal.

Proof. From homework, we know that every ideal class has an ideal avoiding some finite set of primes. But then we can have all ideal classes avoid all of the primes at once, of which the only available ideal representative is (1). So all ideal classes are (1), so all ideals are principal. ■

In particular, local rings found from localization are principal. For example, $A_{\mathfrak{p}}$ from above is principal.

3.2.3 Discrete Valuation Rings

We have the following definition.

Definition 3.31 (Discrete valuation ring)**.** A *discrete valuation ring* is a principal, local, entire ring, which is not a field.

This is the most algebraic way to define a discrete valuation ring, but it is not the most concrete.

Proposition 3.32. The following are equivalent.

(a) A is a principal, local, entire ring which is not a field.

(b) A is a Noetherian, local, entire ring whose maximal ideal is nonzero and principal.

(c) A is a local, Dedekind ring which is not a field.

Proof. All of these are local, entire, Noetherian, and not a field for free. So the main work is showing that being principal is the same as maximum ideal nonzero and principal is the same as integrally closed plus dimension 1.

The hardest part is getting integrally closed from the other assertions. As usual, we will not do this here. ■

We should probably talk about what it means to be a valuation.

Proposition 3.33. Fix $(A, \mathfrak{m})$ a discrete valuation ring with K its fraction field, and find some π with $\mathfrak{m} = (\pi)$. Then there is a unique isomorphism

$$K^\times / A^\times \to \mathbb{Z}$$

by $\pi \mapsto 1$, and in fact the choice of π is irrelevant. The isomorphism is given by $\alpha \in K^\times \longmapsto n$ such that $(\alpha) = \mathfrak{m}^n$.

Proof. Fix π as above. Note that A being principal implies that A has unique factorization, so let's classify our primes. Well, if ρ is an irreducible, then $\rho \notin A^\times = A\mathfrak{m}$, so $\rho \in \mathfrak{m}$, but (ρ) is prime, so (ρ) is maximal, so $(\rho) = \mathfrak{m} = (\pi)$, so $\rho = u\pi$ for some $u \in A^\times$.

Thus, every nonzero $a \in A$ can be uniquely written as

$$a = u\pi^n$$

for some $u \in A^\times$ and $n \in \mathbb{N}$. This extends uniquely to a homomorphism $K^\times \twoheadrightarrow \mathbb{Z}$ with kernel $A^\times$, so we get our isomorphism $K^\times / A^\times \to \mathbb{Z}$. ■

This gives the following more standard definition of a discrete valuation ring.

Definition 3.34 (Valuation)**.** Fix A an entire ring with fraction field K. Then a *valuation* on K $\nu : K^\times \to G$ is a group homomorphism to a totally ordered group G. It is a valuation on A if it satisfies the following.

- $\nu(a) \geq 0$ for $a \in A \setminus \{0\}$.
- For convenience, we will append $\nu(0) = \infty > g$ for any $g \in G$.
- $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$. (Note $a + b = 0$ is legal by the above convention.)

A valuation $\nu : K^\times \to G$ is *discrete* if and only if it has image isomorphic to $\mathbb{Z}$.

The definition of a totally ordered group is exactly what we expect: $x \leq y$ is equivalent to $xz \leq yz$ if and only if $zx \leq zy$. Note that we permit nonabelian G above, but in practice we will only use abelian groups.

This lets us define the following.

Definition 3.35 (Valuation ring)**.** The *valuation ring* of a valuation $\nu : K^\times \to G$ is the set

$$A := \{\alpha \in K : \nu(\alpha) \geq 0\}.$$

This is a ring because it is closed under addition and multiplication by the requirements on ν. In fact, A is local ring with maximal ideal

$$\mathfrak{m} := \{\alpha \in K : \nu(\alpha) > 0\}.$$

In particular, we get the following.

Proposition 3.36. A ring A is a discrete valuation ring if and only if it is a valuation ring of a discrete valuation.

Proof. The forwards direction is Proposition 3.33. In the backwards direction, we already know that A is local, entire, and not a field. Then it is principal because its maximal ideal is principal (which we don't show here) and then do something funny. ■

We'll close with the following definition.

Definition 3.37. Fix A a Dedekind domain and K its field of fractions. Fixing $\mathfrak{p}$ a nonzero prime ideal in A, we define $\nu_{\mathfrak{p}} : K^\times \to \mathbb{Z}$ to send $x \in K^\times$ to $\alpha_{\mathfrak{p}}$ in the factorization

$$(x) = \prod_{\mathfrak{q}} \mathfrak{q}^{\alpha_{\mathfrak{q}}}.$$

And now we bring things full-circle.

Proposition 3.38. It happens that $\nu_{\mathfrak{p}}$ is always a discrete valuation, with valuation ring $A_{\mathfrak{p}}$. It follows $A_{\mathfrak{p}}$ is a discrete valuation ring and that

$$A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}.$$

Proof. Omitted because of course. ∎

3.3 October 1

Today, A will be a Dedekind domain except when we explicitly say otherwise, and K is its fraction field.

3.3.1 Localizing Away from Primes

The book has the following definition.

Definition 3.39 (Localization away from primes)**.** Fix $X \subseteq \operatorname{Spec} A$ a subset with finite complement. Then we define

$$\mathcal{O}(X) := \left\{ \frac{f}{g} : f, g \in A \text{ and } \nu_{\mathfrak{p}}(g) = 0 \text{ for each } \mathfrak{p} \in X \setminus \mathfrak{p} \right\}.$$

Note that we are allowing $(0) \in X$, but we will actively pretend it does not exist, making "for all $\mathfrak{p} \in X$" mean "for all $\mathfrak{p} \in X \setminus \{(0)\}$."

We make a few short remarks.

Remark 3.40. We note that $\mathcal{O}(X) \subseteq K$ is a subring of K, and $A \subseteq \mathcal{O}(X)$ as well. In fact, we note that $\mathcal{O}(X)$ is a localization of

$$S := \{g : \nu_{\mathfrak{p}}(g) = 0 \text{ for all } \mathfrak{p} \in X\}$$

so that $\mathcal{O}(X) = S^{-1}A$. Then, because A is Dedekind, we see that $\mathcal{O}(X)$ is Dedekind.

Warning 3.41. It is not in general true that $\operatorname{Spec} \mathcal{O}(X) = X \cup \{(0)\}$.

To fix the problem in the warning, we take the following definition.

Definition 3.42 (Localizing, again)**.** Fix $X \subseteq \operatorname{Spec} A$ a subset with finite complement. Then we define

$$\mathcal{O}(X)_{\text{Vojta}} := \bigcap_{\mathfrak{p} \in X} A_{\mathfrak{p}} \subseteq K,$$

which is $\{x \in K^\times : \nu_{\mathfrak{p}}(x) \geq 0 \text{ for each } \mathfrak{p} \in X\} \cup \{0\}$.

We now have the following proposition to reconcile the two definitions.

Proposition 3.43. Suppose that all (nonzero) primes $\mathfrak{p} \in \operatorname{Spec} A \setminus X$ are torsion in the class group. Then $\mathcal{O}(X)_{\text{Vojta}} = \mathcal{O}(X)$.

Proof. Professor Vojta hasn't worked this out yet, so it will be on the homework. ■

Remark 3.44. It is also true that $\mathcal{O}(X)_{\text{Vojta}} = \mathcal{O}(X)$ if A is of finite type over a field using some results from algebraic geometry. Note that the Picard group need not be finite: elliptic curves over (say) the rationals may have infinite elements.

Here is one reason we are bringing up localizing: it behaves nicely with our short exact sequence.

Proposition 3.45. We have the following canonical exact sequence.

$$1 \to A^\times \to \mathcal{O}(X)^\times \to \bigoplus_{\mathfrak{p} \notin X} (K^\times / A_{\mathfrak{p}}^\times) \to \operatorname{Cl}(A) \to \operatorname{Cl}(\mathcal{O}(X)) \to 0.$$

Proof. We check exactness one at a time.

- Exactness at $A^\times$ holds because $A \subseteq \mathcal{O}(X)$.
- Exactness at $\mathcal{O}(X)^\times$: fix $\alpha \in \mathcal{O}(X)^\times$ with

$$\alpha \in \ker \left(\mathcal{O}(X)^\times \to \bigoplus_{\mathfrak{p} \notin X} K^\times / A_{\mathfrak{p}}^\times \right).$$

wut

This is equivalent to $\alpha, \alpha^{-1} \in A_{\mathfrak{p}}$ for each $\mathfrak{p} \notin X$, which is equivalent to $\alpha, \alpha^{-1} \in A_{\mathfrak{p}}$ for each $\mathfrak{p} \in \operatorname{Spec} A$ because the primes in X survive anyways, and lastly this is equivalent to $\alpha, \alpha^{-1} \in A$ by checking the $\nu_{\mathfrak{p}}$ coordinates.

- Exactness as $\bigoplus_{\mathfrak{p} \notin X} K^\times / A_{\mathfrak{p}}^\times$: observe that $\nu_{\mathfrak{p}} : K^\times / A_{\mathfrak{p}}^\times \to \mathbb{Z}$ is an isomorphism for each of the $\mathfrak{p} \notin X$ because $A_{\mathfrak{p}}$ definitionally have $\nu_{\mathfrak{p}}$ vanish. Now suppose

$$n := (n_{\mathfrak{p}})_{\mathfrak{p} \notin X} \in \ker \left(\bigoplus_{\mathfrak{p} \notin X} K^\times / A_{\mathfrak{p}}^\times \to \operatorname{Cl}(A) \right).$$

Because we are taking n to the product of its primes' ideal class, n is in the kernel if and only if we can find some $\alpha \in K^\times$ such that

$$\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{n_{\mathfrak{p}}} = \alpha A.$$

Professor Vojta got confused, so we will come back to this proof later.

- Exactness at $\operatorname{Cl}(A)$: Suppose $c \in \operatorname{Cl}(A)$ lives in $\ker\big(\operatorname{Cl}(A) \to \operatorname{Cl}(\mathcal{O}(X))\big)$. This is equivalent to c being represented by a fractional ideal

$$\prod_{\mathfrak{p} \in \operatorname{Spec} A \setminus \operatorname{Spec} \mathcal{O}(X)} \mathfrak{p}^{n_{\mathfrak{p}}}$$

wut

by checking our primes individually. So this is equivalent to c living in the image of $\bigoplus_{\mathfrak{p} \notin X} K^\times / A_{\mathfrak{p}}^\times \to \operatorname{Cl}(A)$.

- Exactness at $\operatorname{Cl}(\mathcal{O}(X))$: essentially, all primes $\mathfrak{q}$ of $\mathcal{O}(X)$ can be pulled back to $\mathfrak{p}\mathcal{O}(X)$ for some prime $\mathfrak{p} \in A$. It follows that the map $J_A \to J_{\mathcal{O}(X)}$ of ideals is surjective. ■

3.3.2 S-integers

Let's see localization do something. Fix K a number field, $A = \mathcal{O}_K$ its ring of integers, and let S be a finite set of nonzero primes. We have the following definition.

Definition 3.46 (S-integers)**.** Fix K a number field. Then we define the *ring of S-integers of K* to be $\mathcal{O}_{K,S} := \mathcal{O}(\operatorname{Spec} \mathcal{O}_K \setminus S)$. THe group of S-units is $\mathcal{O}_{K,S}^\times$.

Let's show a few things.

Proposition 3.47. Fix everything as above. The class group $\operatorname{Cl}(\mathcal{O}_{K,S})$ is finite, and $\mathcal{O}_{K,S}^\times$ has rank $\#S + r + s - 1$ and torsion $\mu(K)$.

Proof. This follows by staring at the exact sequence from earlier. For example, $\operatorname{Cl}(\mathcal{O}_{K,S})$ is finite because

$$\operatorname{Cl} A \to \operatorname{Cl}(\mathcal{O}_{K,S})$$

is a surjective map from a finite set. Further, we can compute the rank of $\mathcal{O}_{K,S}^\times$ as

$$\operatorname{rank} \mathcal{O}_K^\times + \operatorname{rank} \bigoplus_{\mathfrak{p} \in S} K^\times / (\mathcal{O}_K)_{\mathfrak{p}}^\times$$

because all rank from $\mathcal{O}_{K,S}^\times \to \bigoplus_{\mathfrak{p} \in X} K^\times / A_{\mathfrak{p}}^\times$ must vanish when going into $\operatorname{CL} A$ because $\operatorname{Cl} A$ is finite and hence fully torsion. So we can compute the rank of $\mathcal{O}_{K,S}^\times$ is $r + s - 1 + \#S$. ∎

So we have the following general idea.

Idea 3.48. In general, $\mathcal{O}_{K,S}$ has many similar properties as $\mathcal{O}_K$, but with fewer primes to worry about.

3.3.3 Extensions of Dedekind Domains

We now take the $AKLB$ setup, where A is a Dedekind ring, K is its fraction field, L/K is a finite extension, and B is the integral closure of A in L.

$$\begin{array}{ccc} B & \subseteq & L \\ \vdots & & | \\ A & \subseteq & K \end{array}$$

We will also assume that B is finite over A, which is true in the cases we care about (i.e., $A = \mathcal{O}_K$ for a number field K or if A is of finite type over a field or if A is a localization of one of those). We note that B is Dedekind by some theorem by Krull–Akizuki.

We also take the following definition.

Definition 3.49 (Ramification, inertial index)**.** Work in the $AKLB$ setup, and let $\mathfrak{p} \in \operatorname{Spec} A \setminus \{(0)\}$. Then $\mathfrak{p}B$ is a nonzero ideal of B with prime factorization

$$\mathfrak{p}B = \prod_{k=1}^{r} \mathfrak{q}_k^{e_k}.$$

We say that $\mathfrak{q}_k$ *lies over* $\mathfrak{p}$. Then we have the following definitions.

- The *ramification degree* $e(\mathfrak{q}_k/\mathfrak{p})$ is e_k in the above factorization.
- The *inertial index* $f(\mathfrak{q}_k/\mathfrak{p})$ is the dimension of the field extension $[B/\mathfrak{q}_k : A/\mathfrak{p}]$.

We note that the claimed field extension exists because $\mathfrak{q}_k \cap A \subseteq \mathfrak{p}$ and some isomorphism theorem.

There are some claims about to be proven (namely, that the factorization is nonempty) as well as that $\mathfrak{q}_k \cap A = \mathfrak{p}$.

3.4 October 4

Today we continue with ramification theory.

3.4.1 Review

Last time we had some trouble showing exactness of

$$1 \to A^\times \to \mathcal{O}(X) \to \bigoplus_{\mathfrak{p} \notin X} \left(K^\times / A_{\mathfrak{p}}^\times\right) \to \mathrm{Cl}(A) \to \mathrm{Cl}(\mathcal{O}(X)) \to 0$$

at $\bigoplus_{\mathfrak{p} \notin X} \left(K^\times / A_{\mathfrak{p}}^\times\right)$ and at $\mathrm{Cl}(\mathcal{O}(X))$.

- For exactness at $\bigoplus_{\mathfrak{p} \notin X} \left(K^\times / A_{\mathfrak{p}}^\times\right)$, there is an example making this not exact[1]. However, it is exact in the situation given in the last homework problem for this week.
- Similarly, exactness at $\mathrm{Cl}(\mathcal{O}(X))$ is on the homework.

We remark that the above sequence is also exact if A is of finite type over a field, using some algebraic geometry.

3.4.2 Fundamental Identity

For the rest of today, we take the $AKLB$ setup, where A is a Dedekind domain, K its fraction field, L/K a finite extension (not necessarily separable), and B is the integral closure of A in L.

We continue the definition of ramification degree and inertial index from last time.

Definition 3.50. Fix $\mathfrak{p}$ a nonzero prime of A. Then we may factor

$$\mathfrak{p}B = \prod_{k=1}^{r} \mathfrak{q}_k^{e_k},$$

where $\mathfrak{q}_\bullet$ are primes in B, and $e_k > 0$ for each k.

- The *ramification degree* $e(\mathfrak{q}_k/\mathfrak{p}) = e_k$ as above.
- We say $\mathfrak{q}_\bullet$ *lies over* $\mathfrak{p}$.
- Let $\kappa = A/\mathfrak{p}$ and $\lambda_k = B/\mathfrak{q}_k$, which are fields because primes are maximal. Then $A \hookrightarrow B$ will induce a map $\kappa \hookrightarrow \lambda_k$, which is injective because its a homomorphism of fields, and it is well-defined because the kernel is $A \cap \mathfrak{q}_\bullet = \mathfrak{p}$ as below.

  So κ embeds into λ_k, so we may define

  $$f(\mathfrak{q}_k/\mathfrak{p}) := [\lambda_k : \kappa].$$

We remark that $\mathfrak{q}$ lies above $\mathfrak{p}$ if and only if $\mathfrak{q} \cap A = \mathfrak{p}$. Certainly each $\mathfrak{q}_\bullet$ has $\mathfrak{q}_\bullet \cap A = \mathfrak{p}$; but further, $\mathfrak{q} \cap A = \mathfrak{p}$ implies $\mathfrak{q} \supseteq \mathfrak{p}B$ implies $\mathfrak{q} \mid \mathfrak{p}B$.

With these, we have the following.

[1] There is an example for which $X \neq \operatorname{Spec} A$ while $\mathcal{O}(X) = A$.

Proposition 3.51 (Fundamental Identity)**.** Fix everything as in Definition 3.50. Then

$$\sum_{k=1}^{r} e_k f_k = [L : K].$$

For example, this implies $\mathfrak{p}B \neq B$ because some primes must exist.

Proof. This proceeds in steps.

1. We start by localizing. Fix $S := A \setminus \mathfrak{p}$ with $A_{\mathfrak{p}} := S^{-1}A$ and set $B_{\mathfrak{p}} := S^{-1}B$ as well. Because localization commutes with integral closure, we see that $B_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$ in L. Further, $A_{\mathfrak{p}}$ is Dedekind (it's a Dedekind domain, localized) with fraction field K, and $B_{\mathfrak{p}}$ is finite over $A_{\mathfrak{p}}$ because it was before as well.

   So we have the usual picture, as follows.

$$\begin{array}{ccc} B_{\mathfrak{p}} & \subseteq & K \\ \vdots & & | \\ A_{\mathfrak{p}} & \subseteq & L \end{array}$$

   Now, from our localization theory, we see that

$$\mathfrak{p}_{\mathfrak{p}} B_{\mathfrak{p}} = (S^{-1}\mathfrak{p}) \underbrace{(S^{-1}B)}_{\text{trivial}} = \prod_k (S^{-1}\mathfrak{q}_k)^{e_k}.$$

   Further, we see that $S^{-1}\mathfrak{q}_k$ is a prime ideal of $B_{\mathfrak{p}}$ for each k (because $\mathfrak{q}_\bullet \cap A = \mathfrak{p}$, we have $\mathfrak{q}_\bullet \cap S = \varnothing$), and the e_k match from before because we just factored $\mathfrak{p}$.

   And because localization is an exact sequence, we see that

$$0 \to \mathfrak{q}_k \to B \to \lambda_k \to 0$$

   localizes down to

$$0 \to S^{-1}\mathfrak{q}_k \to B_{\mathfrak{p}} \to S^{-1}\lambda_k \to 0$$

   is also exact. (Here, $S^{-1}\lambda_k$ has to mod out by $\mathfrak{q}_k$ first, but $0 \notin S$ makes this safe because $\mathfrak{q}_k \cap S = \varnothing$, so nothing gets killed on modding.) Similarly,

$$0 \to \mathfrak{p}_{\mathfrak{p}} \to A_{\mathfrak{p}} \to S^{-1}\kappa \to 0$$

   is exact. The point is that our residue fields are also unchanged, so our inertial indices are also unchanged.

2. It remains to work locally. Fix $(A, \mathfrak{p})$ a local field with residue field κ, and fix $n := [L : K]$. By the Chinese remainder theorem, we see that

$$B/\mathfrak{p}B \cong \prod_{k=1}^{r} (B/\mathfrak{q}_k^{e_k}).$$

   We start with the right-hand side. We saw sometime ago that $\mathfrak{q}_k^{e+1}/\mathfrak{q}_k^{e} \cong B/\mathfrak{q}_k$ (say, as groups), so we can compute indices

$$\dim_\kappa (B/\mathfrak{q}_k^{e_k}) = e_k \dim_\kappa B/\mathfrak{q}_k = e_k \dim_\kappa B/\lambda_k = e_k f_k.$$

   Now we study the left-hand side of our Chinese remainder theorem. We recall that A being Dedekind with finitely many primes (!) makes it a principal ideal domain, which gives B an integral basis over A, implying $\dim_\kappa B/\mathfrak{p}B = [L : K]$. Indeed,

$$B/\mathfrak{p}B \cong B \otimes_A (A/\mathfrak{p}) \cong A^n \otimes_A (A/\mathfrak{p}) \cong \kappa^{[L:K]}.$$

   This finishes. ∎

wut

3.4.3 Dedekind–Kummer Theorem

We take the following definition.

Definition 3.52 (Conductor)**.** Fix the $AKLB$ in the usual picture, and suppose θ is a primitive element of L/K such that $\theta \in B$ (by clearing denominators). Then $A[\theta]$ is a full submodule of L over A contained in B, and we define the *conductor* of $A[\theta]$ to be

$$\{\alpha \in B : \alpha B \subseteq A[\theta]\}.$$

We note that the conductor is an $A[\theta]$-ideal: given $r_1, r_2 \in A[\theta]$ and $\alpha_1, \alpha_2 \in B$, we have that

$$(r_1\alpha_1 + r_2\alpha_2)B = r_1(\alpha_1 B) + r_2(\alpha_2 B) \subseteq A[\theta].$$

However, the main point to the conductor is that the conductor is B if and only if $B = A[\theta]$. The point here is to try to figure out when we can find a power basis for our integral basis.

We also note that the conductor is nonzero because B is finite over A, meaning that we just have to check that α times each generator of B is safely in $A[\theta]$, and we can construct something.

We have the following proposition.

Proposition 3.53 (Dedekind–Kummer)**.** Work in the $AKLB$ set-up. Fix θ as above with minimal polynomial $p(x) \in A[x]$, and let $\mathfrak{f}$ be the conductor of $A[\theta]$.

Now, let $\mathfrak{p}$ be a nonzero prime of A, and fix $\overline{p} \in (A/\mathfrak{p})[x]$ to be the image of p. Further, assume $\mathfrak{p}$ is coprime to $\mathfrak{f}$ so that $B = A[\theta]$. Now, if we factor into irreducible polynomials by

$$\overline{p} = \prod_{k=1}^{r} \overline{p_k}^{e_k}$$

in $(A/\mathfrak{p})[x]$, where $p_k \in A[x]$ is monic, then

$$\mathfrak{q}_k := \mathfrak{p}B + p_k(\theta)B$$

describes the factorization of $\mathfrak{p}B$ in B, where $e(\mathfrak{q}_k/\mathfrak{p}) = e_k$ and $f(\mathfrak{q}_k/\mathfrak{p}) = \deg \overline{p_k}$.

Proof. We again have two steps: deal with the local case, and then expand out. We start with the local case.

1. We start by taking $(A, \mathfrak{p}, \kappa)$ to be a local ring. We claim

$$B/\mathfrak{p}B \cong \kappa[x]/\left(\overline{p}(x)\right)$$

as A-modules; indeed, because $\mathfrak{p}$ is coprime to $\mathfrak{f}$, we should have $\mathfrak{f} = B$ ($\mathfrak{p}$ is the only prime lying around), so

$$B = A[\theta] \cong A[x]/\big(p(x)\big) \to \kappa[x]/\left(\overline{p}(x)\right)$$

is some surjective chain of homomorphisms. The kernel here is $\mathfrak{p}A[x]/(p(x))$, which shows the claim. ∎

We will continue the proof next class.

3.5 October 6

As usual, we take the $AKLB$ set-up.

3.5.1 More on Dedekind–Kummer

Last time we were proving the following statement, which we have now amended slightly.

Theorem 3.54 (Dedekind–Kummer)**.** Suppose that L/K has a primitive element $\theta \in B$ where $\mathfrak{f}$ is the conductor of $A[\theta]$. Further, take $\mathfrak{p}$ to be a nonzero prime of A such that $\mathfrak{p}B$ is coprime to $\mathfrak{f}$.

Now, let $p \in A[x]$ be the minimal polynomial for θ over K, and factor it in $(A/\mathfrak{p})[x]$ as

$$\overline{p} = \prod_{k=1}^{r} \overline{p_k}^{e_k},$$

where $p_\bullet$ are distinct monic polynomials for which $\overline{p_\bullet}$ is irreducible in $(A/\mathfrak{p})[x]$. Then for each k, we can set $\mathfrak{q}_k := \mathfrak{p}B + p_k(\theta)B$ so that

$$\mathfrak{p}B = \prod_{k=1}^{r} \mathfrak{q}_k^{e_k},$$

where $f(\mathfrak{q}_k/\mathfrak{p}) = \deg \overline{p_k}$.

Before going into this proof, we take the following lemmas.

Lemma 3.55. In the $AKLB$ setup, let $\mathfrak{q}$ be a nonzero prime of B. Then $\mathfrak{q} \cap A \neq 0$.

Proof. Find any $\alpha \in \mathfrak{q} \setminus \{0\}$. Then $\mathrm{N}_K^L(\alpha)/\alpha \in B$ because it is the product of conjugates of α, and α being integral forces the entire product to be integral. So now $\mathrm{N}_K^L(\alpha)$ is a nonzero element of $\mathfrak{q} \cap A$. ∎

Lemma 3.56. Fix $A_1, \dots, A_r$ rings. Then

$$\operatorname{Spec}\left(\prod_{k=1}^{r} A_k\right) = \bigsqcup_{k=1}^{r} \pi_k^* \operatorname{Spec} A_k,$$

where π_ℓ is the projection $\prod_{k=1}^r A_k \twoheadrightarrow A_\ell$. Further, the map $\pi_\ell^* : \operatorname{Spec} A_k \to \operatorname{Spec} \prod_{k=1}^r A_k$.

Proof. By induction, we only have to look at $r = 2$. (There is nothing to show for $r = 0$ or $r = 1$.) Now, fix any $\mathfrak{p} \in \operatorname{Spec}(A_1 \times A_2)$, and the trick is that

$$(1,0) \cdot (0,1) = (0,0) \in \mathfrak{p}.$$

Namely, either $(1,0) \in \mathfrak{p}$ or $(0,1) \in \mathfrak{p}$; without loss of generality, we take $(1,0) \in \mathfrak{p}$. Note that $(0,1) \notin \mathfrak{p}$, for this would imply that $A_1 \times A_2 \subseteq \mathfrak{p}$.

Thus, $(a,b) \in \mathfrak{p}$ if and only if $(a,b)(0,1) \in \mathfrak{p}$ if and only if $(0,b) \in \mathfrak{p}$, so we can write $\mathfrak{p} = A_1 \times \mathfrak{p}'$ for some $\mathfrak{p}'$, and we can verify by hand that $\mathfrak{p}'$ is a prime ideal. ∎

We now go into the proof.

Proof of Theorem 3.54. We have two steps.

1. We start with the local case, where A is a local ring, $\mathfrak{p}$ its unique prime, and $\kappa = A/\mathfrak{p}$. By assumption, $\mathfrak{f}$ is not divisible by any nonzero prime of B lying over $\mathfrak{p}$, and in fact these are all the primes of B because each prime in B must lie over some prime in A, and the only prime available is $\mathfrak{p}$.

   Thus, $\mathfrak{f}$ is not divisible by any prime, so it follows $\mathfrak{f} = (1)$, so $B = A[\theta]$. We now have a nice power basis. We now claim that

   $$B/\mathfrak{p}B \cong \kappa[x]/\left(\overline{p}(x)\right).$$

The point here is that we have the sequence of maps

$$B = A[\theta] \cong \frac{A[x]}{(p(x))} \twoheadrightarrow \frac{(A/\mathfrak{p})[x]}{(p(x))}.$$

Then the kernel of this map consists of the elements of $A[\theta]$ whose coefficients were in $\mathfrak{p}$, which is exactly $\mathfrak{p}B$. So the claim follows.

Continuing, we have by the Chinese remainder theorem that

$$\frac{\kappa[x]}{(\overline{p}(x))} \cong \prod_{k=1}^{r} \frac{\kappa[x]}{(\overline{p}_k(x)^{e_k})}.$$

wut

Now, the point of Lemma 3.56 is that the primes of B lying over $\mathfrak{p}$ are the same as the primes of $B/\mathfrak{p}B$, which is simply the above product, so the primes of B can be identified with the disjoint union

$$\bigsqcup_{k=1}^{r} \operatorname{Spec} \kappa[x]/\left(\overline{p}_k^{e_k}\right).$$

However, any prime $\mathfrak{p}$ of $\kappa[x]/\left(\overline{p}_k^{e_k}\right)$ must contain the zero element $\overline{p}_k^{e_k} + \left(\overline{p}_k^{e_k}\right)$, so any prime must be $\overline{p}_k^{e_k}$. Now going back up to $\operatorname{Spec} \kappa[x]/(\overline{p})$, we find that its prime are the $\overline{p}_\bullet$, which gives

$$\operatorname{Spec} B/\mathfrak{p}B = \{p_k(\theta) : 1 \le k \le r\},$$

so the primes over $\mathfrak{p}$ are of the form $p_k(\theta) + \mathfrak{p}B =: \mathfrak{q}_k$.

Furthermore, we have the diagram for each k.

$$\begin{array}{ccc} \theta & \longrightarrow & x + \left(\overline{p}_k^{e_k}\right) \\ \downarrow & & \downarrow \\ B & \longrightarrow & \kappa[x]/\left(\overline{p}_k^{e_k}\right) \\ \uparrow & & \uparrow \\ A & \longrightarrow & A/\mathfrak{p} \end{array}$$

what is happening

The point here is that $B/\mathfrak{q}_k \cong \kappa[x]/(\overline{p}_k)$, which is a field due to the unique factorization in $\kappa[x]$, so $\mathfrak{q}_k$ is maximal and in particular a nonzero prime of B. Further, we can see that $\kappa \to \kappa[x]/\left(\overline{p}_k\right)$ is injective. The point is that

$$f(\mathfrak{q}_k/\mathfrak{p}) = [B/\mathfrak{q}_k : A/\mathfrak{p}] = [\kappa[x]/\left(\overline{p}_k\right) : \kappa] = \deg \overline{p}_k.$$

wut

We also note that the $\mathfrak{q}_k$ are distinct because the $\overline{p}_k$ are distinct. In fact the $\mathfrak{q}_\bullet$ are all the primes of B because all primes must lie over some prime of A, so all primes of B must lie over $\mathfrak{p} \subseteq A$, so each prime must be a prime in $B/\mathfrak{p}B$, which we classified as our $\mathfrak{q}_\bullet$.

And lastly we have to cover the ramification indices. The point is that

$$\mathfrak{p}B = \prod_{k=1}^{r} \mathfrak{q}_k^{d_k}$$

must be our factorization because the $\mathfrak{q}_\bullet$ are the only available primes. We note that $e_k \ge d_k$ because lots of distribution gives

$$\prod_{k=1}^{r} \mathfrak{q}_k^{e_k} = \prod_{k=1}^{r} (\mathfrak{p}B + p_k(\theta)B)^{e_k} \subseteq \mathfrak{p}B + \left(\prod_{k=1}^{r} p_i(\theta)^{e_k}\right) B = \mathfrak{p}B + p(\theta)B,$$

which is $\mathfrak{p}B$ because $p(\theta) = 0$. Thus,

$$\prod_{k=1}^{r} \mathfrak{q}_k^{d_k} \mathfrak{p}B \;\Big|\; \prod_{k=1}^{r} \mathfrak{q}_k^{e_k},$$

which tells us $d_k \le e_k$ for each k, which is what we wanted.

To finish, we note that

$$n = \sum_{k=1}^{r} e(\mathfrak{q}_k/\mathfrak{p}) f(\mathfrak{q}_k/\mathfrak{p}) = \sum_{k=1}^{r} d_k f_k$$

while

$$\sum_{k=1}^{r} e_k f_k = \deg \overline{p} = \deg p = n,$$

so the termwise $e_k \ge d_k$ inequalities forces $e_k = d_k$ everywhere. This finishes the local case.

2. Now we show the general case. Fix A and B as before, and set $\mathfrak{q}_k := \mathfrak{p}B + p_k(\theta)B$ as in the statement of the problem. Letting $\mathfrak{q}_k' := \mathfrak{p}B_{\mathfrak{p}} + p_i(\theta)B_{\mathfrak{p}}$, we note that the local case above tells us that the $\mathfrak{q}_\bullet'$ are the primes of $B_{\mathfrak{p}}$ lying over $\mathfrak{p}A_{\mathfrak{p}}$, but it is not clear if $\mathfrak{q}_\bullet$ are the primes of B lying over $\mathfrak{p}$. Well,

$$\mathfrak{q}_k B_{\mathfrak{p}} = \mathfrak{p}BB_{\mathfrak{p}} + p_i(\theta)BB\mathfrak{p} = \mathfrak{p}B_{\mathfrak{p}} + p_k(\theta)B_{\mathfrak{p}} = \mathfrak{q}_k'.$$

Now, $\mathfrak{q}_k \supseteq \mathfrak{p}B$, so all the primes in the factorization of $\mathfrak{q}_k$ must consist of primes lying over $\mathfrak{p}$ as well; we let our factorization be

$$\mathfrak{q}_k = \prod_{\ell} \widetilde{\mathfrak{q}_{k\ell}}^{\widetilde{e_{k\ell}}}.$$

Localizing, we set $S := A/\mathfrak{p}$ so that

$$\mathfrak{q}_k' = \mathfrak{q}_k B_{\mathfrak{p}} = S^{-1}\mathfrak{q}_k = \prod_{\ell} \left(S^{-1}\widetilde{\mathfrak{q}_{k\ell}}\right)^{\widetilde{e_{k\ell}}}$$

wut

is a prime factorization of $\mathfrak{q}_k'$. But $\mathfrak{q}_k'$ is prime, so this factorization must collapse into a single prime.

Now, we can get the e_k and the f_k from the local case, and the $\mathfrak{q}_\bullet$ are the only primes above $\mathfrak{p}$ because $\mathfrak{q}_\bullet B_{\mathfrak{p}} = S^{-1}\mathfrak{p}$ is still prime ni $B_{\mathfrak{p}}$, so it must hit one of the $\mathfrak{q}_\bullet'$. So our factorization remains valid up in B.

wut

■

3.6 October 8

3.6.1 Some Examples

Let's do some computations. It'll be fun.

Example 3.57. Take d a squarefree integer not equal to 1, and set $K = \mathbb{Q}(\sqrt{d})$. If for primes $p \nmid d$, we set $\mathcal{O}_K = \mathbb{Z}[\theta]$, where $\theta := \sqrt{d}$. It follows from our computation of $\mathcal{O}_K$ that

$$\mathfrak{f} \mid (2),$$

so we can factor (p) using Dedekind–Kummer. Explicitly, (p) remains prime if and only if $x^2 - d$ remains irreducible if and only if $x^2 \equiv d \pmod{p}$ has a solution.

And we can actually do class group computations now!

Proposition 3.58. We compute the class group of $K := \mathbb{Q}(\sqrt{10})$.

Proof. Here $d_K = 40, n = r = 2, s = 0$, so our Minkowski bound is

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{d_K} = \frac{2}{4}\sqrt{40} = \sqrt{10} < 4.$$

So every ideal class has a representative with an ideal of norm less than 4. This leaves available norms of 2 or 3, which correspond to primes lying over (2) or (3) in $\mathbb{Z}$.

Well, note that with $\theta := \sqrt{10}$, our conductor $\mathfrak{f} = (1)$, so we can use Dedekind–Kummer somewhat freely.

- We have $x^2 - 10 \equiv x \cdot x \pmod 2$, so $(2) = (2, \sqrt{10})^2$. So we see that (2) ramifies.[2] Define $\mathfrak{p} := (2, \sqrt{10})$.
- We have $x^2 - 10 \equiv (x-1)(x+1) \pmod 3$, so $(3) = (3, \sqrt{10}-1)(3, \sqrt{10}+1)$. So we see that (3) splits. Define $\mathfrak{q} := (3, \sqrt{10}+1)$ and $\overline{\mathfrak{q}} := (3, \sqrt{10}-1)$.
- For fun, we can also check that $x^2 - 10$ has no roots $\pmod 7$, so (7) is inert.

So every ideal class has a representative among $\{\mathfrak{p}, \mathfrak{q}, \overline{\mathfrak{q}}\}$. We have the following observations.

(i) However, $[\mathfrak{p}]^2 = [(2)] = [(1)]$. Further, $[\mathfrak{q}][\overline{\mathfrak{q}}] = [(3)] = [(1)]$, so $\mathfrak{q} = \overline{\mathfrak{q}}^{-1}$.

(ii) Additionally, we can check that $\mathfrak{p}$ is not principal. Indeed, if $\mathfrak{p} = (\alpha)$, then $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = 2$, so $\alpha = a + b\sqrt{10}$ forces
$$a^2 - 10b^2 = \pm 2,$$
which is not possible by checking $\pmod 5$. Thus, $[\mathfrak{p}]$ is an element of order 2 in Cl_K.

(iii) We can check in a similar way that $\mathfrak{q}, \mathfrak{q} \neq [(1)]$ because the argument above would ask for
$$a^2 - 10b^2 = \pm 3,$$
which still has no solutions $\pmod 5$.

(iv) To check if $\mathfrak{pq}$ is principal, the argument above requires
$$a^2 - 10b^2 = \pm 4,$$
which has solutions $a \in \{\pm 4\}$ and $b \in \{\pm 1\}$. But we can compute
$$\mathfrak{pq} = (2, \sqrt{10}), (3, 1+\sqrt{10}) = (6, 2+2\sqrt{10}, 3\sqrt{10}, 10+\sqrt{10}),$$
which contains $4 + \sqrt{10}$, so a norm argument forces $\mathfrak{pq} = (4+\sqrt{10})$. Thus, $[\mathfrak{q}] = [\mathfrak{p}^{-1}] = [\mathfrak{p}]$, and so it follows $[\overline{\mathfrak{q}}] = [\mathfrak{p}]$.

So we see that $\mathrm{Cl}_K = \{[(1)], [\mathfrak{p}]\} \cong \mathbb{Z}/2\mathbb{Z}$. ■

3.6.2 Describing Factorization

We have the following definition.

Definition 3.59 (Factoriation types)**.** Fix A, K, L, B as in the $AKLB$ set-up. Fix $\mathfrak{p}$ a nonzero prime of A, and factor $\mathfrak{p}$ by
$$\mathfrak{p} = \prod_{k=1}^{r} \mathfrak{q}_k^{e_k}.$$
Then we have the following.

- $\mathfrak{p}$ is *inert* if and only if $r = e_1 = 1$. (In particular, $f_1 = [L:K]$.)
- $\mathfrak{p}$ is *unramified* if and only if $e_\bullet = 1$ always and $B/\mathfrak{q}_k$ is separable over $A/\mathfrak{p}$. (In global fields, this extra condition does not matter.)
- $\mathfrak{p}$ is *ramified* if and only if is is not unramified.
- $\mathfrak{p}$ is *totally ramified* if and only if $r = f_1 = 1$. (In particular, $e_1 = [L:K]$.)
- $\mathfrak{p}$ is *split completely* if and only if $r = [L:K]$. (In particular, $e_k = f_k = 1$ for each k.)

[2] This is wild.

Example 3.60. Back in $\mathbb{Q}(\sqrt{10})$, we saw (2) was totally ramified, (3) was totally split, and (7) was inert.

We note that if $A = \mathbb{Z}$ with $K = \mathbb{Q}$ so that L is a number field, then for all $\mathfrak{p}$ lying over a nonzero prime $(p) \in \operatorname{Spec} \mathbb{Z}$, then

$$\mathrm{N}\,\mathfrak{q} = [A/\mathfrak{q} : \mathbb{F}_p] = p^{f(\mathfrak{q}/(p))},$$

so norm computations are fairly nice.

We also have the following fact.

Proposition 3.61. Consider the chain of extensions as follows, where $\mathfrak{Q}$ lies above $\mathfrak{q}$ lies above $\mathfrak{p}$.

$$\begin{array}{ccccc} \mathfrak{Q} & \subseteq & C & \subseteq & M \\ | & & | & & | \\ \mathfrak{q} & \subseteq & B & \subseteq & L \\ | & & | & & | \\ \mathfrak{p} & \subseteq & A & \subseteq & K \end{array}$$

Then

$$e(\mathfrak{Q}/\mathfrak{p}) = e(\mathfrak{Q}/\mathfrak{q})e(\mathfrak{q}/\mathfrak{p}) \qquad \text{and} \qquad f(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{q})f(\mathfrak{q}/\mathfrak{p}).$$

Proof. The ramification statement holds by "plugging in" the factorization of $\mathfrak{p}$ from $\mathfrak{q}$ up to $\mathfrak{Q}$ because $\mathfrak{Q}$ will lie over exactly one prime in B.

The inertial degree statement holds because it is merely asserting

$$[C/\mathfrak{Q} : A/\mathfrak{p}] = [C/\mathfrak{Q} : B/\mathfrak{q}][B/\mathfrak{q} : A/\mathfrak{p}],$$

which is true in any tower of fields. ■

3.6.3 Discriminants

We have the following definition.

Definition 3.62. Fix the $AKLB$ setup, as usual. Then the *discriminant* of B over A is the ideal

$$\mathcal{D}_{B/A} := \langle d(\omega_1, \dots, \omega_n) : \{\omega_k\}_{k=1}^n \text{ is a basis of } L/K \text{ in } B \rangle .$$

why

We note that if B/A has an integral basis for B over A, then all the $d(\omega_\bullet)$ will be generated by the discriminant of our integral basis. For example, this occurs when A is a discrete valuation ring. Similarly, because all number rings have an integral basis, we have

$$\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}} = (\operatorname{disc} \mathcal{O}_K)$$

for each number field K.

Naturally, it turns out that discriminants work well localization.

Proposition 3.63. Fix the $AKLB$ setup and S a multiplicative subset of A not containing 0. Then

$$\mathcal{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathcal{D}_{B/A}.$$

Proof. The fact that

$$\mathcal{D}_{S^{-1}B/S^{-1}A} \supseteq S^{-1}\mathcal{D}_{B/A}$$

holds because any generator in $S^{-1}\mathcal{D}_{B/A}$ works as a generator for $S^{-1}B/S^{-1}A$.

For the other inclusion, let $\omega_1, \dots, \omega_n$ be an $S^{-1}B$-basis for L/K. Then multiplying through by the denominators in B, we see that there are $s_\bullet$ such that $\{s_k\omega_k\}$ form a basis for L over K in B. Then

$$d(s_1\omega_1, \dots, s_n\omega_n) = (s_1 \cdots s_n)^n d(\omega_1, \dots, \omega_n),$$

so the extra generators do not help us. ■

The reason that we care about discriminants is the following.

Proposition 3.64. Fix $\mathfrak{p}$ a nonzero prime of A. Then $\mathfrak{p}$ ramifies in B if and only if $\mathfrak{p} \supseteq \mathcal{D}_{B/A}$.

Proof. Localization at $\mathfrak{p}$ does not affect ramification information or the status if $\mathfrak{p}$ dividing the discriminant, so we may suppose that $\mathfrak{p}$ is the only prime of A. But now, $B = A[\theta]$ for some θ for reasons which are unclear, so powers of θ make an integral basis. Letting p be the minimal polynomial of θ, we see

$$\mathcal{D}_{B/A} = \langle \operatorname{disc} \theta^\bullet \rangle = \langle \operatorname{disc} p(x) \rangle.$$

Now, $\mathfrak{p}$ ramifies if and only if $e_\bullet > 1$ somewhere or $(B/\mathfrak{q}_\bullet)/(A/\mathfrak{p})$ is inseparable. This is equivalent to $\overline{p}$ having a repeated factor in its factorization $\pmod{\mathfrak{p}}$ or some factor is inseparable, and this laster statement is equivalent to some factor having multiple roots.

review

So in total, this is equivalent to $\overline{p}$ having multiple roots, which is equivalent to its discriminat $\pmod{\mathfrak{p}}$ vanishing, which is equivalent to $\mathfrak{p}$ dividing into $\mathcal{D}_{B/A}$. ■

3.7 October 11

Maybe we do quadratic reciprocity today.

3.7.1 Housekeeping

Question 3 from homework 6, which asked localization to commute with the conductor, actually applies in the general $AKLB$ set-up. Namely, the assumption that L/K is separable is only needed to have B finite over A. So the proof of Dedekind–Kummer from in class is valid of the $AKLB$ set-up.

Questions 1 and 2 of homework 6, people should have used the fact that the equivalence relation on $S^{-1}A$ was minimal with respect to $\frac{a}{s} = \frac{as'}{ss'}$. In particular, we have the following corollary.

Corollary 3.65. Fix A a ring and S a multiplicative subset. Then for functions $f : S \times A \to B$, if $f(s, a) = f(ss', s'a)$ for each $s, s' \in S$ and $a \in A$, then there is a unique function $f : S^{-1}A \to B$ commuting.

Last time we ended with the following.

Proposition 3.66. Fix the $AKLB$ set-up. A nonzero prime $\mathfrak{p}$ ramifies if and only if $\mathfrak{p} \mid \mathcal{D}_{B/A}$.

We showed this under the assumption $B_\mathfrak{p} = A_\mathfrak{p}[\theta]$ for some $\theta \in B$; we'll need a little more theory (of completions) to prove the result in general.

We do have the following corollary, which we can prove without that theory.

Proposition 3.67. If L/K is separable, then only finitely many primes ramify.

Proof. We note that $\mathcal{D}_{B/A}$ is nonzero, so there are only finitely many prime divisors of $\mathcal{D}_{B/A}$. Further, we can somewhat control the conductor: let θ be a primitive element for L/K in B, and only finitely many primes will divide the conductor for $A[\theta]$ (the conductor is nonzero). So we do have $A_\mathfrak{p}[\theta] = B_\mathfrak{p}$ for all but finitely many primes $\mathfrak{p}$, and the argument works. ■

The above result need not true when L/K fails to be separable.

Non-Example 3.68. Let $A = \overline{\mathbb{F}_p}[t]$ and K its fraction field. Then $L = \overline{\mathbb{F}_p}(t^{1/p})$ and $B = \overline{\mathbb{F}_p}[t^{1/p}]$ (indeed, B is integrally closed and integral over A). Now, for any $\alpha \in \overline{\mathbb{F}_p}$ implies

$$(t-\alpha)B = (t^{1/p} - \alpha^{1/p})^p$$

is ramified for each $\alpha \in \overline{\mathbb{F}_p}$, so there are infinitely many ramified primes.

3.7.2 Quadratic Reciprocity

We start with the following definition.

Definition 3.69 (Legendre symbol)**.** Fix $p \in \mathbb{Z}$ an odd, rational prime. Then, given $a \in \mathbb{Z}$ not divisible by p, we define the *Legendre symbol*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ is a nonzero square} \pmod p, \\ -1 & \text{else.} \end{cases}$$

We have the following.

Proposition 3.70 (Euler's criterion)**.** Fix $p \in \mathbb{Z}$ an odd, rational prime and $a \in \mathbb{Z}$ not divisible by p. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1/2} \pmod p.$$

Proof. Recall that $\mathbb{F}_p^\times$ is cyclic (it is a finite multiplicative subgroup of a field), so fix g a generator so that $a \equiv g^r$ for some $r \in \mathbb{Z}$.

Now, $a^{(p-1)/2} \equiv 1$ if and only if $\zeta^{r(p-1)/2} \equiv 1$ if and only if $p-1 \mid \frac{p-1}{2} \cdot r$ if and only if $2 \mid r$ if and only if a is a square.[3] And to finish, we note that at least

$$a^{(p-1)/2} \in \{\pm 1 \pmod p\}$$

because it squares to $a^{p-1} \equiv 1$, and $x^2 - 1$ only has roots $\{\pm 1\}$. ∎

Corollary 3.71. Fix p an odd, rational prime. Then, for each $a, b \in \mathbb{Z}$ not divisible by p, we have

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. Plug into Euler's criterion to get

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.$$

Now, $p > 2$ implies that we must have equality because $1 \not\equiv -1 \pmod 2$. ∎

And here is quadratic reciprocity.

[3] Showing that $2 \nmid r$ implies that a is not a square is somewhat annoying, but it is not too hard.

Theorem 3.72. Fix p an odd rational prime. Then we have the following.

(a) For an odd rational prime $\ell \neq p$, we have

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}.$$

(b) We have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}.$$

(c) We have

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof. We show (a) but not the others.

(a) Let ζ be a primitive ℓth root of unity (in $\mathbb{C}$), and we work in $\mathbb{Z}[\zeta]$. The key is to try and induce an element in the quadratic subfield of $\mathbb{Z}[\zeta]$; for this, we set

$$\tau := \sum_{a\in\mathbb{F}_\ell^\times} \left(\frac{a}{\ell}\right)\zeta^a.$$

We claim $\tau^2 = \left(\frac{-1}{\ell}\right)\ell$. Indeed, we have

$$\begin{aligned}
\left(\frac{-1}{\ell}\right)\tau^2 &= \sum_{a,b\in\mathbb{F}_\ell^\times} \left(\frac{-1}{\ell}\right)\left(\frac{a}{\ell}\right)\left(\frac{b}{\ell}\right)\zeta^{a+b} \\
&= \sum_{a,b\in\mathbb{F}_\ell^\times} \left(\frac{a}{\ell}\right)\left(\frac{-b}{\ell}\right)\zeta^{a-(-b)} \\
&= \sum_{a,b\in\mathbb{F}_\ell^\times} \left(\frac{a}{\ell}\right)\left(\frac{b}{\ell}\right)\zeta^{a-b} \\
&= \sum_{a,b\in\mathbb{F}_\ell^\times} \left(\frac{ab^{-1}}{\ell}\right)\zeta^{a-b} \\
&= \sum_{b,c\in\mathbb{F}_\ell^\times} \left(\frac{c}{\ell}\right)\zeta^{bc-b} \\
&= \sum_{c\in\mathbb{F}_\ell^\times\setminus\{1\}} \left(\frac{c}{\ell}\right)\sum_{b\in\mathbb{F}_\ell^\times}(\zeta^{c-1})^b + \sum_{b\in\mathbb{F}_\ell^\times} 1 \\
&\overset{*}{=} \sum_{c\in\mathbb{F}_\ell^\times\setminus\{1\}} \left(\frac{c}{\ell}\right)(-1) + (\ell-1) \qquad = \ell,
\end{aligned}$$

where $\overset{*}{=}$ used the fact that ζ^{c-1} will be a primitive ℓth root of unity.

Continuing, we have the equality

$$\tau^p = \tau\left(\tau^2\right)^{(p-1)/2} = \tau\left(\left(\frac{-1}{\ell}\right)\ell\right)^{(p-1)/2} \equiv \tau(-1)^{\frac{\ell-1}{2}\cdot\frac{p-1}{2}}\left(\frac{\ell}{p}\right).$$

On the other hand, applying the Frobenius automorphism tells us

$$\tau^p \equiv \sum_{a\in\mathbb{F}_\ell^\times}\left(\frac{a}{\ell}\right)\zeta^{ap} = \left(\frac{p}{\ell}\right)\sum_{a\in\mathbb{F}_\ell^\times}\left(\frac{pa}{\ell}\right)\zeta^{ap} = \left(\frac{p}{\ell}\right)\tau.$$

So in total, we divide out by τ (which is a unit $\pmod p$ because $\tau^2 \in \{\pm\ell\}$ is a unit)

$$(-1)^{\frac{\ell-1}{2}\cdot\frac{p-1}{2}}\left(\frac{\ell}{p}\right) \equiv \left(\frac{p}{\ell}\right) \pmod p,$$

which finishes because $1 \not\equiv -1 \pmod p$, even in $p\mathbb{Z}[\zeta]$. ■

3.8 October 13

Here we go.

3.8.1 Quadratic Reciprocity Example

Let's start with some applications of quadratic reciprocity.

Example 3.73. We can check if 101 is a square $\pmod{223}$. Well, $101 \equiv 1 \pmod 4$, so we have

$$\left(\frac{101}{223}\right) = \left(\frac{223}{101}\right) = \left(\frac{21}{101}\right).$$

Now, factoring $21 = 3 \cdot 7$, we can compute

$$\left(\frac{21}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{7}{101}\right) = \left(\frac{101}{3}\right)\left(\frac{101}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{7}\right).$$

because $101 \equiv 1 \pmod 4$. We can compute by hand that $\left(\frac{2}{3}\right) = -1$ and $\left(\frac{3}{7}\right) = -1$, so indeed, $\left(\frac{101}{223}\right) = 1$.

3.8.2 Decomposition Groups

Fix $AKLB$ as usual, and for this subsection will assume that L/K is a Galois extension with $G := \mathrm{Gal}(L/K)$. The point is that G acts on B fixing A, which will give us some structure. Here, fix $\mathfrak{p}$ a nonzero prime of A, and we let

$$\mathfrak{p} = \prod_{k=1}^{r} \mathfrak{q}_k^{e_k}$$

our factorization of $\mathfrak{p}B$ up in B. And as usual, take $f_k := f(\mathfrak{q}_k/\mathfrak{p})$. The key claim is as follows.

Lemma 3.74. Fix everything as above. Then G acts transitively on the $\{\mathfrak{q}_k\}_{k=1}^r$.

Proof. That there is a G-action comes down to the fact that, for each $\sigma \in G$, $\sigma\mathfrak{q}_\bullet$ must be some prime (σ is an automorphism, so this is not hard to check), and $\sigma\mathfrak{q}_\bullet$ must live over $\mathfrak{p}$ because $\sigma\mathfrak{q}_\bullet \cap A = \sigma(\mathfrak{q}_\bullet \cap A) = \sigma\mathfrak{p} = \mathfrak{p}$.

Showing that the action is transitive requires some trickery. Suppose for the sake of contradiction that $\mathfrak{q}_k$ and $\mathfrak{q}_\ell$ have different orbits under the G-action. The trick is to find $\alpha \in B$ such that

$$\alpha \equiv 1 \pmod{\sigma\mathfrak{q}_k} \qquad \text{and} \qquad \alpha \equiv 0 \pmod{q_\ell}$$

for each $\sigma \in G$; this exists by the Chinese remainder theorem. But now $\mathrm{N}_K^L\,\alpha \notin \mathfrak{q}_k \cap A = \mathfrak{p}$ from the left while $\mathrm{N}_K^L\,\alpha \notin \mathfrak{q}_\ell \cap A = \mathfrak{p}$ from the right. This is a contradiction. ■

And here is the main result.

Corollary 3.75. The e_k and f_k do not depend on k.

Proof. Apply σ to the prime factorization of $\mathfrak{p}$ to get that the e_k are independent of k. To get that the f_k are independent of k, we note that $\mathfrak{q}_k = \sigma\mathfrak{q}_\ell$ has the isomorphism

$$A/\mathfrak{q}_k \to A/\mathfrak{q}_\ell$$

by applying σ. ∎

The above tells us that

$$n := [L : K] = \sum_{k=1}^{r} e(\mathfrak{q}_k/\mathfrak{p}) f(\mathfrak{q}_k/\mathfrak{p}) = ref,$$

where $e = e_k$ and $f = f_k$ for each k. Namely, $\#G = ref$.

To keep better track of our data, we have the following definitions.

Definition 3.76 (Decomposition group)**.** Fix everything as above, and fix some $\mathfrak{q}$ over $\mathfrak{p}$. Then we define the *decomposition group* of $\mathfrak{q}$ is

$$G_{\mathfrak{q}} = \{\sigma \in G : \sigma\mathfrak{q} := \mathfrak{q}\},$$

the stabilizer of $\mathfrak{q}$ under the G-action.

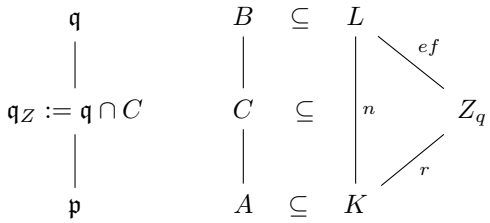
We have some small remarks.

- We remark that $[G : G_{\mathfrak{q}}]$ is the size of the orbit of $\mathfrak{q}$ by group theory, which is exactly the number of primes r. It follows $\#G_{\mathfrak{q}} = \#G/r = ef$ from earlier.
- Note that if we place $\mathfrak{q}$ with some $\sigma\mathfrak{q}$, then we have $G_{\sigma\mathfrak{q}} = \sigma G_{\mathfrak{q}} \sigma^{-1}$, again by group theory.

And Galois theory also provides us with a decomposition field.

Definition 3.77 (Decomposition field)**.** Fix everything as before. Then the *decomposition field* of $\mathfrak{q}$ is $Z_{\mathfrak{q}}$ is the fixed field of $G_{\mathfrak{q}}$.

Here is the diagram.



So what is $\mathfrak{q}_Z$? Well, because $\mathrm{Gal}(L/Z_{\mathfrak{q}}) = G_{\mathfrak{q}}$, all the primes over $\mathfrak{q}_Z$, of which $\mathfrak{q}$ is one, need to live in the orbit of $\mathfrak{q}$, which is $\{\mathfrak{q}\}$. So the only prime above $\mathfrak{q}_Z$ is $\mathfrak{q}$, and our r here is 1.

We can also check that $\#G_{\mathfrak{q}} = e(\mathfrak{q}/\mathfrak{q}_Z) f(\mathfrak{q}/\mathfrak{q}_Z) = ef$ because they are both the size of the decomposition group for $\mathfrak{q}$ for L/Z_q and L/K respectively. But multiplicativity forces

$$e(\mathfrak{q}/\mathfrak{q}_Z) \le e \qquad \text{and} \qquad f(\mathfrak{q}/\mathfrak{q}_Z) \le e.$$

So we are forced into $e(\mathfrak{q}_Z/\mathfrak{q}) = e$ and $f(\mathfrak{q}_Z/\mathfrak{q}) = f$, which forces $e(\mathfrak{q}_Z/\mathfrak{p}) = f(\mathfrak{q}_Z/\mathfrak{p}) = 1$. The point is the following.

Proposition 3.78. Fix everything as above. Then we have the following.

1. $\mathfrak{q}_Z$ is nonsplit in B.
2. $e(\mathfrak{q}/\mathfrak{q}_Z) = e$ and $f(\mathfrak{q}/\mathfrak{q}_Z) = f$.
3. $\mathfrak{q}_Z$ has ramification index and inertial degree 1 over $\mathfrak{p}$.

Proof. This follows from the above discussion. ■

Here is another reason why the decomposition group is good: they help control our residue fields.

Proposition 3.79. Fix evreything as above. We have that $B/\mathfrak{q}$ is a normal field extension of $A/\mathfrak{p}$, and there is a canonical surjective group homomorphism

$$G_{\mathfrak{q}} \twoheadrightarrow \mathrm{Gal}\left(\frac{B/\mathfrak{q}}{A/\mathfrak{p}}\right).$$

Even though we are writig Gal, we are not actually requiring the field extension to be Galois. (Namely, we ought work in the maximal separable subextension of $B/\mathfrak{q}$ over $A/\mathfrak{p}$.)

Proof. We note that $f(\mathfrak{q}_Z/\mathfrak{p}) = 1$ forces $C/\mathfrak{q}_Z \cong A/\mathfrak{p}$, so we are allowed to focus on $\mathfrak{q}_Z$ instead, by taking $K \leftarrow Z_{\mathfrak{q}}$ and $G \leftarrow G_{\mathfrak{q}}$. Namely, the corresponding residue fields we care about remain unchanged.

Now, set $\lambda := B/\mathfrak{q}$ and $\kappa := A/\mathfrak{p}$, for convenience. We have two claims.

- We show that λ/κ is normal by showing that all irreducible polynomials of $\kappa[x]$ which have a root in λ will fully factor in λ.

  Indeed, take some irreducible polynomial $\overline{g} \in \kappa[x]$ with a root of $\overline{\theta} \in B$. Pulling back $\overline{\theta}$ to some $\theta \in B$, we can give it minimal polynomial $f \in A[x]$. But now f has a root in L, and because L/K is normal (!), f will fully split up in $L[x]$, so $\overline{f}$ will also fully split down in $\lambda[x]$.

  Now, because $\overline{\theta}$ is a root of $\overline{f}$, the fact that $\overline{g}$ was irreducible will force $\overline{g} \mid \overline{f}$, but $\overline{f}$ fully splits into linear factors, so $\overline{g}$ also fully splits into linear factors. This finishes the proof that λ/κ is normal.

- We define our map $G_{\mathfrak{q}} \to \mathrm{Hom}_{\kappa}(\kappa(\overline{\theta}), \lambda)$ by

  $$\varphi : \sigma \mapsto (\overline{\theta} \mapsto \overline{\theta}),$$

  upon fixing some primitive element for the separable closure of λ over κ. (In particular, we will see that $\mathrm{Hom}_{\kappa}(\kappa(\overline{\theta}), \lambda) = \mathrm{Gal}(\lambda^{\mathrm{sep}}/\kappa)$.) We can check that this is well-defined: if $\overline{\alpha_1} = \overline{\alpha_2}$ for $\alpha_1, \alpha_2 \in K(\theta) \cap B$, then this is equivalent to $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{q}}$, so $\alpha_1 - \alpha_2 \in \mathfrak{q}$, so

  $$\sigma(\alpha_1 - \alpha_2) \in \sigma\mathfrak{q} = \mathfrak{q}$$

  because $\sigma \in G_{\mathfrak{q}}$, from which $\overline{\sigma(\alpha_1)} = \overline{\sigma(\alpha_2)}$ follows.

  We note that $\sigma \mapsto \overline{\sigma}$ is canonical because $\overline{\sigma}$ always takes $\overline{\alpha}$ to $\overline{\sigma(\alpha)}$, no matter what choice of $\overline{\theta}$ we made. So no choices were "required" for the proof.

  It remains to show $\sigma \mapsto \overline{\sigma}$ is surjective. So let $\overline{\tau}$ be any element of $\mathrm{Gal}(\lambda/\kappa)$. Again using our primitive element $\overline{\theta}$, we set $\overline{g}$ its minimal irreducible polynomial and plug into the normality argument above. Using that notation, $\overline{\theta}$ is the root of $\overline{f}$, as is $\overline{\tau}(\overline{\theta})$, and pulling everything back we have $\tau \in G_{\mathfrak{q}}$ such that $\tau(\theta)$ has $\overline{\tau(\theta)} = \overline{\tau}(\overline{\theta})$. But then see τ goes to $\overline{\tau}$ because they have the same behavior on $\overline{\theta}$, finishing. ■

3.9 October 15

For today, our $AKLB$ setup will require L/K to be a Galois extension, with $G := \mathrm{Gal}(L/K)$. We also fix $\mathfrak{p}$ a nonzero prime of A with $\mathfrak{q}$ over $\mathfrak{p}$. As usual, we take $G_{\mathfrak{q}}$ the decomposition group (stabilizer) of $\mathfrak{q}$ under the G-action.

For brevity, we will also define $\lambda := B/\mathfrak{q}$ and $\kappa := A/\mathfrak{p}$.

3.9.1 Inertia Groups

Recall that we defined a surjective group homomorphism $\varphi : G_{\mathfrak{q}} \twoheadrightarrow \mathrm{Gal}(\lambda/\kappa)$ such that

$$\varphi(\sigma)(\overline{\alpha}) = \overline{\sigma\alpha},$$

where $\sigma \in G_{\mathfrak{q}}$ and $\alpha \in B$.

We want the above to be an isomorphism, so let's make it an isomorphism.

Definition 3.80 (Inertia group)**.** The group *inertia group* $I_{\mathfrak{q}}$ of $\mathfrak{q}$ over K is the kernel of our map $G_{\mathfrak{q}} \twoheadrightarrow \mathrm{Gal}(\lambda/\kappa)$. In other words, $\sigma \in I_{\mathfrak{q}}$ if and only if

$$\sigma\theta \equiv \theta \pmod{\mathfrak{q}}$$

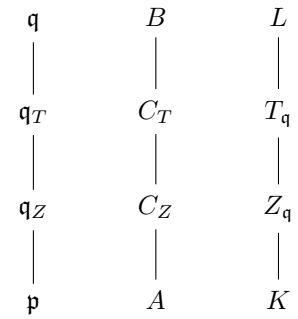
for each $\theta \in B$. This also lets us define $T_{\mathfrak{q}}$, the *inertial field*.

We remark that we could also define

$$I_{\mathfrak{q}} = \{\sigma \in G : \sigma\theta \equiv \theta \pmod{\mathfrak{q}} \text{ for all } \theta \in B\}.$$

Indeed, the only thing to check here is that $\sigma \in I_{\mathfrak{q}}$ implies $\sigma \in G_{\mathfrak{q}}$, which is true because $\sigma \in G_{\mathfrak{q}}$ only means that $\theta \equiv 0$ implies $\sigma\theta \equiv 0 \pmod{\mathfrak{q}}$.

So the chain of subgroups $I_{\mathfrak{q}} \subseteq G_{\mathfrak{q}} \subseteq G$ gives the following diagram.



So what do we expect based on the numbers?

Proposition 3.81. We have that $T_{\mathfrak{q}}$ is Galois over $Z_{\mathfrak{q}}$, and $\mathrm{Gal}(T_{\mathfrak{q}}/Z_{\mathfrak{q}}) \cong \mathrm{Gal}(\lambda/\kappa)$ and $\mathrm{Gal}(L/T_{\mathfrak{q}}) \cong I_{\mathfrak{q}}$.

Proof. This is essentially Galois theory. Namely, $I_{\mathfrak{q}}$ is normal in $G_{\mathfrak{q}}$ because it is a kernel, so $T_{\mathfrak{q}}$ is normal over $Z_{\mathfrak{q}}$. Then $\mathrm{Gal}(T_{\mathfrak{q}}/Z_{\mathfrak{q}}) \cong \mathrm{Gal}(\lambda/\kappa)$ and $\mathrm{Gal}(L/T_{\mathfrak{q}}) \cong I_{\mathfrak{q}}$ by tracking the quotient of the Galois groups through in the diagram. ∎

Proposition 3.82 (Split, inert, ramify)**.** Suppose that λ is separable over κ (which is reasonable because most cases we care about will have κ finite). Then $\#I_{\mathfrak{q}} = [L : T_{\mathfrak{q}}] = e$ and $[G_{\mathfrak{q}} : I_{\mathfrak{q}}] = [T_{\mathfrak{q}} : Z_{\mathfrak{q}}] = f$. It follows

$$e(\mathfrak{q}/\mathfrak{q}_T) = e(\mathfrak{q}/\mathfrak{p}) \qquad \text{and} \qquad e(\mathfrak{q}_T/\mathfrak{p}) = 1,$$

and

$$f(\mathfrak{q}/\mathfrak{q}_T) = 1 \qquad \text{and} \qquad f(\mathfrak{q}_T/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}).$$

Proof. We see $\#I_{\mathfrak{q}} = [L : T_{\mathfrak{q}}]$ and $[G_{\mathfrak{q}} : I_{\mathfrak{q}}] = [T_{\mathfrak{q}} : Z_{\mathfrak{q}}]$ by Galois theory. The other claims are left as an exercise. ■

Corollary 3.83. Still taking λ separable over κ, we have $\mathfrak{q}$ unramified over K if and only if $\#I_{\mathfrak{q}} = 1$.

Proof. This follows by tracking our indices through in the above discussion. ■

So here is our diagram.

$$\begin{array}{ccc}
\mathfrak{q} & B & L \\
{\scriptstyle e=e,f=1}\big| & \big| & \big| \\
\mathfrak{q}_T & C_T & T_{\mathfrak{q}} \\
{\scriptstyle e=1,f=f}\big| & \big| & \big| \\
\mathfrak{q}_Z & C_Z & Z_{\mathfrak{q}} \\
{\scriptstyle e=1,f=1}\big| & \big| & \big| \\
\mathfrak{p} & A & K
\end{array}$$

We remark that we also have the following definition.

Definition 3.84 (Higher ramification)**.** There are *higher ramifiaction* groups

$$I_{\mathfrak{q}} = I_{\mathfrak{q},0} \supseteq I_{\mathfrak{q},1} \supseteq I_{\mathfrak{q},2}.$$

These are useful to keep track of the following.

Definition 3.85 (Tame and wild ramification)**.** We say that $\mathfrak{q}$ is *tamely ramified* if and only if $\operatorname{char}\kappa = 0$ or $\operatorname{char}\kappa \nmid \#I_{\mathfrak{q}}$ with λ/κ separable. Then $\mathfrak{q}$ is *wildly ramified* otherwise.

Namely, $I_{\mathfrak{q},1}$ helps capture wild ramification.

3.9.2 Cyclotomic Fields

In the discussion that follows, fix n a positive integer, and let ζ be a primitive nth root of unity. Then we recall from Galois theory that

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) \qquad \text{and} \qquad \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

where the isomorphism on the right is by taking $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ to $a \mapsto (\zeta \mapsto \zeta^n)$.

Removing our picture from view, we fix $K = \mathbb{Q}(\zeta)$. Our goal for now is to compute $\mathcal{O}_K$. As a spoiler, we want it to be $\mathbb{Z}[\zeta]$. Let's start with prime powers.

Lemma 3.86. Fix $n := \ell^\nu$ a prime-power, where ℓ is prime and ν a positive integer. Fixing $K := \mathbb{Q}(\zeta)$ and $\lambda := 1 - \zeta$, and we claim the following.

(a) The ideal (λ) is prime with absolute norm ℓ.

(b) We have $\ell\mathcal{O}_K = (\lambda)^d$, where $d = \varphi(n)$.

(c) The power basis $\{\zeta^k\}_{k=0}^{d-1}$ of $K/\mathbb{Q}$ has discriminant $\pm\ell^s$, where $s = \ell^{\nu-1}(\nu\ell - \nu - 1)$.

Proof. Let f be the irreducible polynomial of ζ, which is

$$f(x) = \frac{x^n - 1}{x^{n/p} - 1} = 1 + x^{n/p} + x^{2n/p} + \cdots + x^{n-n/p},$$

which is

$$f(x) = x^{\ell^{\nu-1}(\ell-1)} + x^{\ell^{\nu-1}(\ell-2)} + \cdots + x^{\ell^{\nu-1}} + 1.$$

Now, the irreducible polynomial of λ is $(-1)^d f(1-x)$, where the $(-1)^d$ adjusts for sign. In particular, we can compute that our degree is $d = \ell^{\nu-1}(\ell-1)$, and the constant term is $(-1)^d\ell$.

It follows that the product of the conjugates of λ is $(-1)^d\ell$, so (λ) has absolute norm ℓ, implying that (λ) is a prime and lies over ℓ. Further, its conjugates are of the form, for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$(1 - \zeta^a) = (1 - \zeta)\left(1 + \cdots + \zeta^{a-1}\right),$$

which is divisible by λ, but this forces $(1 - \zeta^a) = (1-\zeta)$ because both factors need to have the same absolute norm (we can apply an automorphism to get one from the other). Thus, we see that

$$(\ell) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (1 - \zeta^a) = (\lambda)^d,$$

so in fact ℓ fully splits, with inertial index 1, ramification index d, and only a single prime above it.

It remains to check (c). Well, we have to compute

$$\prod_{1 \le k < \ell \le d-1} \left(\zeta^k - \zeta^\ell\right)^2 = \pm \prod_{\substack{k,\ell=1 \\ k \ne \ell}}^{d-1} \left(\zeta^k - \zeta^\ell\right).$$

But now $\zeta^k - \zeta^\ell$ is a power of λ (it might not equal to λ because it might have $k - \ell$ not coprime to ℓ). Then this will eventually fully collapse down to $\pm\ell^s$ by tracking all of this through, where s as in the statement. ■

And now we can show $\mathcal{O}_K = \mathbb{Z}[\zeta]$ in this case.

Lemma 3.87. Again fix $n := \ell^\nu$ a prime-power as before, with $K := \mathbb{Q}(\zeta)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Proof. The index of $[\mathcal{O}_K : \mathbb{Z}[\zeta]]$ must be a power of ℓ because it needs to divide the discriminat of the power bases $\zeta^\bullet$. By our computation of the inertial index, we see that

$$\mathcal{O}_K/\lambda\mathcal{O}_K \cong \mathbb{Z}/\ell\mathbb{Z},$$

so in particular, the map $\mathbb{Z} \to \mathcal{O}_K/\lambda\mathcal{O}_K$ is surjective (with kernel $\ell\mathbb{Z}$). Then we have the computation

$$\mathcal{O}_K = \mathbb{Z} + \lambda\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda\mathcal{O}_K,$$

but now we can re-substitute (!) back into $\mathcal{O}_K$ as many times as we wish to see that $\mathcal{O}_K = \mathbb{Z}[\zeta] + \ell^\bullet\mathcal{O}_K$ for as high a power of $\ell^\bullet$ as we please. But by our disctiminat computation, $\ell^s \in \mathbb{Z}[\zeta]$, so at this point we conclude that $\mathcal{O}_K = \mathbb{Z}[\zeta]$. ■

Next time we will take n arbitrary, using the prime-power case and some strong induction.

3.10 October 18

We do more on cyclotomic fields today. In today's class, we will fix n a positive integer, and $\zeta = \zeta_n = e^{2\pi i/n} \in \mathbb{C}$ (more generally, any primitive nth roof of unity will do).

3.10.1 Talking $\mathcal{O}_{\mathbb{Q}(\zeta)}$

Recall that last time we showed the following.

Proposition 3.88. Fix $n = \ell^\nu$ with ℓ prime and $\nu \in \mathbb{Z}^+$. Setting $\lambda := 1 - \zeta$ and $K = \mathbb{Q}(\zeta)$, then we have the following.

- $\mathcal{O}_K = \mathbb{Z}[\zeta]$
- $\ell\mathcal{O}_K = (\lambda)^{\varphi(n)}$
- (λ) is prime of absolute norm ℓ
- $d_K = \ell^{\nu-1}(\nu\ell - \nu - 1)$

We now move to general positive integers.

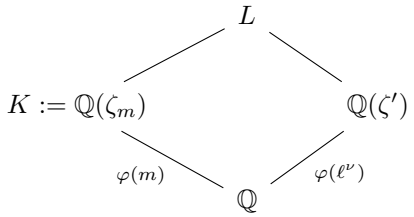
Proposition 3.89. For any positive integer n, we set $L = \mathbb{Q}(\zeta)$ so that $\mathcal{O}_L = \mathbb{Z}[\zeta] >$

Proof. The book uses an intermediate lemma that two Galois extensions with rings of integers with coprime discriminant lets us compute the ring of integers of the composite field by direct multiplication. We will not do this here.

We do strong induction on n. The base case is if n is a prime power, which we already took care of above. (If $n = 1$, this taking $L = \mathbb{Q}$ where $\mathcal{O}_L = \mathbb{Z}$.) Otherwise, we take n with at least two distinct prime factors. Suppose for the sake of contradiction that $\mathcal{O}_L \neq \mathbb{Z}[\zeta]$, and we take

$$p \mid [\mathcal{O}_L : \mathbb{Z}[\zeta]]$$

and ℓ a prime divisor of n not equal to p. Now factor $n = \ell^\nu m$ with $\ell \nmid m$, and set $\zeta' := \zeta_{\ell^\nu}$. This gives the following tower of fields.



We note that $L = K(\zeta')$ because we can write $\zeta = (\zeta')^r(\zeta_m)^s$ for some $r, s \in \mathbb{Z}$ because ℓ^ν and m are relatively prime, letting us use Bezout's lemma here. Additionally, we notice that

$$[L : K] = \frac{\varphi(n)}{\varphi(m)} = \varphi\left(\ell^\nu\right) = [\mathbb{Q}(\zeta') : \mathbb{Q}],$$

so the extension L/K is a "lifting" of $\mathbb{Q}(\zeta')/\mathbb{Q}$. In particular, this degree comparison forces that ζ' has the same irreducible polynomial over K as over $\mathbb{Q}$.

Now, by the inductive hypothesis, take $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, and let $S = \mathbb{Z} \setminus (p)$. We have two parts to the rest of the proof.

- We quickly claim that $S^{-1}\mathcal{O}_L \neq S^{-1}\mathbb{Z}[\zeta]$. In other words, our inequality of rings is preserved under this localization. Well, we have the following diagram of abelian groups with exact row and column.

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ & & & & & & \mathbb{Z}/p\mathbb{Z} & & \\ & & & & & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}[\zeta] & \longrightarrow & \mathcal{O}_L & \longrightarrow & \mathcal{O}_L/\mathbb{Z}[\zeta] & \longrightarrow & 0 \end{array}$$

  Namely, $p \mid \#(\mathcal{O}_L/\mathbb{Z}[\zeta])$, so there's an element of order p in the group by Cauchy's theorem. Localizing by S everywhere, we maintain exactness, giving the following diagram.

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ & & & & & & S^{-1}\mathbb{Z}/p\mathbb{Z} & & \\ & & & & & & \downarrow & & \\ 0 & \longrightarrow & S^{-1}\mathbb{Z}[\zeta] & \longrightarrow & S^{-1}\mathcal{O}_L & \longrightarrow & S^{-1}\mathcal{O}_L/\mathbb{Z}[\zeta] & \longrightarrow & 0 \end{array}$$

wut

  Here, we do have that $S^{-1}\mathbb{Z}/p\mathbb{Z} \neq 0$ because embedding S into $\mathbb{Z}/p\mathbb{Z}$ must send it to nonzero elements, so we are merely inverting out the nonzero elements of the field, so there are nonzero elements to mod out here. It follows that $S^{-1}\mathcal{O}_L \neq S^{-1}\mathbb{Z}[\zeta]$ by the exactness of the bottom row because the quotient object of the short exact sequence is nonzero.

- But now we claim the opposite, that $S^{-1}\mathcal{O}_L = S^{-1}\mathbb{Z}[\zeta]$. Indeed, we have that

$$\mathcal{O}_K = \mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta^{n/m}],$$

it is?

  but now because ζ' has the same irreducible polynomial over K as over $\mathbb{Q}$, we find that ζ' gives a power basis for L over K, and the discriminant is again a power of ℓ up to sign, but this is a unit in $S^{-1}\mathcal{O}_K$ and hence in $S^{-1}\mathbb{Z}$ (!).

why

  In particular, $S^{-1}\mathcal{O}_K$ only has finitely many maximal ideals (it only has the ones lying above (p)) and Dedekind, it is a principal ideal domain, and in particular, we see that $S^{-1}\mathcal{O}_L$ has an integral basis over $S^{-1}\mathcal{O}_K$, which we call $\{\omega_k\}_{k=1}^d$, where $d := \varphi(\ell^\nu)$. Letting M be the matrix expressing the $(\zeta')^\bullet$ in terms of the $\omega_\bullet$, we see that

$$d(1, \zeta', \dots, (\zeta')^{d-1}) = (\det M)^2 d(\omega_\bullet).$$

  But now the left hand-side is a unit in $S^{-1}\mathcal{O}_K$, and both factors are in $S^{-1}\mathcal{O}_K$, we must have that both factors are themselves units, so in particular $\det M$ is a unit in $S^{-1}\mathcal{O}_K$. Now it follows that

$$S^{-1}\mathcal{O}_L = S^{-1}\mathcal{O}_K[\zeta']$$

  by change of basis with M, and

$$S^{-1}\mathcal{O}_K[\zeta'] = S^{-1}\mathbb{Z}[\zeta]$$

  because $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta_m, \zeta'] = \mathcal{O}_K[\zeta']$. This finishes the proof. ∎

3.10.2 Combining Cyclotomic Fields

Here are some extra definitions.

Definition 3.90 (Roots of unity)**.** Fix k a field with n a positive integer. Then we set

$$\mu_n(k) := \{x \in k : x^n = 1\}.$$

With no argument, we set $\mu_n = \mu_n(\overline{k})$.

Observe that as long as the characteristic of k does not divide n, then μ_n will have n elements by looking for a primitive root of unity; otherwise, it might have fewer.

We recall we have the following lemmas.

Lemma 3.91. We have that $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\operatorname{lcm}(m,n)})$.

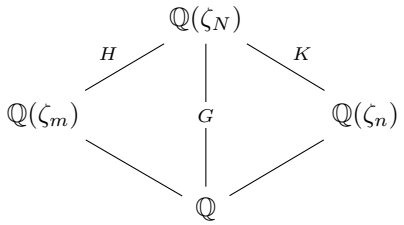
Proof. Indeed, $\zeta_n, \zeta_m \in \mathbb{Q}(\zeta_{\operatorname{lcm}(m,n)})$ shows that $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{\operatorname{lcm}(m,n)})$; and in the other direction, note that $\frac{\operatorname{lcm}(n,m)}{n}$ and $\frac{\operatorname{lcm}(n,m)}{m}$ are relatively prime, so we can find integers r and s so that

$$r \cdot \frac{\operatorname{lcm}(n,m)}{n} + s \cdot \frac{\operatorname{lcm}(n,m)}{m} = 1,$$

from which it follows $\zeta_{\operatorname{lcm}(m,n)} = \zeta_m^r \zeta_n^s$. ∎

Lemma 3.92. We have that $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\gcd(m,n)})$.

Proof. Certainly $\zeta_n, \zeta_m \in \mathbb{Q}(\zeta_{\gcd(m,n)})$, so $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{\gcd(m,n)})$. In the other direction, we use Galois theory. Fix $N := \operatorname{lcm}(m,n)$ and $g := \gcd(m,n)$. We have the following Galois diagram.



In particular, we set H and K to be the corresponding subgroups of $G := \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ which fix $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$ respectively. Namely, $G \cong (\mathbb{Z}/N\mathbb{Z})^\times$, and H is the kernel of $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ by projection, or in other words

$$H = \left\{a \in (\mathbb{Z}/N\mathbb{Z})^\times : a \equiv 1 \pmod{m}\right\},$$

and similar for K as $\{a \in (\mathbb{Z}/N\mathbb{Z})^\times : a \equiv 1 \pmod{n}\}$. We would like to show that $\mathbb{Q}(\zeta_{\gcd(m,n)}) \subseteq \mathbb{Q}(\zeta_n) \cap (\zeta_m)$, which the Galois correspondence says is the same as showing the reverse $HK \subseteq \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_g))$.

Well, if we factor $N = \prod \ell^{\nu_\ell}$, then

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong \prod (\mathbb{Z}/\ell^{\nu_\ell}\mathbb{Z})^\times,$$

and H and K will correspond to some product of these subgroups, as HK will be. This finishes, where the details are left as exercise. ∎

wut

And we'll close off by working towards the following result.

Proposition 3.93. Fix n a positive integer and p a prime, and write $n = p^\nu m$ (where $\nu = 0$ is permitted) with $p \nmid m$. Fixing $\mathfrak{q}$ a prime of $K := \mathbb{Q}(\zeta_n)$ lying over (p), and set f_p the multiplicative order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then

$$f(\mathfrak{q}/p) = f_p \qquad \text{and} \qquad e(\mathfrak{q}/p) = \varphi\left(p^\nu\right).$$

Proof. We'll save this proof for Wednesday. ■

Here is a corollary of this result.

Corollary 3.94. Fix n a positive integer. Then odd primes p ramify in $\mathbb{Q}(\zeta_n)$ if and only if $p \mid n$. Further, (2) ramifies if and only if $4 \mid n$.

Proof. By the previous result, we are testing for $\varphi(p^\nu) \geq 1$. If p is odd, this is equivalent to $\nu \geq 1$ is equivalent to $p \mid n$. If $p = 2$, then this is equivalent to $\nu \geq 2$ is equivalent to $4 \mid n$. ■

Note the second part roughly comes from the fact that $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$ when m is odd.

3.11 October 20

The fun continues.

3.11.1 Splitting in Cyclotomic Fields

As usual, for each $n \in \mathbb{Z}^+$, we set $\zeta_n := e^{2\pi i/n}$. We recall the following proposition.

Proposition 3.95. Fix n a positive integer and p a prime, and write $n = p^\nu m$ (where $\nu = 0$ is permitted) with $p \nmid m$. Fixing $\mathfrak{q}$ a prime of $K := \mathbb{Q}(\zeta_n)$ lying over (p), and set f_p the multiplicative order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then

$$f(\mathfrak{q}/p) = f_p \qquad \text{and} \qquad e(\mathfrak{q}/p) = \varphi(p^\nu).$$

Proof. We do some cases.

- Suppose that $p \nmid n$. We can use Dedekind–Kummer freely because our extension is monogenic, so we note that $x^n - 1$ has p distinct roots in $\overline{\mathbb{F}_p}$, so it follows that our ramification index is 1 everywhere. Fix $\mathfrak{q}$ some prime over $\mathfrak{p}$.

  Now, by homework, there is a unique $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that for each α,

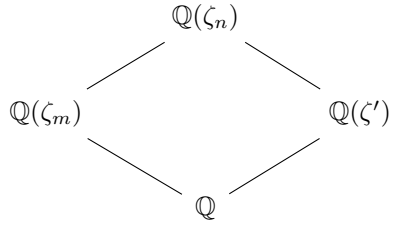
  $$\sigma\alpha \equiv \alpha^p \pmod{\mathfrak{q}},$$

  which is our Frobenius element. By taking $a = \zeta_n$, we see that σ is simply $\overline{p} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Now, the inertial index $f(\mathfrak{q}/\mathfrak{p})$ is equal to the degree $\mathcal{O}_K/\mathfrak{q}$ over $\mathbb{F}_p$, so by looking at the size of the Galois group (here we are using that the Galois group is cyclic generated by this σ), it is the least f for which

  $$\alpha^{p^f} \equiv \alpha \pmod{\mathfrak{q}}$$

  for each α. But now pushing this through into our Galois group, we are asserting that f is minimal for $\sigma^f = \mathrm{id}$, which is equivalent to f minimal for $\overline{p}^f = 1$. So indeed, $f(\mathfrak{q}/\mathfrak{p})$ is the multiplicative order of $p \pmod{m}$.

- Let's do the general case now. Fix $\zeta' := \zeta_{p^\nu}$. We have the following diagram.



Indeed, because $\gcd(m, p^\nu) = 1$, we have that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta') = \mathbb{Q}$ and $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta') = \mathbb{Q}(\zeta_n)$.

However, the main point is that the irreducible polynomial of ζ_m over $\mathbb{Q}(\zeta')$ is the same as the irreducible polynomial over $\mathbb{Q}$, using our Galois extension lifting argument.

Now, because $p \nmid m$, primes over p in $\mathbb{Q}(\zeta_m)$ are unramified, essentially using the special case above. By the Galois lifting, the irreducible polynomial of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}(\zeta')$ is the same as the irreducible polynomial for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$, so this comes from Dedekind–Kummer.

So checking our tower, we see that $e(\mathfrak{p}/K) = e(\mathfrak{p}/\mathbb{Q}(\zeta'))$, which is $\varphi(p^\nu)$ because (p) totally ramifies here. (For example, check the irreducible polynomial again.)

It remains to compute the inertial degree $f(\mathfrak{p}/K)$. The point is that the unique prime over p in $\mathbb{Q}(\zeta')$ is totally ramified over $\mathbb{Q}(\zeta_n)$, so the inertial index is 1 here. Thus, for each prime $\mathfrak{q}$ lying over $\mathfrak{p}$ in K, we have

$$e(\mathfrak{q}/\mathbb{Q}(\zeta_n)) = [\mathbb{Q}(\zeta') : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_m)] = \varphi(m),$$

so bounding with the fundamental identity gives

$$f(\mathfrak{q}/\mathbb{Q}) = f((\mathfrak{q} \cap \mathbb{Q}(\zeta_m))/\mathbb{Q}) = \operatorname{ord}_p(f)$$

by the special case above. ■

3.11.2 Totally Real Subfields

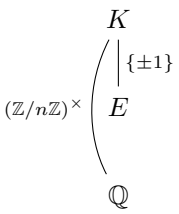
This is not in the book, but it should be fun. We have the following definition.

Here is the set-up. Fix n a positive integer, and fix $K := \mathbb{Q}(\zeta_n)$. Now, for each embedding $\tau : K \hookrightarrow \mathbb{C}$, there is an involution of K by

$$\tau^{-1} \circ (z \mapsto \overline{z}) \circ \tau.$$

Because complex conjugation is an automorphism this involution is actually independent of τ. (The main point here is that we may embed K into $\mathbb{C}$ however we please so that the exact choice of ζ_n is $\mathbb{Q}(\zeta_n)$.) Explicitly, $\tau : \zeta_n \mapsto \zeta_n^a$, but even still the involution takes $\zeta_n \mapsto \zeta_n^{-1}$ up in $\mathbb{C}$, which does not care for our exact choice of K or τ.

So complex conjugation is nicely canonical, and it corresponds to the element -1 in $(\mathbb{Z}/n\mathbb{Z})^\times$ of the Galois group. For $n > 2$, there is a (canonical!) subgroup $\{\pm 1\}$ of our Galois group of order 2, so taking the fixed field gives E where $[K : E] = 2$ and $[E : \mathbb{Q}] = \varphi(n)/2$. Here is the tower.



So we have the following definition.

Definition 3.96 (Totally real subfield)**.** Fix everything as above. Then E is called the *totally real subfield* of K.

We note that the unit groups of $\mathcal{O}_K^\times$ and $\mathcal{O}_E^\times$ have the same rank by checking Dirichlet's unit theorem, but they are not equal, for example, because $\zeta \in \mathcal{O}_K^\times \setminus \mathcal{O}_E^\times$.

3.11.3 Valuations

Let's return to the book. We have the following definition.

Definition 3.97 (p-adics)**.** We define

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^\bullet\mathbb{Z}$$

in the usual way as a limit of abelian groups where the maps $\mathbb{Z}/p^n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^m\mathbb{Z}$ be the standard projection for $n \geq m$ by $1 \mapsto 1$.

Remark 3.98. We note that $\mathbb{Z}_p$ is not $\mathbb{Z}/p\mathbb{Z}$, nor is it $\mathbb{Z}_{(p)}$.

It is not obvious, though it is true, that $\mathbb{Z}_p$ is a ring. As for why, we work in a little more generality.

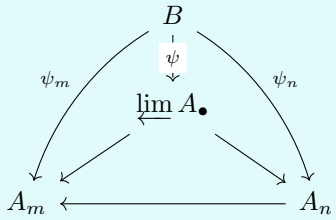
Proposition 3.99. Fix $\{A_k\}_{k\in\mathbb{N}}$ some sequence of groups (rings), and let $\varphi_k : A_k \to A_{k-1}$ be (ring) homomorphisms for each $k > 0$. Then

$$\varprojlim A_\bullet \subseteq \prod_{k\in\mathbb{N}} A_k$$

by

$$\varprojlim A_\bullet = \left\{ \{a_k\}_{k\in\mathbb{N}} \in \prod_{k\in\mathbb{N}} A_k : \varphi(a_k) = a_{k-1} \text{ for each } k > 0 \right\}.$$

And as usual, $\varprojlim A_\bullet$ satisfies the universal property of the limit: for each B with maps $\psi_\bullet : B \to A_\bullet$ commuting with the $\varphi_\bullet$, there is a unique map $\psi : B \to \varprojlim A_\bullet$ making the following diagram commute.



We won't show this here; this is more algebra than number theory.

Example 3.100. We can realize elements of $\mathbb{Z}_p$ as infinite tuples

$$\{a_k\}_{k\in\mathbb{Z}^+} \in \prod_{k\in\mathbb{Z}^+} \mathbb{Z}/p^k\mathbb{Z}$$

such that $a_{k+1} \equiv a_k \pmod{p^k}$ for each $k \in \mathbb{Z}^+$. For example $\{1234\}_{k\in\mathbb{Z}^+}$ is one such element, as is

$$\left\{0, \frac{p+1}{2}, \frac{p^2+1}{2}, \frac{p^3+1}{2}, \dots\right\}$$

for p odd. This last element corresponds to $1/2$.

Theme 4
Local Theory

4.1 October 22

The fun, as they say, never stops.

4.1.1 Talking $\mathbb{Z}_p$

Fix p a (nonzero) prime number. Last time we defined

$$\varprojlim \mathbb{Z}/p^\bullet\mathbb{Z} \subseteq \prod_{k\in\mathbb{N}} \mathbb{Z}/p^k\mathbb{Z}.$$

Namely, we can notate elements of $\mathbb{Z}_p$ by $(a_k)_{k\in\mathbb{N}}$, where $a_{k+1} \equiv a_k \pmod{p^k}$. Viewing $\mathbb{Z}_p$ as a product like this provides us with (surjective) morphisms

$$\pi_k : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^k\mathbb{Z}.$$

We can write this (purely formally) as

$$\alpha := b_0 + b_1 p + b_2 p^2 + \cdots$$

where the $b_\bullet \in \mathbb{Z}$. Here, we set $b_k := \frac{a_{k+1}-a_k}{p}$, where everything is viewed as an integer. (Nuekirch defines the p-adics using these formal power series.) We also note that, when $b_\bullet \in [0, p)$, this representation is unique.

Anyways, by the universal property, we note that the canonical surjections $\psi_k : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^k\mathbb{Z}$ (for each $k \in \mathbb{N}$) provide a unique ring homomorphism $\mathbb{Z} \to \mathbb{Z}_p$.[1] It turns out that this map $\mathbb{Z} \to \mathbb{Z}_p$ is injective: any integer in the kernel must be $0 \pmod{p^k}$ for each k, which forces the kernel to be zero. As such, we have that the map $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ lets us view $\mathbb{Z}$ as a subring of $\mathbb{Z}_p$.

We also remark that any element $a \in \mathbb{Z}_p$ is a unit when $a \not\equiv 0 \pmod{p}$ because in this case we can invert $a \pmod{p^k}$ for each $k \in \mathbb{N}$, letting us construct out inverse. As such, all elements of $\mathbb{Z} \setminus p\mathbb{Z}$ are units in $\mathbb{Z}_p$, which lets us extend $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ to the localization

$$\mathbb{Z}_{(p)} \to \mathbb{Z}_p$$

by the universal property. Recall that $\mathbb{Z}_{(p)}$ allows denominators outside of (p).

[1] We could note that $\mathbb{Z}$ is initial in ring here, but this does not give us the commutativity with the ψ_k.

4.1.2 Solutions in Modular Systems

Why do we care about $\mathbb{Z}_p$? Here are some reasons.

- $\mathbb{Z}_p$ and its specially its fraction field $\mathbb{Q}_p$ let us do analysis, for example by Newton's method/Hensel's lemma.
- Similarly, investigating how $\mathbb{Z}_p$ interact, we can study solutions to polynomial equations in generic modular systems.

Indeed, the second point is codified by the following.

Proposition 4.1. Fix F some polynomial in $\mathbb{Z}[x_1, \dots, x_k]$, and take m and n coprime positive integers. Then there is a canonical bijection between

$$\left\{x \in (\mathbb{Z}/mn\mathbb{Z})^k : F(x) = 0\right\} \leftrightarrow \left\{x \in (\mathbb{Z}/m\mathbb{Z})^k : F(x) = 0\right\} \times \left\{x \in (\mathbb{Z}/n\mathbb{Z})^\times : F(x) = 0\right\}.$$

Proof. Use the Chinese remainder theorem to construct the bijection. ■

Corollary 4.2. Fix F some polynomial in $\mathbb{Z}[x_1, \dots, x_k]$. Then F has solutions in every modulus if and only if it has solutions $\pmod{p^\nu}$ for each $\nu \in \mathbb{N}$.

Proof. If it has solutions $\pmod{p^\nu}$ for each $\nu \in \mathbb{N}$, then we can use the Chinese remainder theorem to get each $\pmod{m}$. The other direction is easier because $\pmod{p^\nu}$ is some modulus. ■

Proposition 4.3. Fix F some polynomial in $\mathbb{Z}[x_1, \dots, x_k]$. We have that $F(x) = 0$ has solutions in every modulus if and only if it has solutions in all $\mathbb{Z}_p^k$.

Proof. It suffices to show that F has a solution $\pmod{p^\nu}$ for each ν if and only if it has a solution in $\mathbb{Z}_p$. In one direction, if we have a solution in $(a_1, \dots, a_k) \in \mathbb{Z}_p^k$, then we can take

$$(a_1 \pmod{p^\nu}, a_2 \pmod{p^\nu}, \dots, a_k \pmod{p^\nu})$$

for our solution $\pmod{p^\nu}$.

The other direction is harder because generic solutions might not lift. For each $\nu \in \mathbb{N}$, set $\Sigma_\nu \subseteq (\mathbb{Z}/p^\nu\mathbb{Z})^k$ be the set of solutions $\pmod{p^\nu}$. By assumption, each $\Sigma_\bullet$ is nonempty. We also note that $\mu \geq \nu$ induces a map $\Sigma_\mu \to \Sigma_\nu$ by reduction. As such, we set

$$\Sigma'_\nu = \bigcap_{\mu \geq \nu} \operatorname{im}(\sigma_\mu \to \Sigma_\nu)$$

to be the set of elements in Σ_ν with lifts from each Σ_μ.

Now, the key trick is to see that Σ'_ν is nonempty because the $\operatorname{im}(\sigma_\mu \to \Sigma_\nu)$ is a decreasing sequence of nonempty subsets of $(\mathbb{Z}/p^\nu\mathbb{Z})^k$, so it must stabilize, and it cannot stabilize to a nonempty set because this would imply some Σ_μ is empty.

We also note that the restricted map $\Sigma'_\mu \to \Sigma_\nu$ will always go into Σ'_ν because anything with an infinite lift from Σ'_μ will have an infinite lift. Further, the map $\Sigma'_\mu \to \Sigma'_\nu$ will be surjective because anything with an infinite lift from Σ'_ν will induce an infinite lift from its lift in Σ'_μ.

So now we have a system of surjective maps

$$\cdots \twoheadrightarrow \Sigma'_3 \twoheadrightarrow \Sigma'_2 \twoheadrightarrow \Sigma'_1 \twoheadrightarrow \Sigma'_0,$$

and we can choose a commuting element from $\varprojlim \Sigma'_\bullet$, which is the needed solution in $\mathbb{Z}_p^k$. ■

Remark 4.4. We can also extend the above logic to work with finite systems of polynomial equations, at the cost of a minor headache.

4.1.3 Basic Properties of $\mathbb{Z}_p$

Let's run through some basic properties.

Proposition 4.5. We have that $\mathbb{Z}_p$ is an integral domain.

Proof. By our construction of $\mathbb{Z}_p$ as a limit object, we know that it is a ring with identity; and we know that it is nonzero because, say, it surjects onto $\mathbb{Z}/p\mathbb{Z}$.

So, of course, the hard part is showing that $\mathbb{Z}_p$ has no nontrivial zero-divisors. For this, we quickly recall that we have a valuation $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ given by

$$\nu_p(q) = \max\{a : p^a \mid q\}.$$

(We could also state this in terms of ideal factorizations, but we won't.) Now fix some $\alpha \in \mathbb{Z}_p$ with

$$\alpha = (a_0, a_1, \ldots),$$

and $a_\bullet \in \mathbb{Z}$ for each $a_\bullet$. If we force $a_\bullet \neq 0$ for each $a_\bullet$ (say, set it to $p^\bullet$ when necessary), then we see that $\alpha = 0$ if and only if the sequence $\nu_p(a_\bullet)$ is unbounded: if α is nonzero, then eventually one of the a_k will not be divisible by p^k, so each subsequent $a_\bullet$ will remain not divisible by p^k; conversely, if $\alpha = 0$, then $\nu_p(a_k) \geq k$ for each k, giving unboundedness.

We now attack zero-divisors directly. Suppose $\alpha\beta = 0$ for $\alpha = (a_0, a_1, \ldots) \in \mathbb{Z}_p$ and $\beta = (b_0, b_1, \ldots) \in \mathbb{Z}_p$, with $a_\bullet$ and $b_\bullet$ notated as above. Now, if $\alpha \neq 0$ and $\beta \neq 0$, then $\nu_p(a_\bullet)$ and $\nu_p(\bullet)$ are bounded, so

$$\nu_p(a_\bullet b_\bullet) = \nu_p(a_\bullet) + \nu_p(b_\bullet)$$

is also bounded, so $\alpha\beta = (a_0b_0, a_1b_1, \ldots)$ is nonzero. ∎

Proposition 4.6. We have that $\mathbb{Z}_p^\times = \pi_1^{-1}(\mathbb{F}_p^\times)$.

Proof. In one direction, the fact that π_1 is a ring homomorphism implies $\pi_1\left(\mathbb{Z}_p^\times\right) \subseteq \mathbb{F}_p^\times$.

In the other direction, suppose $\alpha = (a_0, a_1, \ldots)$ is in $\pi_1^{-1}\left(\mathbb{F}_p^\times\right)$ so that $p \nmid a_1$ and $p \nmid a_k$ for each $k \geq 1$. Thus, for each k, we may find $a_k^{-1} \in \mathbb{Z}/p^k\mathbb{Z}$, and these inverses will commute with each other to give

$$\beta = \left(a_0^{-1}, a_1^{-1}, \ldots\right) \in \mathbb{Z}_p.$$

Then we can compute that $\alpha\beta = (1, 1, \ldots) = 1 \in \mathbb{Z}_p$, so $\alpha \in \mathbb{Z}_p^\times$. ∎

Proposition 4.7. We have that $\mathbb{Z}_p$ is a discrete valuation ring.

Proof. Fix $\alpha \in \mathbb{Z}_p$ with $\alpha \neq 0$. Then we claim $\alpha = (p^\bullet)$ for some $p^\bullet$. Indeed, write $\alpha = (a_0, a_1, \ldots)$, and we see that $\nu_p(a_\bullet)$ is a bounded sequence. Let M be some bound, from which it follows $k, \ell \geq M$ has

$$\nu_p(a_k) = \nu_p(\ell)$$

because here $\nu_p(a_k)$ can only be modified by a power of p^k and therefore cannot change, lest it jump above M. In particular, our sequence eventually stabilizes, so we set m to this limit so that

$$p^{\min\{m,n\}} \mid a_n$$

for each $n \in \mathbb{N}$, even for small n because there we must have $0 \pmod{p^n}$. Then we can set

$$\beta = (a_m/p^m, a_{m+1}/p^m, \ldots) \in \mathbb{Z}_p,$$

eh

with $p^m\beta = \alpha$. We also note that $p \nmid a_m/p^m$ lest we have higher powers later, so β is in fact a unit, so it follows $(\alpha) = (p^m)$, which finishes this claim.

With this in mind, we define $\nu_p(\alpha)$ equal to the integer such that $(\alpha) = \left(p^{\nu_p(\alpha)}\right)$. Now, to get a discrete valuation ring, we note that all nonzero ideals I, set m to the minimum of $\nu_p(\alpha)$ for each $\alpha \in I$, and then we have that

$$I = \bigcup_{\alpha \in I} (\alpha) = \bigcup_{\alpha \in I} \left(p^{\nu_p(\alpha)}\right) = (p^m),$$

so indeed, all ideals of $\mathbb{Z}_p$ are principal. We also note that $\mathbb{Z}_p^\times = \pi_1^{-1}(\mathbb{F}_p^\times) = \mathbb{Z}_p \setminus p\mathbb{Z}_p$ shows that $\mathbb{Z}_p$ is local. We also note $\mathbb{Z}_p$ is not a field because $p\mathbb{Z}_p$ are not units. Thus, we may conclude that $\mathbb{Z}_p$ is a discrete valuation ring. ■

4.2 October 25

So we're still talking about localization.

4.2.1 p-adic Absolute Value

For $a \in \mathbb{Q}^\times$, recall that we define $\nu_p(a)$ equal to the exponent of the prime ideal (p) in the (ideal!) prime factorization of the fractional ideal (a). More concretely, if $a = p^m \cdot \frac{b}{c}$ with $p \nmid b, c$, then $\nu_p(a) = m$. With this in mind, we see that

$$\mathbb{Z}_{(p)} = \left\{a \in \mathbb{Q}^\times : \nu_p(a) \geq 0\right\}.$$

In particular,

$$\nu_p : \mathbb{Q}^\times \to \mathbb{Z}$$

is a surjective homomorphism.

By definition, we will often let $\nu_p(0) = +\infty$ so that $\mathbb{Z}_{(p)}$ becomes a discrete valuation ring, where ν_p is our valuation. We have the following basic properties to check about being a valuation.

Proposition 4.8. Fix p prime and $a, b \in \mathbb{Q}$. Then the following are true.

(a) $\nu_p(a) = +\infty$ if and only if $a = 0$.

(b) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

(c) $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$.

Proof. Some of these follow from the above discussion; the rest are exercises. ■

Remark 4.9. The above arguments work for a general prime $\mathfrak{p}$ of a Dedekind ring.

The point of Proposition 4.8 is that we may define the following.

Definition 4.10 (p-adic absolute value)**.** We define the *p-adic absolute value* for $a \in \mathbb{Q}$ by

$$|a|_p := p^{-\nu_p(a)}.$$

We will also let $|\cdot|_\infty$ be the usual absolute value on $\mathbb{Q}$.

Using Proposition 4.8, we have the following.

Corollary 4.11. For $a, b \in \mathbb{Q}$ and p prime, the following are true.

(a) $|a|_p \geq 0$ with equality if and only if $a = 0$.

(b) $|ab|_p = |a|_p \cdot |b|_p$.

(c) $|a+b|_p \leq \max\{|a|_p, |b|_p\}$.

Proof. These follow directly from Proposition 4.8. ∎

We also have the following cute result.

Proposition 4.12. All triangles in $\mathbb{Q}$ with metric given by $|\cdot|_p$ are isosceles.

Proof. Fix vertices $a, b, c \in \mathbb{Q}$ so that we want to show that two of

$$|a-b|_p, \qquad |b-c|_p, \qquad |c-a|_p$$

are equal. Well, suppose for the sake of contradiction these are unequal, and set $x := |a-b|_p$ to be the largest; then set $y := b - c$. We note also that $|\pm 1|_p = 1$ because $|\pm 1|_p \cdot |\pm 1|_p = |\pm 1|_p$, so it follows $|-b|_p < |a|_p$. Thus,

$$|x|_p = |(x+y)+(-y)|_p \leq \max\{|x+y|_p, |-y|_p\} < |x|_p,$$

which is our contradiction. ∎

Here is an important result on our valuations.

Theorem 4.13 (Product formula on $\mathbb{Q}$)**.** Fix $\alpha \in \mathbb{Q}^\times$. Then $|\alpha|_p = 1$ for all but finitely many $p \in \{\infty\} \cup \{\text{primes}\}$, and

$$\prod_{p \in \{\infty\} \cup \{\text{primes}\}} |\alpha|_p.$$

Proof. Letting $\alpha = \frac{n}{m}$ with $n, m \in \mathbb{Z} \setminus \{0\}$, we note that $p \nmid n, m$ implies that $\alpha = p^0 \cdot \frac{n}{m}$ with $p \nmid n, m$, so it follows that $\nu_p(\alpha) = 0$, so $|\alpha|_p = 1$.

To show the product formula, we note that multiplicativity of $|\cdot|_p$ implies that it suffices to show the formula for $\alpha \in \{-1\} \cup \{\text{primes}\}$. Well, if $\alpha = -1$, then $|\alpha|_p = 1$ for each p. Otherwise, if $\alpha = \ell$ is some prime, then we see that

$$|\alpha|_p = \begin{cases} \ell & \text{if } p = \infty, \\ 1/\ell & \text{if } p = \ell, \\ 1 & \text{otherwise,} \end{cases}$$

where the last follows from writing $\ell = p^0 \cdot \frac{\ell}{1}$. Multiplying over the primes finishes the proof. ∎

4.2.2 Function Field Analogy

Fix k an algebraically closed field, take $A := k[x]$ the polynomial ring and $K := k(x)$ its field of fractions. Then we recall from a course in commutative algebra that the maximal ideals of A all look like

$$(x - \alpha)$$

for some $\alpha \in k$, which follows from k being algebraically closed.

Now, it is true that A is a Dedekind ring. To try to tell the story above, we let $f \in k(x)^\times$ and define

$$\operatorname{ord}_{(x-\alpha)}(f) := \text{order of vanishing of } f \text{ at } \alpha,$$

for each maximal ideal $(x-\alpha)$. We also need to deal with an "infinite prime," which is

$$\operatorname{ord}_\infty(f) := \deg f,$$

for $f \in k(x)^\times$, where $\deg f := \deg g - \deg h$ when $f = g/h$ for some $g, h \in k[x]$. Also, we will by convention take

$$\operatorname{ord}_\mathfrak{p}(0) := +\infty$$

for each $\mathfrak{p}$ described above (either ∞ or $(x-\alpha)$).

For notational convenience, we define

$$M_K := \{\infty\} \cup \{(x-\alpha) : \alpha \in k\},$$

which is the set of places of K. Then we have the following mirror of Proposition 4.8.

Proposition 4.14. We have the following, for $\mathfrak{p} \in M_K$ and $f, g \in k(x)$.

(a) $\operatorname{ord}_\mathfrak{p}(f) \in \mathbb{Z} \cup \{\infty\}$, where $\operatorname{ord}_\mathfrak{p}(f) = \infty$ if and only if $f = 0$.

(b) $\operatorname{ord}_\mathfrak{p}(fg) = \operatorname{ord}_\mathfrak{p}(f) + \operatorname{ord}_\mathfrak{p}(g)$.

(c) $\operatorname{ord}_\mathfrak{p}(f+g) \geq \min\{\operatorname{ord}_\mathfrak{p}(f), \operatorname{ord}_\mathfrak{p}(g)\}$.

Proof. Omitted as an exercise I guess. ∎

Now, for some fixed $c > 1$, we define

$$|f|_\mathfrak{p} := c^{-\operatorname{ord}_\mathfrak{p}(f)}.$$

This turns into the following statement.

Corollary 4.15. We have the following,f or $\mathfrak{p} \in M_K$ and $f, g \in k(x)$.

(a) $|f|_p \geq 0$ with equality if and only if $f = 0$.

(b) $|fg|_\mathfrak{p} = |f|_\mathfrak{p} \cdot |g|_\mathfrak{p}$.

(c) $|f+g|_\mathfrak{p} \leq \max\{|f|_\mathfrak{p}, |g|_\mathfrak{p}\}$.

Proof. These follow from plugging in our definition of $|\cdot|_\mathfrak{p}$ into Proposition 4.14. ∎

We seem to be getting this structure a lot. Let's abstract it.

Definition 4.16 (Non-archimedean absolute value)**.** A *non-archimedean absolute value* on a ring R is a function $|\cdot| : R \to \mathbb{R} \cup \{\infty\}$ satisfying the following for $x, y \in R$.

1. $|x| \geq 0$ with equality if and only if $x = 0$.
2. $|xy| = |x| \cdot |y|$.
3. $|x+y| \leq \max\{|x|, |y|\}$.

Remark 4.17. The "non-archimedean" adjective means that the size $|n|$ of various $n \in \mathbb{Z}$ is bounded above. This is not true for the standard valuation on $\mathbb{Q}$, for example.

It turns out that we also have a product formula for K.

Theorem 4.18 (Product formula for K)**.** For each $f \in k(x)^\times$, then $|f|_\mathfrak{p} = 1$ for each $\mathfrak{p} \in M_K$. Then

$$\prod_{\mathfrak{p} \in M_K} |f|_\mathfrak{p} = 1.$$

Proof. This is similar to the proof in $\mathbb{Q}$ and hence omitted. ■

Example 4.19. With $k = \mathbb{C}$, we have that K is the field of all meromorphic functions on the Riemann sphere, $\mathbb{C} \cup \{\infty\}$. Also note that $\mathbb{C} \cup \{\infty\}$ is in bijection with our elements of M_K, where $\operatorname{ord}_\mathfrak{p}(f) = \operatorname{ord}_c(f)$, where $\mathfrak{p} = (x-c)$, where c is allowed to be ∞. Here the product formula turns into the statement

$$\sum_{z \in \mathbb{C} \cup \{\infty\}} \operatorname{ord}_z(f) = 0.$$

4.2.3 Constructing Local Completions

Fix A a Dedekind ring with K its field of fractions, as usual. Then we set $\mathfrak{p}$ to be a nonzero prime A-ideal. For each $f \in K$, we may define

$$\nu_\mathfrak{p}(f) = \operatorname{ord}_\mathfrak{p}(f)$$

to be the exponent of $\mathfrak{p}$ in the prime factorization of (f). As usual, we have the following statement.

Proposition 4.20. We have the following, for $\mathfrak{p}$ a prime ideal and $f, g \in K$.

(a) $\nu_\mathfrak{p}(f) \in \mathbb{Z} \cup \{\infty\}$, where $\nu_\mathfrak{p}(f) = \infty$ if and only if $f = 0$.

(b) $\nu_\mathfrak{p}(fg) = \nu_\mathfrak{p}(f) + \nu_\mathfrak{p}(g)$.

(c) $\nu_\mathfrak{p}(f+g) \geq \min\{\nu_\mathfrak{p}(f), \nu_\mathfrak{p}(g)\}$.

Proof. Omitted, as usual. ■

Then we can set $c > 1$ some real number and define

$$|f|_\mathfrak{p} := c^{-\nu_\mathfrak{p}(f)}.$$

So we get the following corollary, as usual.

Corollary 4.21. We have that $|\cdot|_\mathfrak{p}$ is a non-archimedean absolute value on K.

Proof. This follows from running through the checks on Proposition 4.20. ■

The notion of "archimedean" makes us think about distances, so we note that it is true that

$$d(f,g) := |f-g|_\mathfrak{p}$$

does turn K into a metric space.

Warning 4.22. For the rest of this discussion, fix $\mathfrak{p}$ and work with $|\cdot| := |\cdot|_\mathfrak{p}$.

More generally, the conditions we need to get a metric space are as follows.

Definition 4.23 (Absolute value)**.** An *absolute value* on a ring R is a function $|\cdot| : R \to \mathbb{R}$ that satisfy the following for $x, y \in R$.

(a) $|x| \geq 0$ with equality if and only if $x = 0$.

(b) $|xy| = |x| \cdot |y|$.

(c) $|x + y| \leq |x| + |y|$.

Then we say that $|\cdot|$ is *non-archimedean* if we satisfy $|x+y| \leq \max\{|x|, |y|\}$ and *archimedean* otherwise.

It is not too hard to check that

$$d(x, y) := |x - y|$$

does induce a metric on R as described above. The main point is that the triangle inequality for d comes from $|x + y| \leq |x| + |y|$.

We also have the following definition to talk about the underlying algebraic structure.

Definition 4.24 (Valued rings, fields)**.** A *valued ring* consists of the data a ring R as well as a valuation $|\cdot|$ on R. A *valued field* is a valued ring where the underlying ring R is a field. Then a valued ring/field is a *non-archimedean* valued ring/field if and only if the underlying valuation is non-archimedean.

Definition 4.25 (Complete valued rings, fields)**.** A valued ring/field is *complete* if and only if it is complete with respect to the distance metric induced by the underlying valuation.

We close by picking up the following definition and theorem.

Definition 4.26 (Morphisms of valued rings)**.** A *morphism* $\varphi : (R, |\cdot|) \to (R', |\cdot|')$ of valued rings is a ring homomorphism $R \to R'$ such that $|r| = |\varphi(r)|'$ for each $r \in R$. This morphism φ is an *embedding* if φ is injective.

Theorem 4.27. Every nontrivial valued ring $(R, |\cdot|)$ can be embedded into a complete valued ring $(R', |\cdot|')$, where R embeds as a dense subset. This embedding is unique up to unique isomorphism. In fact, if R is a field, then R' is also a field.

We'll prove this next time.

4.3 October 27

Here we go.

4.3.1 Metric Completions

We recall we had the following theorem.

Theorem 4.28. Every nontrivial valued ring $(R, |\cdot|)$ can be embedded as a dense subring into of a complete valued ring $(\hat{R}, |\cdot|^\wedge)$, and the latter is unique up to unique isomorphism over R. If R is a field (archimedean) (non-archimedean), then $\hat{R}$ is also a field (archimedean) (non-archimedean).

Proof. Set $R_0 := R^{\mathbb{N}}$ the space of $\mathbb{N}$-indexed sequences of elements of R. Further, let $R_1 \subseteq R_0$ be the subset consisting of the Cauchy sequences. We do the Cauchy sequence construction of $\hat{R}$; we have the following.

Lemma 4.29. We have that R_1 is a subring of R_0.

Proof. We have the following checks.

- We have the identity because $1 = (1, 1, \ldots)$ is constant and hence Cauchy, so $1 \in R_1$.
- We see R_1 is an additive subgroup by adding/subtracting the two Cauchy sequences termwise.
- We have that R_1 is closed under multiplication by multiplying the two Cauchy sequences termwise. Namely, if $\{a_k\}_{k\in\mathbb{N}}, \{b_k\}_{k\in\mathbb{N}} \in R_1$, then

$$|a_n b_n - a_m b_m| \le |a_n| \cdot |b_m - b_n| + |b_m| \cdot |a_m - a_n|$$

by the triangle inequality. The $|a_\bullet|$ and $|b_\bullet|$ are bounded because the sequence is Cauchy, so the above implies our sequence is Cauchy. ■

Lemma 4.30. Fix $\mathfrak{q} := \{(a_n) \in R_1 : |a_n| \to 0\}$. Then $\mathfrak{q}$ is a prime R-ideal.

Proof. The fact that this is an additive subgroup follows by writing out what we need and then doing 104-type arguments. This is an ideal because $a \in \mathfrak{q}$ and $b \in R$ will have $ab \in \mathfrak{q}$ because the sequence b will be bounded.

Lastly, $\mathfrak{q}$ is prime because $1 \notin \mathfrak{q}$ (because $|1| \to 1$), and if $(a_n), (b_n) \notin \mathfrak{q}$, then these are Cauchy sequences and so $|a_\bullet|$ and $|b_\bullet|$ will converge in $\mathbb{R}$, which must converge to some nonzero value. It follows that $|a_\bullet b_\bullet|$ will also converge to a nonzero value, so $(a_n b_n) \notin \mathfrak{q}$ as well. ■

We now set $\hat{R} := R_1/\mathfrak{q}$, and we see that this is entire by the above; it might feel amazing that this means R is entire as well, but this essentially follows from being valued.

To be explicit, we note that each $a, b = (a_n) \in R_1$ must have $\lim_{n\to\infty} |a_n|$ convergent and finite, and similar for b. Then if we suppose $a - b \in \mathfrak{q}$, then we can see that

$$\lim_{n\to\infty} |a_n| = \lim_{n\to\infty} |b_n|,$$

so we may take this limit as our definition of $|\cdot|^\wedge : \hat{R} \to \mathbb{R}$. We can check that this is an absolute value on $\hat{R}$, which we will not show explicitly here because it should mostly be a matter of writing out the checks.

We note that we have the mapping $R \to R_0$ by taking $r \mapsto (r, r, \ldots)$. We can see that this is a ring homomorphism and with image contained in R_1 because constant sequences are Cauchy. So we have a map

$$R \hookrightarrow R_1.$$

Moreover, we can see that the only way for the absolute value to go to 0 is for $|r| = 0$ which is equivalent to $r = 0$, so the pre-image of $\mathfrak{q}$ under this embedding is 0. So we have an induced injective map

$$\iota : R \hookrightarrow \hat{R}.$$

We also note that $|\iota(r)|^\wedge = |r|$, so this is indeed a morphism of valued rings. This lets us view $(R, |\cdot|)$ as a valued subring of $\hat{R}$.

it is? This embedding is dense somewhat clearly, and it is is unique up to unique isomorphism, which we leave as an exercise.[2] Similarly, the last claims about $\hat{R}$ preserving structure for R we leave as an exercise, though we outline them below.

- If R is a field, then we can take the Cauchy sequence in $\hat{R}$ termwise inverting.
- If R is archimedean, then this is equivalent to the statement that $\{|n| : n \in \mathbb{N}\}$ is unbounded in R, so this will also be true in $\hat{R}$.

[2] One way to do this would be universal property for $R \mapsto \hat{R}$.

- If R is non-archimedean, then this is equivalent to the statement that $\{|n| : n \in \mathbb{N}\}$ is bounded in R, so this will also be true in $\hat{R}$. ■

As an aside, we mention the following categorical result.

Proposition 4.31. Fix $(R, |\cdot|)$ and $(S, |\cdot|)$ with a morphism $\varphi : R \to S$ between them. Then the following diagram commutes.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow & & \downarrow \\ \hat{R} & \xrightarrow{\hat{\varphi}} & \hat{S} \end{array}$$

Here, $\hat{\varphi}$ is induced pointwise.

Proof. One can show this by hand using our construction of $\hat{R}$ and $\hat{S}$. ■

Let's now specialize to Dedekind rings.

Proposition 4.32. Fix A a Dedekind ring with K its fraction field. Fix $\mathfrak{p}$ a nonzero prime of A, and let $\nu_{\mathfrak{p}} : K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation of $\mathfrak{p}$. Further fix $c > 1$ and define

$$|x|_{\mathfrak{p}} := c^{-\nu_{\mathfrak{p}}(x)},$$

where $x \in K$. If we complete $(A, |\cdot|_{\mathfrak{p}})$ and $(K, |\cdot|_{\mathfrak{p}})$ to $(\hat{A}, |\cdot|_{\mathfrak{p}}^{\wedge})$ and $(K, |\cdot|_{\mathfrak{p}}^{\wedge})$ respectively, then we have the following.

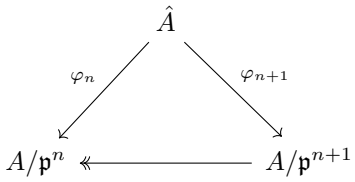
(a) There is a canonical isomorphism
$$\hat{A} \cong \varprojlim A/\mathfrak{p}^{\bullet}.$$

(b) $\hat{A}$ is a discrete valuation ring with valuation $-\log_c |\cdot|_{\mathfrak{p}}^{\wedge}$ and fraction field $\hat{K}$.

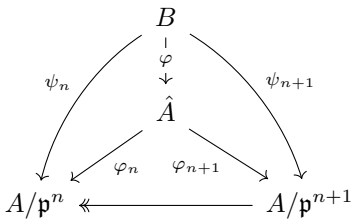
Proof. We do these one at a time.

(a) Fix $n \in \mathbb{N}$. We define $\varphi_n : \hat{A} \to A/\mathfrak{p}^n$. Here, take $\alpha \in \hat{A}$ represented by the Cauchy sequence $(a_0, a_1, \ldots)$, and we note that the Cauchy condition implies there is N such that $|a_k - a_\ell| \le c^{-n}$ for each $k, \ell \ge N$, which implies that $a_k - a_\ell \in \mathfrak{p}^n$, so
$$a_k \equiv a_\ell \pmod{\mathfrak{p}^k}$$
for each $k, \ell \ge N$. In particular, $a_k \pmod{\mathfrak{p}^n}$ has stabilized past N, so we define
$$\varphi_n(\alpha) := [a_k]_{\mathfrak{p}^n}.$$
We note that φ_n is well-defined: the exact lifting does not matter because a different Cauchy sequence $(a_0', a_1', \ldots)$ will also eventually stabilize $\pmod{\mathfrak{p}^n}$ past (say) N', but because the two sequences converge to the same α, we eventually have
$$|a_k - a_k'| \le c^{-n}$$
for sufficiently large k. But now $a_k \equiv a_k' \pmod{\mathfrak{p}^n}$ for sufficiently large n, which is what we wanted.

We now note that φ_n is a ring homomorphism by the "look at it" test, and we also see that the following diagram commutes for a similar reason.



It remains to show that $\hat{A}$ equipped with these morphisms satisfies the universal property. So fix a ring B with maps $\psi_n : B \to A/\mathfrak{p}^n$ making the following diagram commute.



We need to induce φ uniquely. Well, for $b \in B$, we choose $a_n \in A$ to be any lift for $\psi_n(b) \in A/\mathfrak{p}^n$ to make some $(a_0, a_1, \ldots) \in A^{\mathbb{N}}$. We can see that this is a Cauchy sequence because

$$a_{n+1} \equiv a_n \pmod{\mathfrak{p}^n}$$

always, so $a_n - a_m \in \mathfrak{p}^{\min\{n,m\}}$, implying that $n, m \to \infty$ sends the absolute value of the difference to zero. We also note that if chose another lift $(a_0', a_1', \ldots) \in A_0$, then we would have $a_k - a_k' \in \mathfrak{p}^k$ for each k, so $|a_k - a_k'| \to 0$, implying that the output of f_0 is unique up to coset of $\mathfrak{q}$. Thus, we have described a well-defined map

$$\psi : B \to \hat{A}.$$

By construction, we can also check that $\varphi_n(\alpha) = \psi_n(b)$ for each n, which we will not show explicitly here; this also shows that ψ taking $b \mapsto \alpha$ is a ring homomorphism for free, and we will leave the uniqueness of ψ as an exercise. This completes the proof of (a). ■

We'll get to (b) next class.

4.4 October 29

Ok so my keyboard is now working.

4.4.1 Completions of Dedekind Domains

Recall from last time we had the following statement.

Proposition 4.33. Fix A a Dedekind ring with K its fraction field. Fix $\mathfrak{p}$ a nonzero prime of A, and let $\nu_{\mathfrak{p}} : K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation of $\mathfrak{p}$. Further fix $c > 1$ and define

$$|x|_{\mathfrak{p}} := c^{-\nu_{\mathfrak{p}}(x)},$$

where $x \in K$. If we complete $(A, |\cdot|_{\mathfrak{p}})$ and $(K, |\cdot|_{\mathfrak{p}})$ to $(\hat{A}, |\cdot|_{\mathfrak{p}}^{\wedge})$ and $(K, |\cdot|_{\mathfrak{p}}^{\wedge})$ respectively, then we have the following.

(a) There is a canonical isomorphism
$$\hat{A} \cong \varprojlim A/\mathfrak{p}^{\bullet}.$$

(b) $\hat{A}$ is a discrete valuation ring with valuation $-\log_c |\cdot|_{\mathfrak{p}}^{\wedge}$ and fraction field $\hat{K}$.

Proof. We are showing part (b) now. We will now write $|\cdot|$ for all of our valuations because they extend properly. We have the following claims.

Lemma 4.34. For any non-archimedean valued ring $(R, |\cdot|)$, we have that $\{|\alpha| : \alpha \in \hat{R}\} = \{|\alpha| : \alpha \in R\}$.

Proof. Note that R embeds into $\hat{R}$, so of course we get $\supseteq$. For $\subseteq$, we suppose that we have a Cauchy sequence $(a_0, a_1, \ldots)$ approaching some α. Then there exists N for which

$$|a_i - a_j| < \alpha$$

for each $i, j \geq N$ because $\alpha \neq 0$. But then this implies that $|\alpha| = |a_i|$ for each $i \geq N$, so it follows that $|\alpha| \in \{|a| : a \in R\}$. ■

Lemma 4.35. Fix everything as above The function $\nu : \alpha \mapsto -\log_c |\alpha|$ is a discrete valuation on $\hat{K}$.

Proof. The fact that $\nu(x+y) = \nu(x) + \nu(y)$ follows from the multiplicativity of absolute values. We also have tht the range of $|\cdot|$ on $\hat{K}$ is its range on K from the previous claim. We leave the check of the strong triangle inequality as an exercise. ■

Lemma 4.36. Fix everything as above. Then the valuation ring of ν is $\hat{A}$.

Proof. We see that $\hat{A}$ is in the valuation ring because the image of $\hat{A}$ under $|\cdot|$ is the image of A, so indeed, $\hat{A}$ has nonnegative valuation.

In the other direction, suppose that $\alpha \in \hat{K}$ has $\nu(\alpha) \geq 0$ so that $|\alpha| \leq 1$. Then we can make α into a Cauchy sequence $(a_0, a_1, \ldots)$ in K, and now we take N as we did before so that $i \geq N$ implies $|a_i| = |\alpha|$. The point is that

$$|a_i| = |\alpha| \leq 1$$

for each $i \geq N$, which means that the $a_i \in A_{\mathfrak{p}}$, so we may represent α by the Cauchy sequence

$$(a_N, a_{N+1}, a_{N+2}, \ldots) \in \varprojlim A_{\mathfrak{p}}/(\mathfrak{p}A\mathfrak{p})^{\bullet} = \varprojlim A/\mathfrak{p}^{\bullet} = \hat{A}.$$

The middle equality deserves some explanation: we have that $A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^{\bullet} = (A \setminus \mathfrak{p})^{-1}(A/\mathfrak{p}^{\bullet})$, but the $A \setminus \mathfrak{p}$ will add no new units to $A/\mathfrak{p}^{\bullet}$, so it is simply $A/\mathfrak{p}^{\bullet}$. ■

Remark 4.37. Alternatively, we could have noted that $A_{\mathfrak{p}}$ injects into $\hat{A}$ so that α living in the completion of $A_{\mathfrak{p}}$ makes α live in $\hat{A}$.

We finish by noting that it follows $\hat{A}$ is a discrete valuation ring because it is a valuation ring of the discrete valuation ν. This finishes the proof. ■

We note that from the above we get that $\hat{K}$ is the fraction field of $\hat{A}$, and we are granted the unique maximal ideal

$$\hat{m} := \{\alpha \in \hat{A} : \nu(\alpha) \geq 1\}.$$

In fact, we can note that some $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ will give $\hat{m} = \pi\hat{A}$, where

$$A/\mathfrak{p}^{\bullet} \to \hat{A}/(\pi^{\bullet}) = \hat{A}/\hat{m}^{\bullet}$$

wut

is an isomorphism. This more or less follows from our argument earlier for Lemma 4.36.

Example 4.38. Fix k a field and $A = k[x]$ with $K = k(x)$ and $\mathfrak{p} = (x)$. Then $\hat{A} = k[[x]]$ and $\hat{K} = k((x))$.

We also remark that, in general,

$$\hat{K} = \bigcup_{n \geq 0} \pi^{-n}\hat{A}$$

for any Dedekind domain A.

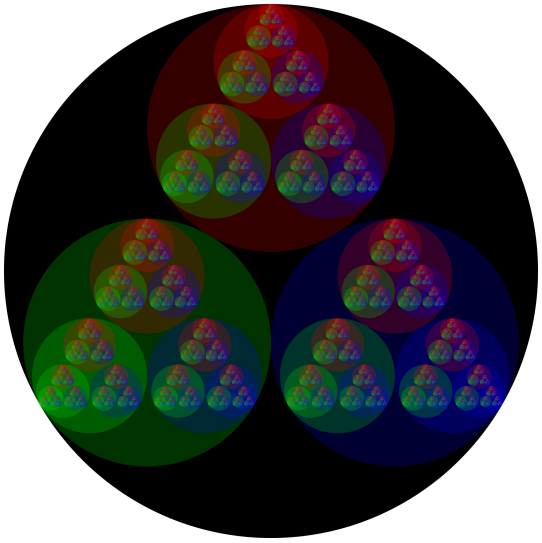
4.4.2 Topological Remarks

We note that if k is infinite, then $k[[x]]$ is not compact (sadly):

$$\{c + (x) : c \in k\}$$

is a disjoint open cover of $k[[x]]$. But $\mathbb{Z}_p$ is compact, as will be shown in the homework.

As an image, we can see $\mathbb{Z}_3$ as follows.



Each circle here corresponds to successively smaller residue classes. More generally, $\hat{A}$ where A is non-archimedean will make $\hat{A}$ totally disconnected.

As an aside, we note that we can let k be an arbitrary field, not necessarily algebraically closed. Then with $A = k[x]$, we have that the set of nonzero of nonzero prime ideals of A is in bijection with the monic irreducible ideals of $k[x]$ by $\pi \mapsto (\pi)$. Then if we let

$$M_k = \{\infty\} \cup \{(\pi) : \pi \in k[x] \text{ irred.}\},$$

we get a $|\cdot|_\nu$ for each place $\nu \in M_K$, induced by $|x|_\mathfrak{p} := c^{-(\deg f)\nu_\mathfrak{p}(x)}$ for some $c > 1$. Then we have the product formula given by

$$\prod_{\mathfrak{p} \in M_K} |x|_\mathfrak{p} = 1$$

for each $x \in k(x)^\times$. Again, this is essentially by unique prime factorization.

4.4.3 Valuations

Yes, we have been talking about valuations already. Let's talk some more.

Definition 4.39 (Trivial)**.** An absolute value $|\cdot|$ is *trivial* if and only if $|x| = 1$ for each $x \in R \setminus \{0\}$ and nontrivial otherwise.

Remark 4.40. The trivial valuation is non-archimedean: it corresponds with the valuation sending everything nonzero to 0.

The trivial absolute value is a perfectly fine valuation, but we don't want to have to care about it.

We have the following.

Proposition 4.41. Fix $(R, |\cdot|)$ a valued ring. Then the following are equivalent.

(a) R is non-archimedean.

(b) $|n| \le 1$ for each $N \in \mathbb{Z}$.

(c) $\{|n| : n \in \mathbb{Z}\}$ is a bounded set.

Proof. We show our implications one at a time.

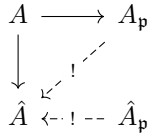
- We get that (a) implies (b) by an induction. If $R = \{0\}$, then this is free; otherwise, $|1| = 1$ and then, for $n \in \mathbb{N}$,
$$|\pm n| = |n| = |\underbrace{1 + \cdots + 1}_{n}| \le \max\{\underbrace{|1|, \ldots, |1|}_{n}\} = 1$$
by the strong triangle inequality.
- We see that (b) implies (c) by definition of bounded.
- We see that (c) implies (a): suppose that $|n| \le L$ for each $n \in \mathbb{Z}$. Then, taking any $x, y \in R$, we find that
$$|x+y|^n = \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \le \sum_{k=0}^{n} \left|\binom{n}{k}\right| \cdot \max\{|x|, |y|\}^n \le (n+1)L \max\{|x|, |y|\}^n.$$
In particular, we see that
$$|x+y| \le \sqrt[n]{(n+1)L} \cdot \max\{|x|, |y|\},$$
so it follows that
$$|x+y| \le \max\{|x|, |y|\} \cdot \limsup_{n\to\infty} \sqrt[n]{(n+1)L} = \max\{|x|, |y|\},$$
which is what we wanted. ∎

4.5 November 1

It is finally November.

4.5.1 Quick Remark

We quickly remark from last time that, given A a Dedekind ring with $\mathfrak{p}$ a nonzero prime, then the canonical map $A \hookrightarrow \hat{A}$ into the metric completion, this will factor uniquely through the map to the local ring, as per the following diagram.



Namely, we have a canonical morphism $\hat{A}_{\mathfrak{p}} \to \hat{A}$ by the universal property.

4.5.2 Equivalent Absolute Values

We have the following definition. Recall that absolute values induce a distance metric and hence a topology. So we have the following notion.

Definition 4.42 (Equivalent)**.** Fix K a field. Two absolute values $|\cdot|$ and $|\cdot|'$ on K are *equivalent* if they induce the same topology on K.

We have the following lemma.

Lemma 4.43. Fix $|\cdot|_1$ and $|\cdot|_2$ nontrivial absolute values on K. Then if

$$\{x \in K : |x|_1 < 1\} \subseteq \{x \in K : |x|_2 < 1\},$$

then there is $s \in \mathbb{R}^+$ such that $|x|_1 = |x|_2^s$.

Proof. Certainly we get this for $x = 0$, where any s will suffice. Otherwise, find some $x \in K$ with $|x|_1 < 1$, which exists because $|\cdot|_1$ is nontrivial, so there is a nonzero element with absolute value not 1, and we can take reciprocals to get our element of absolute value less than 1. We note that $|x|_2 < 1$ as well by hypothesis.

The point of this x is to induce our s by writing

$$s := \frac{-\log |x|_1}{-\log |x|_2}.$$

In particular, by construction $s > 0$ and $|x|_1 = |x|_2^s$. Now, for any other $y \in K^\times$, we note that all $n, m \in \mathbb{Z}$ with $m > 0$ have

$$\left|\frac{x^n}{y^m}\right|_\bullet < 1$$

is equivalent to

$$n \log |x|_\bullet - m \log |y|_\bullet < 0,$$

is equivalent to

$$\frac{n}{m} > \frac{-\log |y|_\bullet}{-\log |x|_\bullet},$$

for either absolute value. Thus, it follows that

$$\frac{-\log |y|_1}{-\log |x| < 1} < \frac{n}{m} \implies \frac{-\log |y|_2}{-\log |x|_2} < \frac{n}{m}$$

by hypothesis on our valuations, so we see that

$$\frac{-\log |y|_1}{-\log |x| < 1} \le \frac{-\log |y|_2}{-\log |x|_2},$$

and taking ratios tells us that $-\log |y|_2 \le \frac{1}{s}(-\log |y|_1)$, so we get $|y|_2 \le |y|_1^s$. Running the same argument through with $1/y$ tells us that $|y|_1 \le |y|_2^s$, so we get the equality here. ∎

Remark 4.44. Note that the conclusion is symmetric even though the hypothesis is asymmetric.

The main result is as follows.

Proposition 4.45. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there is $s \in \mathbb{R}^+$ such that $|\cdot|_1 = |\cdot|_2^s$.

Proof. To start, the absolute value is trivial if and only if it induces the discrete topology on K, which we won't show in detail here. The forward direction is essentially because our distance are always 1, and the backwards direction is because nontrivial valuations will have a nontrivial ball somewhere.

So now take $|\cdot|_1$ and $|\cdot|_2$ nontrivial. Now, if $|\cdot|_1 = |\cdot|_2^s$ for $s \in \mathbb{R}^+$, then of course our balls are the same by some topological open ball argument. Conversely, if $|\cdot|_1$ and $|\cdot|_2$ are equivalent, then we note that $x^n \to 0$ as $n \to \infty$ is equivalent to $|x| < 1$, so

$$\{x \in K : |x|_1 < 1\} = \{x \in K : x^n \to 0\} = \{x : |x|_2 < 1\}$$

because approaching zero is a purely topological concept (!). Now we are able to finish by Lemma 4.43. ■

We also have the following corollary.

Corollary 4.46. Fix $|\cdot|_1$ and $|\cdot|_2$ are absolute values. Then if $|\cdot|_1$ is nontrivial and

$$\{x \in K : |x|_1 < 1\} \subseteq \{x \in K : |x|_2 < 1\},$$

then our absolute values are equivalent.

Proof. This follows from the proof of the previous proposition. ■

4.5.3 Theorems on Valuations

Our notion of equivalence is good enough to deserve a name.

Definition 4.47 (Place)**.** Fix K a field. Then a *place* of a field K is a nontrivial equivalence class of absolute values on K.

We have the following theorem, which essentially says that these absolute values measure numbers about as orthogonally as one could ask for.

Theorem 4.48 (Strong approximation)**.** Suppose that $|\cdot|_1, \dots, |\cdot|_n$ are pairwise nonequivalent, nontrivial absolute values on a field K. Further, fix $a_1, \dots, a_n \in K$ and some $\varepsilon > 0$. Then there exists $x \in K$ such that

$$|x - a_\bullet|_\bullet < \varepsilon$$

for each $a_\bullet$.

Proof. We have the following claim.

Lemma 4.49. There is some $z \in K$ such that $|z|_1 > 1$ and $|z|_\bullet < 1$ for all other absolute values $|\cdot|_\bullet$.

Proof. We induct. For $n = 1$, anything with absolute value bigger than 1 will do, which exists because these absolute values are nontrivial. Then for $n = 2$, we note that reading Corollary 4.46 backwards requires there to be α with $|\alpha|_1 < 1$ and $|\alpha|_2 \geq 1$ and β with $|\alpha|_1 \geq 1$ and $|\beta|_2 < 1$. Then we can check that β/α will induce the correct inequalities.

Otherwise take $n > 2$, and we are promised z with $|z|_1 > 1$ and $|z|_k < 1$ for each $1 < k < n$. We have the following cases. Again using Corollary 4.46 we can find $|y|_1 > 1$ and $|y|_n < 1$, which is from the $n = 2$ case.

- If $|z|_n < 1$ already, we are finished.
- If $|z|_n = 1$, then we can take $z^m y$ for some sufficiently large m. Namely, the power is intended to kill the $|y|_\bullet$ between 1 and n.
- Otherwise $|z|_n > 1$. Now we set
$$t_m := \frac{z^m}{1 + z^m}.$$
Te point is that $z_m \to 1$ in $|\cdot|_1$ and $|\cdot|_n$ by running the manipulation through, and it goes to 0 elsewhere. So $t_m y$ will work for some sufficiently large m. ■

Now from the lemma we can find $z_k \in K$ such that $|z_k|_k > 1$ and $|z_k|_\ell < 1$ for each k, ℓ. In particular, the sequence

$$\frac{z_k^m}{1+z_k^m}$$

goes to 1 with respect to $|\cdot|_k$ and goes to 0 with respect to the other $|\cdot|_\bullet$. So we can set

$$z := \sum_{k=1}^{n} a_k \cdot \frac{z_k^m}{1+z_k^m}$$

as long as m is large enough to overcome ε. ■

We close this subsection with the following statement.

Theorem 4.50. All nontrivial absolute values on $\mathbb{Q}$ are equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.

Proof. This is in the book. Professor Vojta doesn't look this proof, but I do. It's a fun proof. ■

Remark 4.51 (Nir)**.** Of course the above holds in more general global fields.

4.5.4 Units in Discrete Valuation Rings

In this subsection, fix A a discrete valuation ring with $\mathfrak{p}$ its unique maximal ideal. We let $U := A^\times = A \setminus \mathfrak{p}$ be the unit group, and we let

$$U^{(n)} := 1 + \mathfrak{p}^n$$

be the a subgroup of U.

Remark 4.52. Our definition gives the descending chains

$$U^{(0)} \supseteq U^{(1)} \supseteq \cdots$$

We have the following statement.

Proposition 4.53. We have the following.

(a) $U/U^{(n)} \cong (A/\mathfrak{p}^n)^\times$ for each $n \in \mathbb{N}$.

(b) $U^{(n)}/U^{(n+1)} \cong A/\mathfrak{p}$ for each positive integer n.

Proof. We take these one at a time.

1. We note the induced map
$$U \to (A/\mathfrak{p}^n)^\times$$
is onto because $U = A \setminus \mathfrak{p}$. (To be explicit, this map is induced as $u \mapsto u + \mathfrak{p}^n$.) And we also note that we have kernel $U^{(n)}$ essentially by construction of $U^{(n)}$.

2. Fix $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then we note that we have a map $\varphi : U^{(n)} \mapsto A/\mathfrak{p}$ by taking
$$\varphi : 1 + \pi^n a \mapsto a + \mathfrak{p}.$$
We see φ is well-defined because $\mathfrak{p}^n = (\pi^n)$. Then φ is onto by just taking any coset representative backwards. And the kernel happens when $a \in \mathfrak{p} = (\pi)$, which pulls back to the original element living in $1 + \mathfrak{p}^{n+1} = U^{(n+1)}$.

Lastly, we can check by hand that this is homomorphic:

$$\varphi\big((1+\pi^n a)(1+\pi^n b)\big) = \varphi\left(1+\pi^n\left(a+b+\pi^n ab\right)\right) = (a+b)+\mathfrak{p} = (a+\mathfrak{p})+(b+\mathfrak{p}) = \varphi(1+\pi^n a)+\varphi(1+\pi^n b).$$

This finishes. ■

4.6 November 3

It is another day. The reading for Friday is chapter II, §4.

Quickly, we note that two equivalent absolute values $|\cdot|_1$ and $|\cdot|_2$ on K so that $|\cdot|_1 = |\cdot|_2^s$ for some $s \in \mathbb{R}^+$, then the completions $\hat{K}_1$ and $\hat{K}_2$ are isomorphic in such a way that the s is preserved. Essentially this holds because it will hold on the K hiding inside $\hat{K}_1$ and $\hat{K}_2$.

4.6.1 Completions of Archimedean Places

We recall Ostrowski's theorem.

Theorem 4.54 (Ostrowski)**.** Fix $(K, |\cdot|)$ a complete archimedean field. Then K is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ such that $|\cdot|$ becomes the normal absolute value on $\mathbb{R}$ or $\mathbb{C}$.

Proof. This is in the book. We won't give it here even though it is cool. ■

This gives the following corollaries.

Corollary 4.55. We have that any (not necessarily complete) archimedean valued field $(K, |\cdot|)$ has completion $\hat{K}$ isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ such that the absolute value on K is equivalent to the pull-back from either $\mathbb{R}$ or $\mathbb{C}$.

Corollary 4.56. If $(K, |\cdot|)$ is an archimedean valued field, then $(K, |\cdot|^s)$ is as well, for $0 < s \leq 1$.

We note that we are taking $s \leq 1$ because $s > 1$ might break the triangle inequality.

Now we specialize to the case where K is a number field. It has (distinct) real embeddings $\rho_1, \dots, \rho_r$ and (distinct) complex embeddings $\rho_1, \overline{\rho}_1, \dots, \rho_s, \overline{\rho}_s$, where $r + 2s = n = [K; \mathbb{Q}]$. We note that each embedding $K \hookrightarrow \mathbb{C}$ will give rise to an archimedean place on K by taking $x \in K$ to

$$|x|_\tau := |\tau x|.$$

When τ is real, this places are distinct, but when τ is complex, we note that $|x|_\tau = |x|_{\overline{\tau}}$ implies that we only have $r + s$ total embeddings. We show this below.

Proposition 4.57. Fix everything as above. The embeddings

$$|\cdot|_{\rho_1}, \quad \dots, \quad |\cdot|_{\rho_r}, \quad |\cdot|_{\sigma_1}, \quad \dots, \quad |\cdot|_{\sigma_s}$$

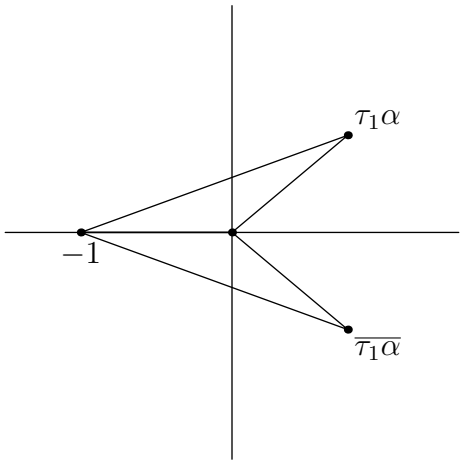
are pairwise nonequivalent.

Proof. Suppose that $\tau_1, \tau_2 \in \mathrm{Hom}(K, \mathbb{C})$ where $\tau_1 \neq \tau_2$ and $\tau_1 \neq \overline{\tau_2}$. Then we want to show that $|\cdot|_{\tau_1} \neq |\cdot|_{\tau_2}$. Well, fix $\alpha \in K$ some primitive element over $\mathbb{Q}$ so that $\tau_1(\alpha) \neq \tau_2(\alpha)$ and $\tau_1(\alpha) \neq \overline{\tau_2(\alpha)}$ because having the same image on α would extend to all of $K = \mathbb{Q}(\alpha)$.

But from this we claim that

$$|\tau_1\alpha| \neq |\tau_2\alpha| \qquad \text{or} \qquad |\tau_1(\alpha+1)| \neq |\tau_2(\alpha+1)|.$$

Indeed, if these were equal, then we can create the following triangles.



Namely, from these triangles we are able to force $\tau_2\alpha$ to be either $\tau_1\alpha$ or its conjugate by side-side-side congruence, where the side between 0 and 1 is fixed.

So without loss of generality (possibly replacing α with $\alpha+1$), we may take $|\tau_1\alpha| < |\tau_2\alpha|$. Now we choose $r \in \mathbb{Q}$ such that $|\tau_1\alpha| < r < |\tau_2\alpha|$ so that

$$\left|\frac{\alpha}{r}\right|_{\tau_1} < 1 \qquad \text{but} \qquad \left|\frac{\alpha}{r}\right|_{\tau_2} > 1.$$

It follows that $(\alpha/r)^\bullet$ will go to 0 under $|\cdot|_{\tau_1}$ but not in $|\cdot|_{\tau_2}$, so their induced topologies are indeed different. ■

4.6.2 Completions of Nonarchimedean Valuations

Fix $(K, |\cdot|)$ be some complete nonarchimedean valued field, and we fix A its valuation ring. For our discussion, we need Hensel's lemma, which we take from the handout.

Lemma 4.58 (Hensel)**.** Fix $f \in A[x]$, and suppose that we have $\alpha_0 \in A$ such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Then the sequence defined recursively by

$$\alpha_{n+1} := \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

for each $n \in \mathbb{N}$ will converge to a root α of f such that

$$|\alpha - \alpha_0| \le \frac{|f(\alpha_0)|}{|f'(\alpha_0)|} < |f'(\alpha_0)|,$$

and in fact α is the only such root with $|\alpha - \alpha_0| < |f'(\alpha_0)|$.

Remark 4.59. We note that the right-hand side $\frac{|f(\alpha_0)|}{|f'(\alpha_0)|}$ is less than 1 because it is less than $f'(\alpha_0)$, which has magnitude no more than 1 because it is in A.

Proof. Quickly, we note that each $\alpha \in K$ which has $|\alpha - \alpha_0| < |f'(\alpha_0)|$ will actually have $|f'(\alpha)| = |f'(\alpha_0)|$. Indeed, because $\alpha_0 \in A$, we see $f'(\alpha_0) \in A$, so it has magnitude at most 1. And then by doing a Taylor expansion, we can find $\beta \in A$ such that

$$f'(\alpha) = f'(\alpha_0) + \beta(\alpha - \alpha_0), \tag{$*$}$$

where β simply accumulates all of the higher-order Taylor terms; to be explicit, $(x-\alpha_0)$ will divide $f'(x)-f'(\alpha_0)$ formally because it vanishes as a polynomial at $x=\alpha_0$, so we can find g such that

$$f'(x)-f'(\alpha_0)=g(x)(x-\alpha_0)$$

and then plug in α. So using the triangle inequality on $(*)$ tells us that

$$|f'(\alpha)|-|f'(\alpha_0)|\le|\alpha-\alpha_0|<|f'(\alpha_0)|,$$

so it follows $|f'(\alpha)|=|f'(\alpha_0)|$ because all triangles are isosceles.

We now attack the proof directly. Set

$$c:=\frac{|f(\alpha_0)|}{|f'(\alpha_0)|^2},$$

which has $c<1$ by hypothesis. We claim the following.

Lemma 4.60. Fix everything as above. For any $k\in\mathbb{N}$, we have the following.

(a) $|\alpha_k-\alpha_0|\le\frac{|f(\alpha_0)|}{|f'(\alpha_0)|}<1$,

(b) $|f'(\alpha_k)|=|f'(\alpha_0)|$, and

(c) $|f(\alpha_k)|\le c^{2^i}|f'(\alpha_0)|$.

Proof. For $k=0$, there is nothing to say. So we jump into the inductive step; take the above true for k, and we show $k+1$. We note that, by definition of α_{k+1},

$$|\alpha_{k+1}-\alpha_k|=\left|\frac{f(\alpha_k)}{f'(\alpha_k)}\right|\overset{(c)}{\le}c|f'(\alpha_0)|=\frac{|f(\alpha_0)|}{|f'(\alpha_0)|}<1,$$

where we have used (c), where marked. This gives (a).

For (b), we start by seeing

$$|\alpha_{k+1}-\alpha_0|\overset{(1)}{\le}\frac{|f(\alpha_0)|}{|f'(\alpha_0)|}=c|f'(\alpha_0)|=c|f'(\alpha_0)|<|f'(\alpha_0)|,$$

from which $|f'(\alpha_{k+1})|=|f'(\alpha_k)|$ is supposed to follow.

Lastly, for (c), we use a Taylor expansion again to write

$$f(\alpha_{k+1})=f(\alpha_k)+f'(\alpha_k)(\alpha_{k+1}-\alpha_k)+\gamma(\alpha_{k+1}-\alpha_k)^2$$

for some $\gamma\in A$ which eats all of the higher-order terms. Plugging in the definition of α_{k+1} causes the first two terms to vanish, so we have that

$$|f(\alpha_{k+1})|\le|\alpha_{k+1}-\alpha_k|^2=\left|\frac{f(\alpha_k)}{f'(\alpha_k)}\right|^2.$$

By (2), the right-hand side is $\left|\frac{f(\alpha_k)}{f'(\alpha_0)}\right|^2$, which is $\left(c^{2^k}|f'(\alpha_0)|\right)^2$ by the inductive hypothesis on (3), which collapses down to (3) after plugging in for the bound on $|f'(\alpha_0)|$. This finishes. ■

We will finish this proof next time. ■

4.7 November 5

The fun will soon continue.

4.7.1 Hensel's Lemma

As usual, we continue setting $(K, |\cdot|)$ is a nonarchimedean valued field, and A is its valuation ring. We continue showing Hensel's lemma.

Lemma 4.61 (Hensel)**.** Fix $f \in A[x]$, and suppose that we have $\alpha_0 \in A$ such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Then the sequence defined recursively by

$$\alpha_{n+1} := \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

for each $n \in \mathbb{N}$ will converge to a root α of f such that

$$|\alpha - \alpha_0| \le \frac{|f(\alpha_0)|}{|f'(\alpha_0)|} < |f'(\alpha_0)|,$$

and in fact α is the only such root with $|\alpha - \alpha_0| < |f'(\alpha_0)|$.

Proof continued from last class. Last time we showed the following, for any $k \in \mathbb{N}$.

(a) $|\alpha_k - \alpha_0| \le \frac{|f(\alpha_)|}{|f'(\alpha_0)|} \le 1$,

(b) $|f'(\alpha_k)| = |f'(\alpha_0)|$,

(c) $|\alpha_{k+1} - \alpha_k| \le c^{2^i}$, and

(d) $|f(\alpha_k)|lec^{2^i}|f'(\alpha_0)|^2$, where $c < 1$.

Our old (c) is now (d), and (c) was proven above as an intermediate step. In particular, (c) implies that $\{\alpha_k\}_{k\in\mathbb{N}}$ is a Cauchy sequence: we can bound, for any $k > \ell \ge 0$,

$$|\alpha_k - \alpha_\ell| = \left| \sum_{n=\ell+1}^{k} \alpha_n - \alpha_{n-1} \right| \le \max_{\ell+1 \le n \le k} |\alpha_n - \alpha_{n-1}| \to 0.$$

So we may conjure $\alpha \in A$ the limit of this sequence, which satisfies $(*)$ because of (a) above and continuity of the function $x \mapsto |x - \alpha_0|$. We will leave the check of uniqueness to the handout. ■

We have the following special case.

Corollary 4.62. Fix $f \in A[x]$. If $\alpha_0 \in A$ has $|f'(\alpha_0)| = 1$ and $|f(\alpha_0)| < 1$, then there is a unique root α of f (described by the above recursion) with $|\alpha - \alpha_0| < 1$. In other words, if κ is the residue field of A, then we are asking for $\alpha_0 \in \kappa$ such that $f(\alpha_0) = 0$ while $f'(\alpha_0) \neq 0$.

Proof. This follows directly from Hensel's lemma. ■

The book has the following form of Hensel's lemma, for the purposes of factoring.

Definition 4.63 (Primitive)**.** Fix A a unique factorization domain. Then $f \in A[x]$ is *primitive* if not all of its coefficients are divisible by any prime. If A is a discrete valuation ring with $\mathfrak{m}$ the unique prime ideal, then we are asserting $f \in A[x] \setminus \mathfrak{m}[x]$.

Lemma 4.64 (Hensel, II)**.** Fix $(K, |\cdot|)$ and A as usual with $\mathfrak{p} := \{\alpha \in A : |\alpha| < 1\}$ the unique prime ideal of A and $\kappa := A/\mathfrak{p}$ the residue field. Now, given $f \in A[x]$ a primitive polynomial and a factorization

$$\overline{f} = \overline{g} \cdot \overline{h}$$

in $\kappa[x]$ such that $\gcd(\overline{g}, \overline{h}) = (1)$, then we can lift $\overline{g}$ and $\overline{h}$ to a factorization $f = gh$ with $g, h \in A[x]$ such that $\deg g = \deg \overline{g}$.

Proof. This is kind of technical, so we just refer to the book. ■

Remark 4.65. To relate this to the original version of Hensel's lemma, we can take $\overline{g} := x - \overline{\alpha_0}$ to be linear in the above so that $\overline{f}(\overline{\alpha_0}) = 0$. Then the condition that $\overline{f}'(\overline{\alpha_0}) \neq 0$ essentially means that $\overline{f}$ does not have a double root at α_0, which corresponds with $\gcd(\overline{g}, \overline{f}/\overline{g}) = (1)$. So the book Hensel's lemma will give us a linear

$$g := x - \alpha,$$

yielding a root α of f.

4.7.2 Applications of Hensel's Lemma

Anyways, we have the following corollary.

Corollary 4.66. Fix $f \in \kappa[x]$ an irreducible polynomial, denoted by

$$f(x) = \sum_{k=0}^{n} a_k x^k,$$

where $a_n \neq 0$. We define $|f| := \max_k\{|a_k|\}$, and we claim $|f| = \max\{|a_0|, |a_n|\}$.

Proof. We do this in cases.

(i) If $a_0 = 0$, then $f = a_1 x$ for f to be irreducible. This immediately gives the result.

(ii) Take $a_0 \neq 0$. By factoring out constants, we may assume that $|f| = 1$ so that $f \in A[x]$ and is primitive. Now, find the smallest r such that $|a_r| = 1$ so that

$$f(x) \equiv \underbrace{x^r}_{\overline{g}} \underbrace{\sum_{k=r}^{n-r} a_k x^{k-r}}_{\overline{h}} \pmod{\mathfrak{p}}.$$

Now we apply the second version of Hensel's lemma with $\overline{g}$ and $\overline{h}$ as above, where $\gcd(\overline{g}, \overline{h}) = (1)$ because $\overline{h}$ has a nonzero constant term and hence is not divisible by x. So we get $g, h \in A[x]$ with $\deg g = r$ such that

$$f = gh.$$

But now f is irreducible, so one of g or h is constant, so $r \in \{0, n\}$. It follows $|a_r| = 1$ is either reading as $|a_0| = 1$ or $|a_n| = 1$, so $\max\{|a_0|, |a_n|\} = 1$, as needed. ■

And here is a corollary to our corollary.

Corollary 4.67. Fix everything as in the previous corollary. Graphic $(k, \nu(a_k))$ for $0 \le k \le n$, we have that none of the points are below the line from $(0, \nu(a_0))$ to $(n, \nu(a_n))$.

Proof. This is more or less given in the previous corollary, but we won't give more details here. ∎

Remark 4.68. This leads to the theory of the Newton polygon, which we won't discuss here.

Here is another corollary.

Corollary 4.69 (Gauss's lemma, nonarchimedean case)**.** Fix $(R, |\cdot|)$ a (not necessarily complete) nonarchimedean valued ring. Then, given $f, g \in R[x]$, we have that $|fg| = |f| \cdot |g|$, where we defined $|f|$ and $|g|$ in the previous corollary.

Proof. Fix

$$f(x) = \sum_{k=0}^{M} a_k x^k \qquad \text{and} \qquad g(x) = \sum_{\ell=0}^{N} b_k x^k.$$

Then we have that

$$f(x)g(x) = \sum_{n=0}^{N+M} c_n x^n,$$

where

$$c_n = \sum_{k+\ell=n} a_k b_\ell,$$

where we extend a_k and b_ℓ with 0s as is necessary. Now, we recall $|f| = \max_k\{|a_k|\}$ and $|g| = \max_\ell\{|b_\ell|\}$, and we note that

$$|c_n| \le \max_{k,\ell\in\mathbb{N}}\{|a_k b_\ell|\} = \max_{k\in\mathbb{N}}\{|a_k|\} \cdot \max_{\ell\in\mathbb{N}}\{|b_\ell|\} = |f| \cdot |g|,$$

so $|fg| \le |f| \cdot |g|$. For the other direction, we find the least k_0 and ℓ_0 with $|a_{k_0}| = |f|$ and $|b_{\ell_0}| = |g|$. Then we see that

$$c_{k_0+\ell_0} = \sum_{k+\ell=k_0+\ell_0} a_k b_\ell.$$

Now, the term $a_{k_0} b_{\ell_0}$ will have size $|f| \cdot |g|$. Each other term $a_k b_\ell$ will either have $k < k_0$ or $\ell < \ell_0$, implying that $|a_k b_\ell| < |a_{k_0} b_{\ell_0}| = |f| \cdot |g|$. Thus, $|c_{k_0+\ell_0}| \ge |f| \cdot |g|$, so $|fg| \ge |f| \cdot |g|$, as needed. ∎

At this point, the corollaries are stacking up on each other.

Corollary 4.70. Fix $\alpha \in \overline{K}$ the algebraic closure of a complete nonarchimedean field K. Then α is integral over A if and only if $|\operatorname{N}_K^{K(\alpha)} \alpha| \le 1$.

Proof. In one direction, take α integral so that $f \in A[x]$ has f monic and $f(\alpha) = 0$. We also set g to be the irreducible polynomial for α over K. Then we see that $g \mid f$ in $K[x]$ and $|f| = 1$ (f is monic), with $|g|, |f/g| \ge 1$ (they are monic), so Gauss's lemma bounds to $|g| = |f/g| = 1$. Thus,

$$\left|\operatorname{N}_K^{K(\alpha)} \alpha\right| = |\pm g(0)| \le 1.$$

For the other direction, still take g the monic irreducible polynomial for α over K. We see that $g(0) = \pm N_K^{K(\alpha)}(\alpha)$, so

$$|g| = \max\{|1|, |g(0)|\} = 1.$$

Thus, $g \in A[x]$, so α is indeed integral over A. This finishes. ∎

4.8 November 8

Here we go.

4.8.1 Extending Absolute Values

We are extending absolute values today.

Theorem 4.71. Fix $(K, |\cdot|)$ a complete valued field. Fix L/K an algebraic extension. Then there exists a unique absolute value $|\cdot|_L : L \to \mathbb{R}_{\geq 0}$ extending the absolute value on K, given by

$$|\alpha|_L = \left|\mathrm{N}_K^{K(\alpha)} \alpha\right|^{1/[K(\alpha):K]}$$

for all $\alpha \in L^\times$.

Proof. We proceed in cases.

- Take K archimedean. If $L = K$, there is nothing to say here. Otherwise, by our classification of complete archimedean fields, $K = \mathbb{R}$ and $L = \mathbb{C}$, so we get the statement by Ostrowski's theorem classifying the places of $\mathbb{C}$. There is some care required to check that equivalence of absolute values becomes full equality, but it can be done.
- Take K nonarchimedean and nontrivial with valuation ring A. We split the proof in half.
  (a) We show that the $|\cdot|_L$ suggested does indeed satisfy the constraints.[3] Namely, $|\alpha|_L = |\alpha|$ for each $\alpha \in K$ by pushing everything through. And otherwise we note that, for any L' containing α, we have
  $$|\alpha|_L = \left|\mathrm{N}_K^{L'} \alpha\right|^{1/[L':K]} \tag{$*$}$$
  by checking things with norms, so we get some well-defined-ness.
  We now need to check that $|\alpha|_L$ is in fact an absolute value. Well, $|\alpha|_L \geq 0$ with equality if and only if $\alpha = 0$ comes from the corresponding statement about norms. Then
  $$|\alpha\beta|_L = |\alpha|_L \cdot |\beta|_L$$
  holds by using $(*)$ on $K(\alpha, \beta)$ and the multiplicativity of the norm.
  Lastly, we need to check the strong triangle inequality, which requires some trickery. Without loss of generality, take $|\alpha|_L \leq |\beta|_L$, and we want to show that
  $$|\alpha + \beta|_L \overset{?}{\leq} |\beta|_L.$$
  By applying division, it suffices to show that $|\alpha/\beta + 1| \leq 1$ given that $|\alpha/\beta| \leq 1$. But $|\alpha/\beta| \leq 1$ implies that α/β is integral over A, so $\alpha/\beta + 1$ is integral over A, so $|\alpha/\beta + 1| \leq 1$. This finishes the proof of existence.
  (b) Take $|\cdot|$ a nontrivial absolute value, and we show uniqueness of the extension. Suppose that $|\cdot|'_L$ be another absolute value on L extending $|\cdot|$. We set
  $$B := \{\alpha \in L : |\alpha|_L \leq 1\} \qquad \text{and} \qquad B' := \{\alpha \in L : |\alpha|'_L \leq 1\}.$$
  We claim that $B \subseteq B'$. Indeed, otherwise there is $\alpha \in B \setminus B'$, which is an $\alpha \in L$ with $|\alpha|_L \leq 1$ and $|\alpha|'_L \geq 1$. But now look at the irreducible polynomial for α as
  $$f(x) = \sum_{k=0}^{n} a_n x^n \in K[x].$$

[3] This even works if $|\cdot|$ on K is trivial, which would imply that $|\cdot|_L$ is also trivial by construction.

We note that we get $A[x]$ because $|\mathrm{N}_K^{K(\alpha)}\alpha| \le 1$, which is the last thing we showed last class. But now $|\alpha^{-1}|'_L < 1$ even though

$$1 = -a_{n-1}\alpha^{-1} - a_{n-2}\alpha^{-2} - \cdots - a_0\alpha^{-n}$$

after doing some rearranging with f, which is monic. It follows that the size of the left-hand side is 1 while the size of the right-hand side is at least 1 by the strong triangle inequality, which is a contradiction.

Now, recall from our discussion about places that $B \subseteq B'$ will imply that $|\cdot|'_L = |\cdot|^s_L$ for some $s > 0$. But now, because $|\cdot|$ is nontrivial on K, we can plug in some value of $\alpha \in K$ giving $|\alpha|_L \neq 1$, which forces $s = 1$. This finishes.

- If $|\cdot|$ is trivial on K, then we leave this as an exercise. The extension should be the trivial absolute value. ■

The above gets us that algebraic extensions of complete valued fields are at least valued. However, they need not be complete.

4.8.2 Normed Vector Spaces

We have the following definition.

Definition 4.72 (Normed vector spaces)**.** Fix V a K-vector space, where $(K, |\cdot|)$ is a valued field. Then we have the following definitions. A *norm* on V is a function $\|\cdot\| : V \to \mathbb{R}$ such that the following hold.

(i) We have $\|v\| \ge 0$ for any $v \in V$ with equality if and only if $v = 0$.

(ii) We have $\|cv\| = |c| \cdot \|v\|$, for any $c \in K$ and $v \in V$.

(iii) We have $\|v + w\| \le \|v\| + \|w+\|$ for each $v, w \in V$.

Example 4.73. Any vector space will have a norm by taking the supremum of the coefficients under the coordinates of a particular basis.

We note that a norm will induce a metric on V in the usual way.

Definition 4.74 (Equivalence of norms)**.** Fix $\|\cdot\|_1$ and $\|\cdot\|_2$ to norms on V. They are *equivalent* if and only if there are constants $\rho_1, \rho_2 > 0$ such that

$$\rho_1\|v\|_1 \le \|v\|_2 \le \rho_2\|v\|_2$$

for each $v \in V$.

It is not hard to see that equivalence is in fact an equivalence relation.

We have the following lemma.

Lemma 4.75. Fix V a finite-dimensional K-vector space, where $(K, |\cdot|)$ is a complete valued field. Then we have the following.

(a) Any two norms on V are equivalent.

(b) V is a complete metric space under the induced metric.

Remark 4.76. Even if K is not complete, neither (a) nor (b) need be true. For example, extensions of number fields do not have unique extensions.

Proof. We sketch. Fix $\{v_k\}_{k=1}^n$ a basis of V over K. Then we define our initial norm as

$$\left\| \sum_{k=1}^n a_k v_k \right\| := \max_{1 \le k \le n} \{a_k\},$$

which we won't check to be a norm. We can check that V is complete with respect to this norm by looking at coordinate-wise convergence in a Cauchy sequence, using the fact that K is complete.

It remains to show that $\|\cdot\|$ is the only equivalence class. For the archimedean case, there are compactness arguments. For the nonarchimedean case, see the book. ■

Anyways, we bring up this machinery because of the following corollary.

Corollary 4.77. Fix $(K, |\cdot|)$ a complete valued field and L/K a finite extension. Then L is complete with respect to the (unique) extension $|\cdot|_L$ described previously.

Proof. This comes from the above, viewing the absolute value on L as a norm on L as a K-vector space. ■

The finite extension hypothesis is necessary.

Example 4.78. The algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ is not complete, but the metric completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}_p}$ is algebraically closed, so there is a field with all the nice properties we want.

4.8.3 Local $AKLB$ Set-Up

So now we can build a local $AKLB$ set-up: fix $(K, |\cdot|)$ a nontrivial complete nonarchimedean valued field with valuation ring A. Then any finite extension L will have a unique extension $|\cdot|_L$ of $|\cdot|$, and we can let B be the corresponding valuation ring.

Now, A and B are local rings, so (say) A is Dedekind if and only if A is a discrete valuation ring if and only if there is a discrete valuation on K (by extension) with valuation ring A. But then this new valuation induces some absolute value $|\cdot|'$ with the same $A = \{\alpha \in K : |\alpha|' \le 1\}$ set, so it is equivalent to the absolute value on K we started with.

The point of this computation is that we need to check if the valuation induced by $|\cdot|$ on K is a discrete valuation, which will make the valuation on L discrete by its construction (it will output into $\frac{1}{[L:K]}\operatorname{im}(|\cdot|)$, which maintains being discrete), so in this case B will also be Dedekind in this case.

So we get the following picture.

$$\begin{array}{ccc} B & \subseteq & L \\ | & & | \\ A & \subseteq & K \end{array}$$

Technically we should check that B is finite over A, but we will not do this here.

Further, we let $\mathfrak{p} \subseteq A$ and $\mathfrak{q} \subseteq B$ be their maximal ideals. Because $|\cdot|_L$ extends $|\cdot|$, we see that checking definitions gives $\mathfrak{q}$ over $\mathfrak{p}$. And in fact $\mathfrak{q}$ is the unique prime ideal of B lying over $\mathfrak{p}$ because there is only one prime in B. So the fundamental identity gives

$$[L : K] = e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p}).$$

So our local theory is nice.

4.8.4 Global Fields

Let's start being a little less local. We have the following definition.

Definition 4.79 (Global field)**.** A *global field* is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$. In other words, a global field is a number field or a "global function field"—function field over a curve over a finite field.

We will not care so much about the latter case because algebraic geometry is not a prerequisite for this course.

4.9 November 10

Let's just get to the point.

4.9.1 Global Fields

Last time we ended by talking about global fields, which were defined as follows.

Definition 4.80 (Global field)**.** A *global field* is either a finite extension of $\mathbb{Q}$ (a number field) or a finite extension of $\mathbb{F}_p[t]$ (a finitely generated extension of a finite field of transcendence degree 1).

In good number theory, all global fields will be considered at once. We remark that we might want to look at any finite extension of $F(t_1, \dots, t_d)$ for arbitrary fields F, but these are not global. Let's discuss why we restrict to $d = 1$ in the above definition.

In what follows, fix F a field and K a finite extension of $F(t)$. Notably, we are not requiring K to be global, but it might be easier psychologically to make F finite so that this is the case. In analogy with the case of number fields, we would like to create a ring of integers in K, but it is not well-defined here: both

$$F[t] \qquad \text{and} \qquad F[1/t]$$

are Dedekind rings with fraction field $F(t)$, so we have difficulties even in the case where $K = F[t]$. Regardless, being Dedekind appears to be good candidate for being a ring of integers.

So let's motivate our definition of a global field. For F a field and A a (non-field) Dedekind ring of finite type over F with fraction field K. Then the transcendence degree of K over F is equal to 1, by some result in algebraic geometry. It follows K is a finite extension of $F(t)$, for any transcendental element $t \in F$.

Definition 4.81 (Funtion field)**.** Fix everything as in the previous paragraph. Then K is a *function field in one variable over* F, where F is our constant field for K.

Remark 4.82. A finite extension of $F(t_1, \dots, t_d)$ is a "function field in d variables over F." Note that this does cover our $d = 1$ case (in contrast to the above definition) because the integral closure of $F[t]$ in K will be a Dedekind ring in K and can serve the role of A above. We will not elaborate on this here.

So now we fix K a number field or function field in one variable over an arbitrary field F (and hence not necessarily global), and let $A = \mathcal{O}_K$ in the number field case or a Dedekind subring of K in the function field case.

4.9.2 Global $AKLB$ Set-Up

Now let's build an $AKLB$ set-up for our global fields. Fix L/K a finite extension of fields, and we take B to be the integral closure of A in L; probably following from some theory we developed long ago, B is finite

over A and Dedekind, giving the following diagram.

$$\begin{array}{ccc} B & \subseteq & L \\ | & & | \\ A & \subseteq & K \end{array}$$

Further, we fix $\mathfrak{p}$ a nonzero prime in A, and let $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ be the primes of $\mathfrak{p}$ lying over $\mathfrak{p}$, which we can add to the diagram as follows. (Namely, extensions of Dedekind rings have the usual prime ideal theory.)

$$\begin{array}{ccccc} \mathfrak{q}_\bullet & \subseteq & B & \subseteq & L \\ | & & | & & | \\ \mathfrak{p} & \subseteq & A & \subseteq & K \end{array}$$

Now we focus locally. As usual, each nonzero prime $\mathfrak{p}$ will induce a nonarchimedean absolute value on K by $|x|_\mathfrak{p} := c^{-\nu_\mathfrak{p}(x)}$ for some fixed $c > 0$. We set $\hat{K}$ to be the completion of K with respect to $|\cdot|_\mathfrak{p}$ and set

$$\hat{A} \cong \varprojlim A/\mathfrak{p}^\bullet$$

to be the valuation ring in $\hat{K}$ with $\hat{\mathfrak{p}}$ is the maximal ideal of $\hat{A}$. By checking the uniformizer of $\mathfrak{p}$, we see that $\mathfrak{p}\hat{A} = \hat{\mathfrak{p}}$.

We remark that if we pull back $\hat{A} \subseteq \hat{K}$ along $\iota : K \hookrightarrow \hat{K}$ to K, then we get the localization $A_\mathfrak{p}$; similarly, if we pull back $\hat{\mathfrak{p}}$, then we get $\mathfrak{p}A_\mathfrak{p}$. More generally, we can check that $\hat{A}/\hat{\mathfrak{p}}^\bullet \cong A/\mathfrak{p}^\bullet$ and the pull-back of $\hat{\mathfrak{p}}^\bullet$ to K is $\mathfrak{p}^\bullet$ and $\hat{\mathfrak{p}}^\bullet = \mathfrak{p}^n\hat{A}$.

We would like to extend $|\cdot|_\mathfrak{p}$ up to L to continus our story. It happens that these extensions are in bijection with the primes $\mathfrak{q}_\bullet$ above $\mathfrak{p}$, where $\mathfrak{q}_\bullet$ induces a nonarchimedean valuation in the usual way. We will fix a chosen prime $\mathfrak{q}$ over $\mathfrak{p}$ so that $|\cdot|_\mathfrak{q} : L \to \mathbb{R}$ extends $|\cdot|_\mathfrak{p} : K \to \mathbb{R}$.

So we set $\hat{L}$ to be the completion of $(L, |\cdot|_\mathfrak{q})$, and we will take care of our book-keeping by setting $j : L \hookrightarrow \hat{L}$ and

$$\hat{B} \cong \varprojlim B/\mathfrak{q}^\bullet$$

to be the valuation ring of $\hat{L}$. Quickly, we see that the universal property of $\hat{K}$, there is a unique map $\hat{K} \to \hat{L}$ of fields commuting (namely, $K \hookrightarrow L \hookrightarrow \hat{L}$, and $\hat{L}$ is complete), which is injective automatically because this is a mapping of fields. So we get the following local diagram.

$$\begin{array}{ccc} \hat{B} & \subseteq & \hat{L} \\ | & & | \\ \hat{A} & \subseteq & \hat{K} \end{array}$$

For fun, we let $\hat{\mathfrak{q}}$ to be the valuation ideal of $\hat{B}$, and we get statements like $j^{-1}(\hat{B}) = B_\mathfrak{q}$ from the preceding discussion.

We would like to make the above local diagram an actual local $AKLB$ set-up. As some book-keeping to keep track of the diagram, we have the following lemma.

Lemma 4.83. We have that $\hat{L} = L\hat{K}$, where the composition is taking place in the canonical embeddings in L.

Proof. We can set

$$L = K(\alpha_1, \dots, \alpha_n).$$

Then $L\hat{K} = \hat{K}(\alpha_1, \dots, \alpha_n)$, and this is finite over $\hat{K}$ because the generators $\alpha_\bullet$ were finite over K, so $L\hat{K}$ is complete. Additinoally, $L\hat{K}$ of course contains L, so the universal property of $\hat{L}$ gives us a unique map

$$\hat{L} \hookrightarrow L\hat{K}$$

commuting with everything. This turns into an equality for reasons which are not clear to me, finishing. ∎

The point of the above statement is to say that $[\hat{L} : \hat{K}]$ is a finite extension. We also remark that $\hat{B}$ is indeed the integral closure of $\hat{A}$ in $\hat{L}$ because $\alpha \in \hat{L}$ is integral over $\hat{A}$ is equivalent to $|\alpha|_{\mathfrak{q}} \leq 1$ from a resul we showed a while ago. We will omit the check that $\hat{B}$ is finite over $\hat{A}$.

So indeed, our local diagram is an actual local $AKLB$ set-up. Now let's start moving towards some number theory. We see that

$$f_{\hat{\mathfrak{q}}/\hat{\mathfrak{p}}} = f_{\mathfrak{q}/\mathfrak{p}}$$

because these residue fields come from $\hat{B}/\hat{\mathfrak{q}} \cong B/\mathfrak{q}$ and $\hat{A}/\hat{\mathfrak{p}} \cong A/\mathfrak{p}$. Additionally, $e_{\hat{\mathfrak{q}}/\hat{\mathfrak{p}}} = e_{\mathfrak{q}/\mathfrak{p}}$ because the factorization of $\mathfrak{p}$ in B will coincide with the factorization of $\hat{\mathfrak{p}}$ in $\hat{B}$ after pushing everything through $L \hookrightarrow \hat{L}$. More rigorously, we can see that $\nu_{\hat{\mathfrak{q}}} \circ j = \nu_{\mathfrak{q}}$ and $\nu_{\hat{\mathfrak{p}}} \circ i = \nu_{\mathfrak{p}}$, and the equality of the valuations gives equality of the ramifiactions.

The point of this is that we get the following version of the fundamental identity by simply pushing our ramification and inertial information through.

Corollary 4.84. Fix everything as above. We have that

$$[L : K] = \sum_{k=1}^{r} [\hat{L}_k : \hat{K}],$$

where $\hat{L}_k$ is the completion of L with respect to $|\cdot|_{\mathfrak{q}_k}$.

Hooray.

4.9.3 A Little Global Function Fields

Let's work more closely with global fields.

Definition 4.85 (Global function field)**.** A *global function field* is a finite extension of $\mathbb{F}_p(t)$.

Proposition 4.86. Fix K a global function field with $\mathbb{F}_q$ its largest finite subfield, which exists because I said so. Then, for any $t \in K \setminus \mathbb{F}_q$, we have that K is a finite extension of $\mathbb{F}_q(t)$. Further, all places of K are trivial on $\mathbb{F}_q$ and come from one of the following $AKLB$ set-ups.

$$\begin{array}{ccc} A & \subseteq & K \\ | & & | \\ \mathbb{F}_q[t] & \subseteq & \mathbb{F}_q(t) \end{array} \qquad \begin{array}{ccc} A & \subseteq & K \\ | & & | \\ \mathbb{F}_q[1/t] & \subseteq & \mathbb{F}_q(t) \end{array}$$

Proof. To see that the valuation is trivial on $\mathbb{F}_q$, we note that all elements of $\mathbb{F}_q$ are torsion. The rest comes from algebraic geometry. ■

4.10 November 12

Ok.

4.10.1 Some Loose Ends

Last time we claimed the following loose ends; let's talk about them.

Lemma 4.87. A global function field K has a largest finite subfield.

Proof. We note that a sub-extension of a finitely generated field extension is finitely generated, so we get the result by noting that $\overline{\mathbb{F}_p} \cap K$ must be finitely generated over $\mathbb{F}_p$ and hence be our largest finite subfield. ■

Lemma 4.88. Fix K a global function field and $\mathfrak{p}$ a nonzero prime of the valuation ring A. Then we can show that all extensions of $|\cdot|_{\mathfrak{p}} : K \to \mathbb{R}$ to some field extension L are induced as $|\cdot|_{\mathfrak{q}}$ from primes $\mathfrak{q}$ in L over $\mathfrak{p}$.

Proof. This will go on the homework. ■

This goes into the $AKLB$ set-up from last time.

Lemma 4.89. Fix $(K, |\cdot|)$ a complete nonarchimedean valued field with valuation ring A. If L/K is a finite field extension with $|\cdot| : L \to \mathbb{R}$ the unique extension of $|\cdot| : K \to \mathbb{R}$, and we set B to be the integral closure of A in L. Then B is finitely generated over A.

Proof. The main point is to forcefully localize. We know that L is complete with respect to $|\cdot|$ already, and we showed some time ago in Corollary 4.70 that B is in fact the valuation ring of L.

Now, fix $\mathfrak{p}$ the valuation ideal of A and $\kappa := A/\mathfrak{p}$ the residue field, and we fix some uniformizer $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Now, $\lambda = B/\mathfrak{p}B$ is not necessarily a field, but it is a κ-vector space (it is an A-module automatically, but the $\mathfrak{p}$-action has been nullified), so find some

$$\{b_i\}_{i \in I} \subseteq B$$

which give a κ-basis for λ upon reduction. We have the following checks.

- We show that I is finite. The main point is to show that $\{b_i\}_{i \in I}$ is linearly independent over K: indeed, any nontrivial linear relation
$$\sum_{i \in I} a_i b_i = 0$$
with $a_\bullet \in K$ can be turned into one where not all of the $a_\bullet$ are in $\mathfrak{p}$ (by dividing out by π enough times), which turns into a nontrivial relation in $B/\mathfrak{p}B$ upon reduction. But this cannot be because the $b_\bullet$ were a basis of $B/\mathfrak{p}B$ and hence linearly independent.

  The above linear independence in L/K shows that $\#I \le [L : K]$ and in particular is finite.

- We now show that the $b_\bullet$ span. Appropriately, we may take E to be
$$E := \bigoplus_{i \in I} A b_i$$
to be generated by the b_i. We note that each $x \in B$ can be reduced $\pmod{\mathfrak{p}}$ to some element in $B/\mathfrak{p}B$, which will have a representative in E by the spanning. Namely, we can write
$$x = c_0 + x_1 \pi,$$
for some $c_0 \in E$. Iterating this process for x_1 and so on, we get a series
$$x = c_0 + c_1 \pi + c_2 \pi^2 + \cdots,$$
where $c_\bullet \in E$. Now, because A is complete, when we expand out the $c_\bullet$ in terms of their $b_\bullet$ components, we will get a power series in π in A, which will have to converge in A by that completeness. In particular, $x \in E$.

  So indeed, $B \subseteq E$, so $B = E$.

Thus, B finitely generated over A, which finishes. ■

4.10.2 Local Fields

Let's now return to our story. We have the following claim.

Proposition 4.90. Fix K a global function field, for concreteness viewed as a finite extension of $\mathbb{F}_p(t)$. Then all places of K come from extensions of places of $\mathbb{F}_p(t)$. All places of $\mathbb{F}_p(t)$ come from prime ideals of $\mathbb{F}_p[t]$ or $\mathbb{F}_p[1/t]$.

Proof. Omitted; is is essentially death by algebraic geometry. ■

Remark 4.91 (Nir)**.** I think the place of $\mathbb{F}_p[1/t]$ we need to worry about is the one which comes from the prime ideal $(1/t)$.

Remark 4.92. The above does induce the set of all places of K and hence is independent of our choice of t in "for concreteness" phrase. So it goes.

Remark 4.93. This statement is not true for more general function fields; e.g., we can take $K = \mathbb{C}(t, u)$ as a one-variable function field over $\mathbb{C}(t)$ or $\mathbb{C}(u)$, which induce disjoint sets of places.

We now have the following definition.

Definition 4.94 (Local fields)**.** A *local field* is the metric completion of a global field at some place. Note that local fields are complete automatically.

Example 4.95. By Ostrowski's theorem, we can enumerate our local fields as one of the following.

- Archimedean localizations of number fields: $\mathbb{R}$ or $\mathbb{C}$.
- Nonarchimedean localizations of number fields: finite extensions of $\mathbb{Q}_p$.
- Nonarchimedean localizations of global function fields: finite extensions of $\mathbb{F}_p(t)$.

Warning 4.96. Some authors actively exclude $\mathbb{R}$ and $\mathbb{C}$ from the definition because everyone else in the club is nonarchimedean.

For example, Serre's *Local Fields* often does not say the term "local field" at all.

To extend our definition, we have the following definition.

Definition 4.97. A *complete discretely valued field* is a complete valued field $(K, |\cdot|)$ such that $x \mapsto -\log|x|$ has discrete image. In particular, such a discretely valued field is automatically nonarchimedean because complete archimedean fields are either $\mathbb{R}$ or $\mathbb{C}$.

Example 4.98. All nonarchimedean local fields are complete discretely valued fields.

Example 4.99. Any finite extension of $F((t))$ for any field F is a complete discretely valued field.

Example 4.100. There are some infinite extensions of $\mathbb{Q}_p$ which are complete discretely valued fields.

4.10.3 Topological Field Theory

We have the following statement.

Proposition 4.101. Fix K a finite extension of $\mathbb{Q}_p$ or $F((t))$ for a ground field F. Then $K^\times$ is homeomorphic to $\mathbb{Z} \times \kappa \times U^{(1)}$, where κ is the residue field of K, A is the valuation ring, and $U^{(1)}$ is the kernel of $A^\times \to \kappa^\times$.

Proof. Pick a uniformizer π for the discrete valuation ring A. Then we see that $K^\times \cong A^\times \times \mathbb{Z}$ by the mapping $u\pi^n \mapsto (u, n)$. Indeed, we have exhibited is a isomorphism of the underlying topological groups, and then $A^\times$ is both open and closed in $K^\times$, which induces the isomorphism after slicing $K^\times$ by norm.

Continuing, we have a short exact sequence

$$1 \to U^{(1)} \to A^\times \to \kappa^\times \to 1.$$

We have two cases.

- If κ is finite with q elements, then $x^{q-1} - 1$ will fully split in $\kappa[x]$, so Hensel's lemma promises that $x^{q-1} - 1$ will fully split in A. This induces $q-1$st roots in K, which will successfully split the short exact sequence.
- Otherwise κ is infinite. In this case we must have K be a finite extension of $F((t))$ for some ground field F. Now, we see $F^\times \subseteq A^\times$. Additionally, $F \hookrightarrow K$, so the Cohen structure theorem[4] implies that $A \cong \kappa[[t']]$, so $\kappa \hookrightarrow K$ again has a lift backwards. This splits the short exact sequence.

Lastly, we note that $U^{(1)} = 1 + \mathfrak{p}$, where $\mathfrak{p}$ is the valuation ideal of A, so $U^{(1)}$ is open in $A^\times$ and hence also closed. So we are partitioning $A^\times \cong \kappa^\times \times U^{(1)}$, finishing. ∎

We remark that, in the case that K is a finite extension of $\mathbb{Q}_p$, we have group homomorphisms $\mathfrak{p}^n \to U^{(n)}$ and backwards: forwards is by taking an exponential, and backwards is by taking a log. This is by doing some power series; we won't be more explicit than this.

4.11 November 15

Stuff happens.

4.11.1 Loose Ends

A while ago we showed that, if K is a complete discretely valued prime and $\mathfrak{p} \subseteq A$ is the unique maximal ideal of the valuation ring, then there is a unique prime $\mathfrak{q}$ over $\mathfrak{p}$ in the extension L/K of complete discretely valued fields.

We also remark that our definition of complete discretely valued fields admits the trivial valuation for any field. This is okay with us, for now.

4.11.2 Unramified Extensions

Neukirch also talks about tamely ramified extensions, but we will probably skip it, at least for now. We set K to be a discretely valued field with absolute value $|\cdot|$ and valuation $\nu : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$. We will give it valuation ring A and $\mathfrak{p}$ the valuation ideal and $\kappa := A/\mathfrak{p}$ the residue field. And to make things interesting, we take L/K a finite extension, with $B, \mathfrak{q}, \lambda$ fixed as in the previous sentence; set $w : L \to \mathbb{Q} \cup \{\infty\}$ the corresponding valuation.

Definition 4.102 (Unramified extension)**.** Fix everything as above. We say that L/K is *unramified* if and only if $e(\mathfrak{q}/\mathfrak{p}) = 1$ and λ/κ is a separable extension.

[4] Professor Vojta does not expect us to know what this is.

Remark 4.103. We have that being unramified is equivalent to having $[L : K] = [\lambda : \kappa]$ because we already know $[L : K] = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p})$, given that λ/κ is separable.

We have the following small results.

Proposition 4.104. We have the following.

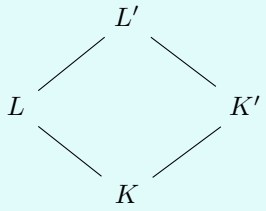
- Fix $M/L/K$ finite extensions. Then M/K is unramified is equivalent to M/L and L/K being unramified.
- A finite Galois extension L/K is unramified if and only if $I_{\mathfrak{q}/\mathfrak{p}} = (1)$.

Proof. We take these one at at time.

- The ramification index condition comes directly from the tower law for e. The separability follows from field theory.
- We have that $I_{\mathfrak{q}/\mathfrak{p}} = (1)$ if and only if L/K unramified because $\#I = e(\mathfrak{q}/\mathfrak{p})$, given that λ/κ is separable. (Namely, $\#I = e(\mathfrak{q}/\mathfrak{p})[L : K]_{\text{sep}}$.). ■

Let's move into something more serious.

Proposition 4.105. Fix the following diagram of fields.



Namely, take K and K' are complete discretely valued fields (such that K'/K have compatible absolute values) with L/K algebraic and $L' = LK'$. Then if L/K is finite and unramified, then L'/K' is finite and unramified.

Proof. The finiteness of L'/K' follows from the finiteness of L/K and some field theory I guess. So now take L'/K' finite and unramified; fix $A', \mathfrak{p}', \kappa'$ and $B', \mathfrak{q}', \lambda'$ to be what they should be for K' and L'.

Now, fix $\overline{\alpha}$ a primitive element for the extension λ/κ; lifting it to some $\alpha \in B$ somehow, so fix f as the irreducible polynomial for α. It follows that f is monic because K is complete, using the strong form of Gauss's lemma for complete nonarchimedean fields. Reducing, we take $\overline{f} \in \kappa[x]$ so that $\overline{f}(\overline{\alpha}) = 0$. Now,

$$\deg \overline{f} = \deg f \le [L : K] = [\lambda : \kappa] = [\kappa(\overline{\alpha}) : \kappa] \le \deg \overline{f},$$

where the last inequality holds because $\overline{\alpha}$ is a primitive element for λ/κ, and $\overline{f}$ vanishes on $\overline{\alpha}$ (though we do not know yet if it is irreducible). So we get that $\deg f = [L : K]$ and so $L = K(\alpha)$; additionally, we see that $\overline{f} \in \kappa[x]$ is irreducible due to the equality case.

We also see that $L'(\alpha) = LK'(\alpha) = K'(\alpha)$, so set $g \in A'[x]$ to be the irreducible polynomial for α over K'. Now, $\overline{g} \mid \overline{f}$, so $\overline{g}$ is separable. Additionally, $\overline{g}$ is irreducible, for otherwise when we factor it into irreducible factors in $\kappa'[x]$, we could lift it via Hensel to a factorization in $K'[x]$. So

$$[\lambda' : \kappa'] \le [L' : K'] = \deg g = \deg \overline{g} = [\kappa'(\alpha) : \kappa'] \le [\lambda' : \kappa'].$$

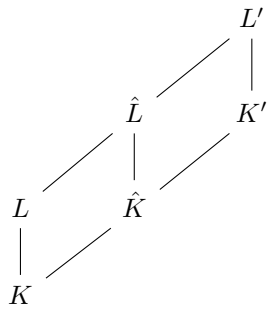
So we get equalities all the way down, meaning that $[\lambda' : \kappa'] = [L' : K']$, and $\lambda' = \kappa'(\alpha)$ is generated by a separable element, so we do indeed see that L'/K' is unramified. ■

Proposition 4.106. Fix K a global field (or a function field in one variable with constant field inside of the valuation ring). Now take K'/K an extension complete with respect to a valuation $\nu_{\mathfrak{p}} : K \to \mathbb{Z}$ for some nonzero prime $\mathfrak{p}$ of A so that we can take $(K', |\cdot|_{\mathfrak{p}})$ a complete discretely valued field.

Further, we take L/K a finite extension with B the integral closure of A in L; take $\mathfrak{q}$ a prime of B lying over $\mathfrak{p}$ with $\mathfrak{q}/\mathfrak{p}$ unramified. Then, $L' = K'L$ is unramified over K'.

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

Proof. We build the following diagram, where $\hat{K}$ and $\hat{L}$ are the completions of $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathfrak{q}}$ respectively.



The point is that $\hat{L}/\hat{K}$ is unramified, essentially by just looking at our local picture, which makes L'/K' unramified by Proposition 4.105. ■

The converse of this statement is also true.

Proposition 4.107. For an extension of global fields L/K in the $AKLB$ set-up, then upon taking $\hat{L}$ the completion of $|\cdot|_{\mathfrak{q}}$ for some prime $\mathfrak{q}$ of B above $\mathfrak{p}$ in A, we also take $\hat{K}$ the completion of K with respect to $|\cdot|_{\mathfrak{p}}$, we claim that $\mathfrak{q}$ is unramified over $\mathfrak{p}$.

Proof. The residue fields of $\hat{K}$ and $\hat{L}$ become the residue fields for L and K, and the ramification indices match as well. So all the data matches as needed. ■

4.11.3 Bigger Unramified Extensions

Let's return to complete fields.

Corollary 4.108. Finite unramified extensions form a distinguished class of extensions, where we borrow the notion from Lang's *Algebra*. In particular, the composite of finite unramified extensions is also finite unramified.

Proof. Being a distinguished class essentially means preserved under towers and liftings, all of which we have discussed already (e.g., see Proposition 4.105). ■

This gives us the following definitin.

Definition 4.109 (Unramified, II)**.** Fix L/K an algebraic extensions of complete discretely valued fields. Then L/K is unramified if and only if all of its finite subextensions are unramified.

Now that this makes sense even for finite unramified extensions because we know that subextensions are unramified when the bigger extension is unramified.

With this notion, we get to talk about the following.

Corollary 4.110. Any finite algebraic extension L/K of complete discretely valued fields has a largest unramified subextension, equal to the composite of all finite unramified extensions.

Proof. Continually lift with Proposition 4.105 until we are done by transfinite induction. ■

So this gives us the following definition.

Definition 4.111. We define K^{unram} to be the largest unramified extension of $\overline{K}/K$, where $\overline{K}$ is the algebraic closure.

Note that even infinite unramified subextensions of $\overline{K}$ will be contained in K^{unram} because all their finite subextensions will be contained in K^{unram}.

Anyways, we hvae the following proposition.

Proposition 4.112. Fix L/K an algebraic extension with T/K the largest unramified extension. Fixing κ, λ, τ the residue fields of K, L, T as one would expect, we have that τ is the separable closure of κ in λ, as in the following diagram.

$$\begin{array}{c} \lambda \\ \Big| \text{ purely insep} \\ \tau \\ \Big| \text{ sep} \\ \kappa \end{array}$$

Proof. Well, fix κ' the separable closure of κ in λ. We see that $\tau \subseteq \kappa'$ because τ is generated by the residue fields of finite unramified subextensions of L/K, and all of these residue fields are separable over κ by definition of unramified. Explicitly, given $\overline{\alpha} \in \tau$, we can lift $\overline{\alpha}$ to some $\alpha \in L$, but then $K(\alpha)$ will be unramified over K, so $\kappa(\overline{\alpha})/\kappa$ will be a separable extension, so $\overline{\alpha} \in \kappa'$.

For the other direction, we reverse the steps. Fix $\overline{\alpha} \in \kappa'$ and take $\overline{f}$ the irreducible polynomial for $\overline{\alpha}$ over κ. Then, lifting $\overline{f}$ to a monic polynomial

$$f \in A[x].$$

Irreducibility of $\overline{f}$ induces irreducibility of f, and Hensel's lemma promises a root $\alpha \in L$ which reduces to $\overline{\alpha} \in \lambda$, due to the separability of f (see Newton's method or something). But now we can check

$$[\kappa(\alpha) : \kappa] = \deg \overline{f} = \deg f = [K(\alpha) : K]$$

with $\kappa(\alpha)/\kappa$ unramified. It follows that $K(\alpha)$ is unramified over K, so $\alpha \in T$, so $\overline{\alpha} \in \tau$. This finishes. ■

4.12 November 17

Here we go.

4.12.1 Unramified Extensions

For today, we will continue to take K a complete discretely valued field, with A its valuation ring, $\mathfrak{p}$ its valuation ideal, and κ its residue field. Then we will also have L/K an algebraic extension (not necessarily finite), with $B, \mathfrak{q}, \lambda$ as one might expect.

Proposition 4.113. Fix λ_0 a separable extension of κ. Then there exists an unramified algebraic extension L/K with residue field isomorphic to λ_0. In fact, this L is unique: given L_1 and L_2 satisfying, there is a unique pair (f, φ) of isomorphisms $f : L_1 \to L_2$ and $\varphi : \lambda_1 \to \lambda_2$, commuting.

Proof. We proceed in steps.

- We start by taking $[\lambda_0 : \kappa] < \infty$, and show that L/K exists. Then there is some $\overline{\alpha} \in \lambda_0$ such that $\lambda_0 \cong \kappa(\overline{\alpha})$, which we we lift by hand to $L := K(\alpha)$. Now we see that $[L : K] = [\lambda_0 : \kappa]$ using our arguments from last class, so L/K is indeed unramified.
- We still take $[\lambda_0 : \kappa] < \infty$, and now we show the uniqueness. Now suppose L_2 and L_2 are two extensions satisfying the needed result. Well, take $\overline{\alpha} \in \lambda_0$ with $\lambda_0 = \kappa(\overline{\alpha})$.

  Then we can lift $\overline{\alpha}$ to $\alpha_1 \in L_1$ and $\alpha_2 \in L_2$ such that $L_1 = K(\alpha_1)$ and $L_2 = K(\alpha_2)$ with irreducible polynomial p. Now we see that

$$L_1 \cong \frac{K[x]}{(p)} \cong L_2$$

  are K-algebra isomorphisms; further, the residue fields under the compatible isomorphism have

$$\lambda_1 \cong \frac{\kappa[x]}{(\overline{p})} \cong \lambda_2.$$

  This isomorphisms are unique because α_1 must get sent to α_2 (they are both roots of p reducing to $\overline{\alpha}$) and $\overline{\alpha_1}$ must get sent to $\overline{\alpha_2}$ (through λ_0, I think) for reasons which are unclear to me.
- For the case of infinite algebraic extensions, throw Zorn's lemma at the problem. ∎

Example 4.114. We have that $\mathbb{Q}_p^{\text{unram}}$ has residue field $\overline{\mathbb{F}_p}$ has the same value group as $\mathbb{Q}_p$. We have that $\mathbb{F}_p((t))^{\text{unram}}$ has residue field $\overline{\mathbb{F}_p}$ has the same value group as $\mathbb{F}_p((t))$.

We have the following corollary.

Corollary 4.115. Take κ finite and n a positive integer. Then there exists exactly one unramified extension of K of degree n.

Proof. The corresponding unramified extension will have residue field of size $(\#\kappa)^n$, of which there is only one field. ∎

Example 4.116. The above corollary includes all nonarchimedean local fields.

4.12.2 Totally Ramified Extensions

We are interested in finite extensions with separable residue fields, such as with number fields. We have the following lemma.

Lemma 4.117 (Krasner's)**.** Fix K a complete discrete valued field. Fix $\alpha, \beta \in \overline{K}$ such that α is separable over K and $|\beta - \alpha| < |\alpha' - \alpha|$ for each Galois conjugate α' of α not equal to α. Then it follows $\alpha \in K(\beta)$.

Remark 4.118. In the condition, we say that α belongs to β.

Proof. By the strong triangle inequality, we observe that $|\alpha' - \beta| = |\alpha - \beta|$ for each Galois conjugate $\alpha' \neq \alpha$, so the strong triangle inequality again gives $|\beta - \alpha| < |\beta - \alpha'|$.

Now, fix $\sigma \in \mathrm{Gal}(\overline{K}/K(\beta))$. Then

$$|\beta - \sigma\alpha| = |\sigma(\beta - \alpha)| = |\beta - \alpha| < |\beta - \alpha'|$$

for each Galois conjugate $\alpha' \neq \alpha$. (That $|\sigma(\beta - \alpha)| = |\beta - \alpha|$ holds because the absolute value must extend properly and uniquely over isomorphic algebraic extensions, and $K(\alpha - \beta) \cong K(\sigma(\alpha - \beta))$.) Thus, $\sigma\alpha = \alpha$ is forced. So because α is separable over $K(\beta)$, we get $\alpha \in K(\beta)$ by Galois theory. ■

So now take L/K a finite extension with λ/κ separable. Setting T to be the largest unramified intermediate extension of L/K. Then it happens that the residue field τ of T will be equal to λ, making L/T a totally ramified extension, as in the following definition.

Definition 4.119 (Total ramified)**.** An extension of complete discretely valued fields L/K is *totally ramified* if and only if $f(\mathfrak{q}/\mathfrak{p}) = 1$ and $e(\mathfrak{q}/\mathfrak{p}) = [L : K]$.

Indeed, the given extension is totally unramified by checking the tower law, I think: T is supposed to absorb all of the inertial degree, for if there is any inertial degree in L/T, then we could find an unramified extension of the required degree to kill that inertial degree.

So now we are interested in totally ramified extensions. Reset L/K to be a totally ramified extension, and take $\pi \in L$ to be a uniformizer for B. Let v and w be the (discrete) valuations of K and L, and we will force $v(K^\times) = \mathbb{Z}$ and $w|_K = v$ to restrict properly, implying $v(L^\times) = \frac{1}{e}\mathbb{Z}$. Now, fix

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + x^n \in A[x]$$

to be the monic irreducible for π. We note that each $a_\bullet$ lives in $\mathfrak{p}$ because these coefficients are elementary symmetric polynomials in the conjugates of π, which must all live in $\mathfrak{q}$, so $a_\bullet \in \mathfrak{q} \cap L = \mathfrak{p}$.

Further, we see that $a_0 \notin \mathfrak{p}^2$ because $v(a_0) = v(\mathrm{N}_K^{K(\pi)}\pi) = [K(\pi) : K]/e$, but $[K(\pi) : K] \leq [L : K] = e$ while $v(a_0) \in \mathbb{Z}$, which gives $L = K(\pi)$ and $v(a_0) = 1$. In particular, f is an Eisenstein polynomial, I guess.

Anyways, we have the following corollary.

Corollary 4.120 (Krasner)**.** Fix $f \in K[x]$ to be a separable, monic irreducible polynomial. Then any $g \in K[x]$ coefficient-wise sufficiently close to f will have the following.

- g is irreducible and separable.
- For each root $\alpha \in \overline{K}$ of f, there is a root $\beta \in \overline{K}$ of g such that $\beta \in K(\alpha)$, a condition which comes from Krasner's lemma. In fact, $K(\alpha) = K(\beta)$.

Proof. By multiplying f through with a sufficiently large constant, we may force $f \in A[x]$ so that sufficiently close g will have $g \in A[x]$. Fix α a root of f. Then $f'(\alpha) \neq 0$ because f is separable, so any g sufficiently close will have

$$|g(\alpha)| < |f'(\alpha)|^2 = |g'(\alpha)|^2.$$

In particular, the sufficiently close can push $|g(\alpha)|$ arbitrarily small and $f'(\alpha)$ componentwise equal to $g'(\alpha)$ in sizes.

Thus, Hensel's lemma promises a root $\beta \in K(\alpha)$ kind of close to α. In particular, for sufficiently close to g,

$$|g(\alpha)| < |f'(\alpha) \cdot \min\{|\alpha' - \alpha|\},$$

where the minimum is taken under all Galois conjugates $\alpha' \neq \alpha$. So Krasner's lemma gives $\alpha \in K(\beta)$, giving $K(\alpha) = K(\beta)$.

To finish, we note that g is irreducible because f is irreducible—they are both monic of the same degree, so $K(\alpha) = K(\beta)$ forces g irreducible. And g is separable by sending g close enough for the above roots promised by Hensel to be necessarily distinct. ■

Anyways, we have the following definition, which we will use later.

Definition 4.121 (p-adic Field)**.** A p-adic field is a finite extension of $\mathbb{Q}_p$.

In particular the above corollary gives the following.

Corollary 4.122. Fix K a p-adic field. Then the following are true.

- Given an $e > 0$, there are only finitely many totally ramified extensions of K of degree e up to isomorphism.
- Given an $n > 0$, there are only finitely many extensions of K of degree n.

Proof. We leave the proof as an exercise. The main point is that (a) comes from compactness of $\mathfrak{p}^{e-1} \times (\mathfrak{p} \setminus \mathfrak{p}^2)$, and (b) follows because any extension can be decomposed into an unramified extension and a totally ramified extension, both of which we know there are finitely many options. ■

Theme 5
Studying Global Places

5.1 November 19

I was not present for class today because I was stuck in Walgreens getting my flu shot. The following notes were transcribed from Austin Lei's notes, so please thank him for the content and blame me for any typos or other errors.

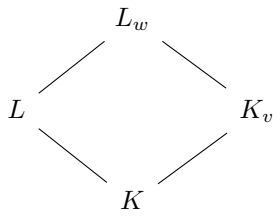
5.1.1 Lifting Places

As usual, we fix K a number field or function field in one variable over a fixed ground field F. (Notably, K need not be global—$\mathbb{Q}(t)$ is permissable.) As in our $AKLB$ set-up for function fields, we will assume that the integer ring A contains the constant field F when K is a function field. In particular, all places are trivial on F.

So let's start building our $AKLB$ set-up here. Fix L/K a finite extension (not necessarily separable) and v a (possible archimedean) place of K, and find some place w of L extending v.

Definition 5.1 (Extending places)**.** Fix L/K as above. Then we say that w *divides* v, and we will notate this by $w \mid v$.

Anyways, we are able to set up the following diagram of field extensions.



We showed a while ago that L_w is indeed the composite LK_v, or at least isomorphic to it.

Continuing our set-up, we fix A the integer ring in K. When K is a number field, this means $\mathcal{O}_K$, and when K is a function field in one variable over a constant field F, we will set $K = F(t)$ for any F-transcendental element $t \in K$ and then fix A to be the integral closure of $F[t]$ or $F[1/t]$ in K.

Now let's discuss our place v a bit more finely.

- In the case where v is nonarchimedean, we are assuming that v is being induced by a nonzero prime ideal of our integer ring A. This is a fact (generalized Ostrowski's theorem) for number fields, and I think it's also true more generally for our function fields.

- If v is archimedean, then we are restricting ourselves to the case where K is a number field. Because the only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$, we must have $K_v \cong \mathbb{R}$ or $K_v \cong \mathbb{C}$, where the absolute value associated to v comes from $\mathbb{R}$ or $\mathbb{C}$, respectively.

This second case can be dealt with quickly.

Proposition 5.2. Fix L/K as above and v an archimedean place. Then v (and w) is induced by restricting $|\cdot|_{\mathbb{R}}$ or $|\cdot|_{\mathbb{C}}$ from an embedding $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$.

Proof. As described above, we have $K_v \cong \mathbb{R}$ or $K_v \cong \mathbb{C}$. Choosing appropriately, we essentially get an embedding

$$K \hookrightarrow K_v,$$

so the behavior of v on K is simply its behavior on K_v (which is either $\mathbb{R}$ or $\mathbb{C}$) properly restricted. This is what we wanted. ■

We would like to generalize this for nonarchimedean places. In particular, we have the following.

Theorem 5.3 (Extension)**.** Fix L/K as above and v a place (not necessarily archimedean). Then we have the following.

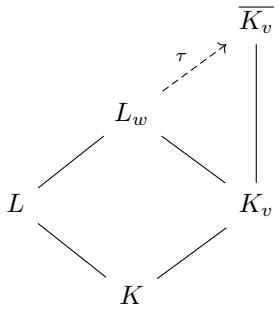
(a) We can induce w as $\overline{v} \circ \tau$ where $\tau : L \hookrightarrow \overline{K_v}$ is some embedding into the algebraic closure of K_v. Here, $\overline{v}$ is the unique extension of v from K_v to the algebraic extension $\overline{K_v}/K_v$.

(b) Two embeddings $\tau_1, \tau_2 : L \hookrightarrow \overline{K_v}$ induce the same place w if and only if they are conjugate. Explicitly, τ_1 and τ_2 are conjugate if and only if there is some $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$ such that $\tau_1 = \sigma\tau_2$.

Proof. We take these one at a time.

(a) Fix w an extension of v to L so that we have a canonical map $K_v \hookrightarrow L_w$ by, say, the universal property of K_v. (Namely, $K \subseteq L \hookrightarrow L_w$ where the metrics cohere, and L_w is complete.)

Now, $L_w = LK_v$ is a finite extensions of K_v, and in particular it will be an algebraic extensions, so fix some embedding $\tau : L_w \hookrightarrow \overline{K_v}$ fixing K_v. This gives the following diagram.



Now, by the uniqueness of extension of the absolute value of complete discretely valued fields, the unique valuation on $\overline{K_v}$ must cohere back with the absolute value in L_w. Namely, for any $\alpha \in L_w$, we have $|\alpha|_w = |\tau\alpha|_{\overline{v}}$, where $|\cdot|_{\overline{v}} : \overline{K_v} \to \mathbb{R}$.

So we see that our chosen embedding $\tau : L_w \hookrightarrow \overline{K_v}$ provides us with some $\tau|_L : L \hookrightarrow \overline{K_v}$ such that the $w = \overline{v} \circ \tau$.

(b) In one direction, suppose that $\tau_1, \tau_2 : L \hookrightarrow \overline{K_v}$ are conjugate so that there is $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$ such that $\tau_1 = \sigma\tau_2\sigma^{-1}$. But we know that

$$|\sigma\alpha|_{\overline{v}} = |\alpha|_{\overline{v}}$$

because automorphisms will preserve the absolute value.[1] So indeed, we find that

$$|\tau_1\alpha|_{\overline{v}} = |\sigma\tau_2\alpha|_{\overline{v}}.$$

In the other direction, suppose that $\tau_1, \tau_2 : L \hookrightarrow \overline{K_v}$ induce the same place of L. Now, we build the following diagram.

$$\begin{array}{ccc} \overline{K_v} & & \overline{K_v} \\ \cup\mathrm{I} & & \cup\mathrm{I} \\ \tau_1(L) & \xrightarrow[\tau_2\circ\tau_1^{-1}]{} & \tau_2(L) \end{array}$$

In particular, we see that we are interested in the map $\sigma := \tau_2 \circ \tau_1^{-1}$. Because our embeddings are preserving our absolute values, we see that σ is a continuous map, where the topologies are induced by $\overline{K_v}$. So we can extend σ to a continuous map

$$\sigma : \overline{\tau_1(L)} \to \overline{\tau_2(L)},$$

where the overline denotes the topological closures. But $\overline{\tau_\bullet(L)}$ is essentially isomorphic to the metric completion of L with respect to the induced placce, so we get that $\overline{\tau_\bullet(L)} = \tau_\bullet(L)K_v$. Continuing up to the algebraic closure, we can extend σ to a map $\overline{K_v} \to \overline{K_v}$.

Continuing, σ is trivial on K because the original embeddings $\tau_\bullet$ cohere on K, so because σ is continuous, σ will be trivial on K_v because K is desnse in K_v. So σ, trivial on K_v, is really an element of $\mathrm{Gal}(\overline{K_v}/K_v)$. So indeed, $\tau_1 = \sigma\tau_2$, finishing. ■

5.1.2 Applcations of Lifting

This gives the following nice version of Dedekind–Kummer.

Proposition 5.4 (Dedekind–Kummer)**.** Fix L/K as before and v a place of K. Further assume that there exists $\alpha \in L$ such that $L = K(\alpha)$, and fix $f \in K[x]$ the monic irreducible polynomial for α. Then, factoring f into $K_v[x]$ as

$$f = \prod_{k=1}^{r} f_k^{e_k},$$

there is a natural bijection between places w over v and monic irreducible polynomials in $K_v[x]$.

Proof. The bijection is actually only natural up to our α chosen in advance. Indeed, there is a bijection

$$\{\tau : L \hookrightarrow \overline{K_v} \text{ fixing } K\} \to \{\beta \in \overline{K_v} : f(\beta) = 0\}$$

by taking $\tau \mapsto \tau\alpha$. Indeed, because $L = K(\alpha)$, the behavior of τ on α will uniquely determine the entire embedding, and τ is allowed to send α to exactly any of the roots.

Now, two embeddings τ_1 and τ_2 induce the same place w over v if and only if they are conjugate over K_v. But the corresponding roots $\tau_1\alpha$ and $\tau_2\alpha$ are also going to be in the same irreducible factor $f_\bullet$ of f if and only if there is an automorphism $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$ such that $\sigma\tau_1\alpha = \tau_2\alpha$, which still implies (and is equivalent to) $\tau_1 = \sigma \circ \tau_2$, so they are conjguate.

So modding out the set of embeddings $\tau : L \hookrightarrow \overline{K_v}$ fixing K gives a set in bijection with the places w over v. And on the other side this modding creates equivalence classes of roots which correspond to the monic irreducibles in the factorization. This is what we wanted. ■

[1] I think this is because K_v is complete: viewing $\overline{K_v}$ as a colimit of finite extensions, there is exactly one way to extend v to any finite extensions of K_v, so the two valuations $\alpha \mapsto |\alpha|_{\overline{v}}$ and $\alpha \mapsto |\sigma\alpha|_{\overline{v}}$ must coincide.

Remark 5.5. This statement is intended to generalize the Dedekind–Kummer theorem, which applied to (finite) prime-splitting and only worked when the (finite) prime was coprime to the conductor of $A[\alpha]$. I am under the impression that factorization in K_v for finite places v is done by factoring modulo the prime and then lifting the factorization via Hensel, so roughly the same hard computations (e.g., factoring over a finite field) are required.

Example 5.6. Fix K a number field, and we study the places extending ∞ of $\mathbb{Q}$. Fixing some α such that $K = \mathbb{Q}(\alpha)$ with monic irreducible f, we see that the factorization of f in $\mathbb{Q}_\infty = \mathbb{R}$ will be into one quadratic for each pair of complex conjugate roots of f and one linear factor for each real root. Each complex conjugate pair does indeed induce exactly one embedding $K \hookrightarrow \mathbb{C}$, and each linear root will induce exactly one embedding $K \hookrightarrow \mathbb{R}$.

Anyways, let's get back to theory. We have the following generalization of the fundamental identity to places.

Proposition 5.7. Fix L/K as before with v a place, and further assume that L/K is separable. Then

$$[L : K] = \sum_{w|v} [L_w : K_v].$$

Proof. Because L/K is finite and separable, we may find $\alpha \in L$ such that $L = K(\alpha)$ and apply our upgrade of Dedekind–Kummer above. Now, taking f the irreducible monic polynomial for α, we see that L/K being separable implies f will fully split into distinct linear factors in $\overline{K}$. So f will fully split into distinct linear factors in $\overline{K_v}$ (by tracking an embedding $\overline{K} \hookrightarrow \overline{K_v}$ induced by the universal property of $\overline{K}$).

In particular, factoring $f = \prod_{k=1}^{r} f_k$ in $K_v[x]$ has all exponents equal to 1, so

$$[L : K] = \deg f = \sum_{k=1}^{r} \deg f_k = \sum_{k=1}^{r} [L_w : K_v],$$

where $\deg f_k = [L_w : K_v]$ because $L_w = K_v L = K_v K(\tau\alpha) = K_v(\tau\alpha)$. Here, the τ has w chosen as the place in the bijection of the extension of Dedekind–Kummer above so that $\deg f_k$ will match up with $[K_v(\tau\alpha) : K_v]$. Anyways, this finishes. ∎

Also, we can now finally classify extensions of nonarchimedean extensions.

Proposition 5.8. Fix L/K as before and v a nonarchimedean place corresponding to a prime $\mathfrak{p}$ of A. Then any extension w of v to L is induced by some prime $\mathfrak{q}$ of B lying over $\mathfrak{p}$.

Proof. As in the extension theorem, we may induce w by some embedding $\tau : L \hookrightarrow \overline{K_v}$ fixing K. Now, the needed prime ideal is

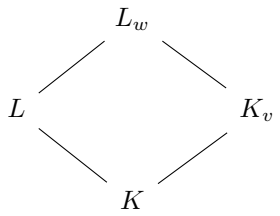
$$\mathfrak{q} := \{\beta \in B : |\tau\beta|_{\overline{v}} < 1\}.$$

We will discuss the primality of $\mathfrak{q}$ momentarily, but we do note that this is indeed the valuation ideal for a place, so it should work.

Now, $\mathfrak{q}$ is the pull-back of the valuation ideal in $\overline{K_v}$, which is certainly prime there, and pull-backs of primes are prime. We are kind of implicitly using that $\tau(B)$ will be in the valuation ring of $\overline{K_v}$, which is true because any $\beta \in B$ is integral over A, so $\tau\beta$ is integral over $\tau(A)$, and $\tau(A)$ is certainly contained in the valuation ring of K_v. ∎

5.2 November 22

For today, we continue to let K be a number field or a function field in one variable over a fixed constant field F. Then we have v a place of K upon which v is trivial. We also take L/K to be a finite extension, where w extends v. This gives the following diagram.



We see that $LK_v = L_w$, so the natural map $L \otimes_K K_v \to L_w$ is an isomorphism because $L \cap K_v = K$, I think.

5.2.1 More Extensions of Valuations

Last time we took L/K to be a separable and achieved

$$[L : K] = \sum_{w|v} [L_w : K_v].$$

Today we show the following.

Proposition 5.9. Take L/K to be separable. Then the map

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

obtained by combining the $L \otimes_K K_v \to L_w$ isomorphisms is in fact an isomorphism of K_v-algebras.

Proof. By separability, we may write $L = K(\alpha)$, and we let $f \in K[x]$ be the irreducible polynomial for α. We can fully factor f as

$$f = \prod_{k=1}^{r} f_r,$$

where f_r are also distinct monic irreducibles in $K_v[x]$. (They are distinct by separability.) Now, the isomorphism $L \cong K[x]/(f)$ becomes

$$L \otimes_K K_v \cong \frac{K_v[x]}{(f)} \cong \prod_{k=1}^{r} \frac{K_v[x]}{(f_r)} \cong \prod_{w|v} L_w.$$

Tracking the isomorphisms through, we are explicitly taking $\alpha \otimes 1$ to $x + (f)$ to $(x + (f_k))_{k=1}^r$ to $(\beta_1, \dots, \beta_r)$, where the $\beta_\bullet$ are a root of $f_\bullet$ in L_w, where the correspondence is explicit from last class. ∎

5.2.2 Local Norms and Traces

Take L/K separable still. Technically, we only need

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

to be an isomorphism, but separability is nice for psychological reasons.

Now fix some $\alpha \in L$. We see that multiplication by α becomes a K-linear map $L \to L$, and so it will induce a K_v-linear map $L \otimes_K K_v \to L \otimes_K K_v$, and in fact we are preserving the multiplication structure in the product

$$L \otimes_K K_v \cong \prod_{w|v} L_w.$$

In particular, multiplication by α corresponds to multiplication by the various $\beta_\bullet$, induced as in the proposition above. This gives us the following definition.

Definition 5.10 (Local norm and trace)**.** Fix everything as in the previous paragraph. Then

$$\mathrm{N}_K^L \alpha := \prod_{w|v} \mathrm{N}_{K_v}^{L_w} \beta_\bullet.$$

We also define

$$\mathrm{T}_K^L \alpha = \sum_{w|v} \mathrm{T}_{K_v}^{L_w} \alpha$$

in essentially the same way.

These correspond to the usual definition of the norm and trace by using the definition of norm that is the determinant of the multiplication map. We discussed above how this multiplication map behaves via the isomorphisms, so the above does indeed work out, I think.

5.2.3 $AKLB$ Set-Up: Function Field Edition

We are going to start chapter 3 today. Our main point is that function fields are easier than number fields because we have access to algebraic geometry for function fields. So one strategy is to try to push these function field ideas back to number fields to prove things.

So let's study function fields. Take X to be a compact Riemann surface, like a torus or something. Fix $\pi : X \to \mathbb{C}$ be some nonconstant meromorphic function on X. Viewing $\mathbb{C}$ as a subset of the Riemann sphere $\mathbb{CP}^1$ (as $\mathbb{C} \cup \{\infty\}$). If π has a pole at some point $p \in X$, then $\frac{1}{\pi}$ has a removable singularity at p, which just turns into a zero. The point is that π extends to a holomorphic map

$$\pi : X \to \mathbb{CP}^1.$$

We have the following statement.

Proposition 5.11. We define

$$K := \{\text{meromorphic functions } f : \mathbb{CP}^1 \to \mathbb{C}\}.$$

Here K is a field, and in fact it is $\mathbb{C}(z)$, where $\mathbb{C}$ is identified with our constant functions, and z is identified with reversing the natural embedding $\mathbb{C} \hookrightarrow \mathbb{CP}^1$.

Proof. Fix $f : \mathbb{C} \to \mathbb{C}$ some meromorphic function. Then we may multiply out the roots via some finite polynomial $\prod_\bullet (z - \zeta_\bullet)^{n_\bullet}$ which extends to a holomorphic function on $\mathbb{C}$. In particular, our new function as a pole at ∞ of finite order (holomorphic functions only have finitely many roots), so it is a polynomial $g \in \mathbb{C}[z]$ so that

$$f = \frac{g}{\prod_\bullet (z - \zeta_\bullet)^{n_\bullet}} \in \mathbb{C}(z).$$

Of course, the converse is also true: anyone in $\mathbb{C}(z)$ will give a meromorphic function $\mathbb{CP}^1 \to \mathbb{C}$. ∎

Remark 5.12. By doing the extending process described above, we get

$$K = \{\text{holomorphic functions} \mathbb{CP}^1 \to \mathbb{CP}^1\}.$$

We claimed earlier that we had the following; let's prove it now.

Proposition 5.13. The places of $\mathbb{C}(z)$ which are trivial on $\mathbb{C}$ are in canonical bijection with

$$(\operatorname{Spec} \mathbb{C}[z] \setminus \{0\}) \cup (\operatorname{Spec} \mathbb{C}[1/z] \setminus \{0\}).$$

Proof. Let's prove this. In particular, any absolute value $|\cdot|$ on $\mathbb{C}[z]$ trivial on $\mathbb{C}$ will necessarily have $|z| \le 1$ or $|1/z| \le 1$, so either $\mathbb{C}[z]$ or $\mathbb{C}[1/z]$ is in the valuation ring. We also remark that $|\cdot|$ is trivial on $\mathbb{C}$ and hence trivial on $\mathbb{Z}$, so $|\cdot|$ is nonarchimedean.

Remark 5.14. The above union is not disjoint because $\mathbb{C}[z]$ and $\mathbb{C}[1/z]$ will both localize to $\mathbb{C}[z, 1/z]$.

We now just take our cases one at a time.

- If $\mathbb{C}[z]$ is in the valuation ring A of $|\cdot|$, then $\{\alpha \in K : |\alpha| < 1\} \subseteq A$ pulls back to a prime ideal $\mathfrak{p}$ of $\mathbb{C}[z]$, notably not everything because $\mathbb{C}$ is excluded.

  We would like this prime ideal to be nonzero; well, $|\cdot|$ is nontrivial, so there is some $\alpha \in \mathbb{C}(z)^\times$ suc that $|\alpha| \neq 1$. Without loss of generality, we take $|\alpha| < 1$. But now setting $\alpha = f/g$ with $f, g \in \mathbb{C}[z]$, we find that $|g| \le 1$ because $|z| \le 1$ and $|\cdot|$ is trivial on $\mathbb{C}$, and so $|f| = |\alpha| \cdot |g| < 1$. So $f \in \mathfrak{p}$ is in our prime ideal.

- The case where $\mathbb{C}[1/z]$ is in the valuation ring is analogous. ∎

We remark that our copies of $\mathbb{C}$ cover the Riemann sphere $\mathbb{CP}^1$ by stereographic projection. There's a nice circular picture, or we can just draw the picture with $\mathbb{C}$ as a line. I'm too lazy to live-TeX this diagram.

Now let's return to X. We set

$$L = \mathcal{K}(X) := \{\text{meromorphic functions } f : X \to \mathbb{C}\}.$$

This is a field because look at it. Now, if we take any $\pi : X \to \mathbb{C}$ meromorphic and lift it up to $\pi : X \to \mathbb{CP}^1$, we see that we get a function induced by π which sends $\mathbb{C}(z) = \mathcal{K}(\mathbb{CP}^1)$ into $\mathcal{K}(X)$ by pre-composition. In fact, this is a ring homomorphism of fields, so it becomes a field homomorphism, so it becomes injective for free.

The point is that, when we let $A = \mathbb{C}[z]$ to be the meromorphic functions $\mathbb{CP}^1 \to \mathbb{C}$ (where we are using the correct copy of $\mathbb{C}$ for our chosen π), then we can look at the integral closure B in L is the set of holomorphic maps $\pi^{-1}\mathbb{C} \to \mathbb{C}$ which extend fully to $X \to \mathbb{C}$. It also happens that L/K is finite, which gives us an $AKLB$ set-up, as follows.

$$\begin{array}{ccc} B & \subseteq & L = \mathcal{K}(X) \\ | & & | \\ A & \subseteq & K = \mathbb{C}(z) \end{array}$$

We will not prove actually prove that we are getting an $AKLB$ set-up because it would take us a bit too far afield.

5.3 November 29

5.3.1 Advertisement: Riemann Surface

We continue to take X to be a connected, compact Riemann surface. We also define

$$L := \mathcal{K}(X) := \operatorname{Hom}_{\text{meromorphic}}(X, \mathbb{C}),$$

which is in fact a field. We also recall that $K := \mathcal{K}(\mathbb{CP}^1) = \mathbb{C}(t)$, where t corresponds to $\mathrm{id} : \mathbb{C} \to \mathbb{C}$, induced by the canonical map $\mathbb{C} \hookrightarrow \mathbb{CP}^1$.

Now, we set

$$A := \mathbb{C}[t] := \{\text{holomorphic maps } \mathbb{C} \to \mathbb{C} \text{ extending to meromorphic } \mathbb{CP}^1 \to \mathbb{C}\},$$

and we set B to be the integral closure of A in L. Given the canonical embedding $X \twoheadrightarrow \mathbb{CP}^1$, we get an $AKLB$ set-up as follows.

$$\begin{array}{ccccc} B & \subseteq & L & & X \\ | & & | & & \downarrow \pi \\ A & \subseteq & K & & \mathbb{CP}^1 \end{array}$$

Note that there is also a "dual" $AKLB$ set-up by setting $A' = \mathbb{C}[1/t]$ and B' the integral closure of A' in L. It is a theorem that these $AKLB$ set-ups give all nontrivial valuations on L which are trivial on $\mathbb{C}$. Roughly speaking, this is because we spent so much time working in general function fields in one variable.

Note that, for each $a \in \mathbb{CP}^1 \setminus \{\infty\}$, we can view $a \in \mathbb{C}$ so that $t - a \in A = \mathbb{C}[t]$, which will lift to an element of B which is holomorphic on $\pi^{-1}(\mathbb{C})$, vanishing at all points of $\pi^{-1}(a)$. For some given $p \in \pi^{-1}(a)$, we let the order of vanishing be $e_p > 0$, and it is true that

$$\sum_{pin\pi^{-1}(a)} e_p = \deg \pi = [L : K]$$

by essentially doing complex analysis. Additionally, the residue field at our $a \in \mathbb{CP}^1$ for given $p \in \pi^{-1}(a)$ is in fact $\mathbb{C}$, for reasons I don't understand, so the inertial degree $f_p$is 1. So we have verified our fundamental identity by hand.

Additionally, by complex analysis/algebraic geometry, it is true that any $x \in \pi^{-1}(\mathbb{C})$ has

$$\mathfrak{q}_x := \{f \in B : f(x) = 0\}$$

is a prime ideal of B (which is not hard to see by checking primality by hand), which provides a bijection between $\pi^{-1}(\mathbb{C})$ and the nonzero primes of B (which is hard to see). Regardless, it is true that

$$(t-a)B = \prod_{p \in \pi^{-1}(a)} \mathfrak{q}_p^{e_p}.$$

And here, the ramification index e_p is actually ramifiaction in the sense of a Riemann surface. Again using our trivial inertial indices, we see that, again, we have

$$[L : K] = \sum_{p \in \pi^{-1}(a)} e_p f_p,$$

which we computed by hand again.

5.3.2 Setting Up Riemann–Roch

Let's start building the machinery for Riemann–Roch. In short, we will be interested in sets of the form

$$\{f \in \mathcal{K}(X) : f \text{ has poles only on } S \text{ of order } \nu_s \in \mathbb{Z} \text{ for each } s \in S\}.$$

The reason we are allowing poles, though with some control, is because holomorphic functions on these sorts of spaces are quite boring. Note that we are allowing the order to be negative, which corresponds to order of vanishing. In other words, given a tuple $\{n_Q\} \in \mathbb{Z}^{\oplus X}$ of integers, we are looking at

$$L(\{n_Q\}_{Q \in X}) = \{f \in \mathcal{K}(X) : \nu_Q(f) \geq -n_Q \text{ for each } Q \in X\}.$$

This set turns into a $\mathbb{C}$-vector space (which we can see by hand) and is finite-dimensional (which is harder to see—roughly speaking, poles induce constraints on the functions).

Example 5.15. Using $X = \mathbb{CP}^1$ with $n_2 = 1$ and $n_5 = 3$ and $n_\infty = 10$ and $n_8 = 9$ and $n_p = 0$ elsewhere, out set consists of functions which have poles of order less than equal to 1 at 2, less than or equal to 3 at 5, a pole of at most 10 at ∞, a zero of order at least 9 at 8, and holomorphic everywhere else.

In particular, any f satisfying these constraints has $f(z-1)(z-5)^3(z-8)^{-9}$ will extend to a holomorphic function (on $\mathbb{C}$) with a pole of order at most $10+1+3-9=5$ at ∞. So we see we it suffices to describe a fifth-degree polynomial, for which there are six dimensions needed.

The point of Riemann–Roch is to approximate the dimensions of these sets we are looking at.

Here is a small example.

Proposition 5.16. Given a tuple $\{n_Q\}_{Q\in X} \in \mathbb{Z}^{\oplus X}$ has

$$\sum_{Q\in X} n_Q < 0,$$

then

$$L(\{n_Q\}_{Q\in X}) = \{0\}.$$

Proof. This is because we have a product formula for $\mathbb{C}(t)$: given $f \neq 0$, we have

$$\sum_{Q\in X} \nu_Q(f) = 0,$$

which holds by complex analysis or our product formula for number fields or similar. The point is that it is impossible to satisfy the given constraints when we have

$$\sum_{Q\in X} \nu_Q(f) \leq \sum_{Q\in X} n_Q < 0.$$

This finishes. ∎

5.3.3 Places of Number Fields

Let's quickly return to number fields.

Definition 5.17 (In/finite places)**.** A place ν of a number field is *finite* if and only if nonarchimedean or *infinite* if and only if nonarchimedean. Finite places are denoted by $\nu \nmid \infty$, and infinite places are denoted by $\nu \mid \infty$, essentially meaning that ν "lies over" the infinite place ∞ of $\mathbb{Q}$.

Definition 5.18 (Real/complex places)**.** An infinite place ν of a number field K is *real* if and only if $K_\nu = \mathbb{R}$ and *complex* if and only if $K_\nu = \mathbb{C}$.

We quickly remark that finite places are neither real nor complex places. Let's start our discussion of extensions.

Definition 5.19 (Infinite inertia/ramification)**.** Fix L/K an extension of number fields. Given v an infinite place of K and w an infinite place of L extending v. Now we set $\kappa(v) := K_v \in \{\mathbb{R}, \mathbb{C}\}$ and define

$$f_{w/v} := [\kappa(w) : \kappa(v)] = [L_w : K_v]$$

and $e_{w/v} := 1$ so that $[L_w : K_v] = e_{w/v} f_{w/v}$, in accordance with the case with finite places.

Warning 5.20. Here Neukirch is forcing $\mathbb{C}/\mathbb{R}$ to be unramified, but other authors prefer this to be ramified.

Definition 5.21 (Norms of places)**.** Fix v a place of a global field K, and we define a *norm* $\|\cdot\|_v$ as follows.

(a) If v is finite, then let $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ be the corresponding valuation ideal. We define $\mathrm{N}(v) := \mathrm{N}(\mathfrak{p})$ to be the absolute norm of $\mathfrak{p}$. Then by convention we will take

$$\|x\|_v := \mathrm{N}(v)^{-\nu_{\mathfrak{p}}(x)}$$

to be an absolute value representing our place v. (Namely, $\mathrm{N}(v) = p^{f_v}$ with $v(p) = e_v$ so that $\|p\|_v = p^{-e_v f_v} = |p|_p^{e_v f_v}$ so that $\|x\|_v = |x|_p^{[K_v:\mathbb{Q}_p]}$.)

(b) For real place v coming from $\rho : K \hookrightarrow \mathbb{R}$, we set $\|x\|_v = |\rho x|$.

(c) For complex places v coming from $\sigma : K \hookrightarrow \mathbb{C}$, we set $\|x\|_v = |\sigma x|^2 = |\overline{\sigma} x|^2$.

In the above set-up with v finite, we note that, setting $p := \operatorname{char} \kappa(v) \in \mathfrak{p}$, we have that K_v is a finite extension of $\mathbb{Q}_p$ of degree $e_v f_v$. Additinoally, by construction, we see that

$$\|x\|_\nu = |x|_p^{[K_\nu:\mathbb{Q}_p]}$$

for any place ν, by construction. Namely, when ν is complex, we want to square here, as we did in the above definition.

Warning 5.22. When v is complex, $\|\cdot\|_\nu$ violates the triangle inequality, so it is not an absolute value. For example, $\|2\| > \|1\| + \|1\|$.

5.4 December 1

Here we go.

5.4.1 Product Formula for Number Fields

We have the following lemma.

Lemma 5.23. Fix L/K an extension of number fields and v a place of K. Then

$$\prod_{\substack{w \in M_L \\ w|v}} \|x\|_w = \|\mathrm{N}_K^L x\|_v$$

for each $x \in L$.

Proof. We simply write

$$\|x\|_w = \|\mathrm{N}_{K_v}^{L_w} x\|_w^{1/[L_w:K_v]}$$

from last class, which becomes $\|\mathrm{N}_{K_v}^{L_w} x\|_v$ by our discussion on extending norms. But now

$$\prod_{w|v} \|x\|_w = \left\| \prod_{w|v} \mathrm{N}_{K_v}^{L_w} x \right\|_v = \|\mathrm{N}_K^L x\|$$

by the fact that local norms multiply to give global norms. ∎

This gives us the following theorem.

Theorem 5.24. Fix K a number field. Then

$$\prod_{v \in M_K} \|x\| = 1$$

for each $x \in K^\times$.

Proof. The key is to use the fact K is lying over $\mathbb{Q}$. Indeed,

$$\prod_{v \in M_K} \|x\|_v = \prod_{p \in M_{\mathbb{Q}}} \prod_{\substack{v \in M_K \\ v|p}} \|x\|_v,$$

which by lemma is equal to

$$\prod_{p \in M_{\mathbb{Q}}} \|\mathrm{N}_{\mathbb{Q}}^K x\|,$$

which we know is equal to 1 because we showed the product formula for $\mathbb{Q}$. ■

Remark 5.25. We can extend this proof to global fields without too much pain, where we reduce to the case of $\mathbb{F}_p[t]$ instead of reducing to $\mathbb{Q}$, but Professor Vojta is worried about inseparable extensions.

Remark 5.26. The product formula is somewhat akin to the fact that the sum of the zeroes and poles is zero for a compact Riemann surface.

5.4.2 Replete Ideals

We have the following definition.

Definition 5.27 (Picard group)**.** Fix K a number field and define $J(\mathcal{O}_K)$ to be the fractional ideals of K and $P(\mathcal{O}_K)$ to be the principal fractional ideals. Then we define the *Picard group of* K to be

$$\mathrm{Pic}(\mathcal{O}_K) = J(\mathcal{O}_K)/P(\mathcal{O}_K) \cong \mathrm{Cl}_K\,.$$

Sometimes we choose to write Pic additively.

The Picard group is not including the infinite places, which would be akin to working over a Riemann surface which is not compact.

Definition 5.28 (Replete ideal)**.** Fix K a number field. A *replete ideal* (i.e., an Arakelov divisor of $\operatorname{Spec} \mathcal{O}_K$) is an element of the group

$$\overline{J}(\mathcal{O}_K) := J(\mathcal{O}_K) \times \prod_{v|\infty} \mathbb{R}_{>0}^\times.$$

We will think $J(\mathcal{O}_K) \subseteq \overline{J}(\mathcal{O}_K)$ by the canonical embedding.

Essentially we are just adding points to $\operatorname{Spec} \mathcal{O}_K$ corresponding to the infinite places. We are allowed to take a Cartesian product in the above definition (instead of a direct sum) because there will only be finitely many infinite places anyways.

Definition 5.29 (Notation for places)**.** Given a number field K, we continue to set M_K to be the set of places of K, but we define

$$M_K^\infty := \{v \in M_K : v \mid \infty\} \qquad \text{and} \qquad M_K^\circ = M_K \setminus M_K^\infty.$$

We note that we have a natural embedding $M_K^\infty \hookrightarrow \overline{J}(\mathcal{O}_K)$.

In fact, we have a nice embedding taking $\mathfrak{p} \in M_K^\infty$ and $\nu \in \mathbb{R}$ to

$$\mathfrak{p}^\nu := \left\{(1), (e^{\nu 1_{\mathfrak{q}=\mathfrak{p}}})_{\mathfrak{q}|\infty}\right\}.$$

The point of saying is that we can write any element of $\overline{J}(\mathcal{O}_K)$ in the form

$$\prod_{\mathfrak{p} \in M_K} \mathfrak{p}^{\nu_\mathfrak{p}}$$

where $\nu_\mathfrak{p}$ is an integer when $\mathfrak{p}$ is finite and real when $\mathfrak{p}$ is infinite, and we also require that all but finitely many of the $\nu_\mathfrak{p}$ vanish.

Remark 5.30. Professor Vojta is unsure if we should instead define

$$\mathfrak{p}^\nu := \left\{(1), (e^{-\nu 1_{\mathfrak{q}=\mathfrak{p}}})_{\mathfrak{q}|\infty}\right\}.$$

We might change this definition for convenience later.

Anyways, this gives us the following definition.

Definition 5.31 (Valuation at a place)**.** For all $a \in K^\times$ and place $v \in M_K$, we define

$$v(\alpha) := \begin{cases} \nu_\mathfrak{p}((a)) & v \in M_K^\circ \text{ belongs to } \mathfrak{p} \nmid \infty, \\ -\log|\tau a| & v \in M_K^\infty \text{ belongs to } \tau : K \hookrightarrow \mathbb{C}. \end{cases}$$

Definition 5.32 (Norm at a place)**.** Fix v a place of a number field K. We define $\mathrm{N}(v)$ to be $\mathrm{N}(\mathfrak{p})$ when v is finite, $\mathrm{N}(v) = e$ when v is real, and $\mathrm{N}(v) = e^2$ when v is complex. This extends multiplicatively to a full map on $\overline{J}(\mathcal{O}_K)$.

This gives us $\|a\|_v = \mathrm{N}(v)^{-\nu(a)}$ for each $a \in K^\times$. Additionally, if $\mathfrak{p} \in M_K$ lies over $p \in M_\mathbb{Q}$ then $\mathrm{N}(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$. This comes out to

$$\mathrm{N}(\mathfrak{p}) = \|\pi\|_v^{-1},$$

where π is a uniformizer of K_v in K when $\mathfrak{p}$ is finite and π is some element such that $|\tau\pi| = \frac{1}{e}$ where $\tau : K \hookrightarrow \mathbb{C}$ corresponds to v.

Definition 5.33 (Principal replete ideal)**.** Fix $a \in K^\times$. Then the *principal replete ideal* of a is defined as

$$[a] := \prod_{\mathfrak{p} \in M_K} \mathfrak{p}^{\nu_\mathfrak{p}(a)}.$$

The set of all principal replete ideals is $\overline{P}(\mathcal{O}_K.)$

Example 5.34. For $K = \mathbb{Q}$, we have $[2] = (2)^{\nu_2(2)} \cdot (\infty)^{\nu_\infty(2)}$ by unwinding all of our definitions. Then

$$\mathrm{N}([2]) = 2^1 \cdot e^{-\log 2} = 2 \cdot \frac{1}{2} = 1$$

by tracking everything through.

We can see that, for a given $a \in K^\times$, we have

$$\mathrm{N}([a]) = \prod \mathfrak{p} \in M_K \, \mathrm{N}(\mathfrak{p})^{\nu_\mathfrak{p}(a)} = \prod \mathfrak{p} \in M_K \|a\|_\mathfrak{p}^{-1} = 1$$

by using the product formula and tracking through the definitions. This gives the following.

Definition 5.35 ($\overline{\mathrm{Pic}}$)**.** We define

$$\overline{\mathrm{Pic}}(\mathcal{O}_K) := \overline{J}(\mathcal{O}_K)/\overline{P}(\mathcal{O}_K).$$

Note that N will descend to a homomorphism on $\overline{\mathrm{Pic}}$. We also define

$$\overline{\mathrm{Div}}(\mathcal{O}_K) = \left(\bigoplus_{\mathfrak{p} \in M_K^\circ} \mathbb{Z} \right) \times \left(\bigoplus_{\mathfrak{p} \in M_K^\infty} \mathbb{R} \right)$$

to be the additive version, and we denote its elements additively.

Note that $\overline{J}(\mathcal{O}_K)$ and $\overline{\mathrm{Div}}(\mathcal{O}_K)$ contain essentially the same data, where

$$\prod_{\mathfrak{p} \in M_K} \mathfrak{p}^{\nu_\mathfrak{p}} \longleftrightarrow \sum_{\mathfrak{p} \in M_K} \nu_\mathfrak{p} \mathfrak{p}.$$

Similarly, an element $a \in K^\times$ will go to $[a]$ of $\overline{J}(\mathcal{O}_K)$ and $\sum_\mathfrak{p} \nu_\mathfrak{p}(a)\mathfrak{p}$ as above.

5.4.3 A Little with Riemann Surfaces

Let's go back to setting X to be a compact Riemann surface, and as usual fix $K := \mathcal{K}(X)$ with B the integral closure of $\mathbb{C}[t]$ in K, where t is some map $\pi : X \to \mathbb{CP}^1$.

Now, when $f \in K^\times$ is a nonzero map where $f : X \to \mathbb{C}$ is a meromorphic map, we define

$$\|f\|_v := e^{-\operatorname{ord}_v(f)},$$

where v is an place of K trivial on $\mathbb{C}$ and in particular belonging to a point of X. Now, we see that the product formula will let us say

$$\sum_{p \in X} \operatorname{ord}_p(f) = 0,$$

so we define our divisor group by

$$\mathrm{Div}(X) := \bigoplus_{p \in X} \mathbb{Z}.$$

More or less, this corresponds to $\overline{\mathrm{Div}}$.

5.5 December 3

The fun continues.

5.5.1 Riemann–Roch

As before, take X beo a compact Riemann surface, and we defined

$$\operatorname{Div}(X) := \mathbb{Z}^{\oplus X}.$$

Elements of $\operatorname{Div}(X)$ are called *divisors*, notated by

$$\sum_{p \in X} n_p p.$$

We have the following definition.

Definition 5.36 (Degree)**.** Fix X a compact Riemann surface. The *degree* of a divisor $D = \sum_p n_p p$ is

$$\deg D := \sum_p n_p.$$

Note that

$$\deg : \operatorname{Div}(X) \to \mathbb{Z}$$

is a homomorphism, well-defined because all but finitely many of the coordinates of $\operatorname{Div}(X)$ vanish. We also define

$$H^0(X, \mathcal{O}(D)) := \{f \in \mathcal{K}(X) : \operatorname{ord}_p f \geq -n_p \text{ for each } p \in X\},$$

which is a finite-dimensional $\mathbb{C}$-vector space. Here the $-$ in $-n_p$ is present in order to expand the set when n_p increases.

The Riemann–Roch theorem gives us a little information on the dimension of $H^0(X, \mathcal{O}(D))$ in terms of $\deg D$.

Theorem 5.37 (Riemann–Roch)**.** Fix X a compact Riemann surface. There exists a canonical divisor class K such that

$$\dim H^0(X, \mathcal{O}(D)) - \dim H^0(X, \mathcal{O}(K - D)) = \deg D + 1 - g,$$

where g is the genus of X.

We will not prove this because it will take us a bit far afield.

For number fields, we have the following.

Definition 5.38 ($H^0(\operatorname{Spec} \mathcal{O}_K, \mathcal{O}(D))$)**.** Fix K a number field and $D = \sum_{\mathfrak{p} \in M_K} \nu_{\mathfrak{p}} \mathfrak{p} \in \overline{\operatorname{Div}}(\mathcal{O}_K)$ a divisor. Then we define

$$H^0(\operatorname{Spec} \mathcal{O}_K, \mathcal{O}(D)) = \left\{x \in K : \|x\|_{\mathfrak{p}} \leq \mathrm{N}(\mathfrak{p})^{\nu_{\mathfrak{p}}} \text{ for each } \mathfrak{p} \in M_O\right\}.$$

This is a finite set.

Note that we can equivalently write the above as

$$\left\{x \in \prod_{\mathfrak{p} \in M_K^\circ} \mathfrak{p}^{-\nu_{\mathfrak{p}}} : \|x\|_v \leq e^{\nu_v} \text{ for each } v \in M_K^\infty\right\},$$

which is a bounded region of a lattice in Minkowski space, so indeed this set is finite. I cannot really be bothered to check that all the signs go through, but they are supposed to; one can sanity-check that larger values of $\nu_{\mathfrak{p}}$ will give a larger set.

Minkowski's theorem on lattices is able to force large $\deg D$ to have

$$H^0(\operatorname{Spec} \mathcal{O}_K, \mathcal{O}(D)) \neq \{0\}$$

by placing a lattice point in our lattice. We also remark that $\deg D < 0$ will force $H^0(\operatorname{Spec} \mathcal{O}_K, \mathcal{O}(D)) = \{0\}$ by the product formula.

Remark 5.39. One can imagine using something akin to the Gauss circle problem to get an asymptotic for $H^0(\operatorname{Spec} \mathcal{O}_K, \mathcal{O}(D))$. We will not do this because I don't know what's happening anymore.

5.5.2 The Different Ideal

Let's go back to doing algebraic number theory. Fix an $AKLB$ set-up with L/K separable with separable residue field extensions. The separability of L/K tells us that T_K^L is nonzero (and in fact this is equivalent), so the corresponding symmetric bilinear form $\langle \alpha, \beta \rangle \mapsto \mathrm{T}_K^L(\alpha\beta)$ is nonzero.

To define the relative discriminant, we have the following definition.

Definition 5.40 (Dual module)**.** Fix $\mathfrak{b}$ a finitely generated full A-submodule of L. (Most of the time we will take $\mathfrak{b}$ to be a fractional ideal.) Then we define the *dual module of* $\mathfrak{b}$ by

$$\mathfrak{b}^* := \left\{ x \in L : \mathrm{T}_K^L(x\mathfrak{b}) \subseteq A \right\}.$$

We pick up the following lemma.

Lemma 5.41. Fix $\mathfrak{b}$ a (nonzero) fractional ideal of L, then $\mathfrak{b}^*$ is a (nonzero) fractional ideal as well.

Proof. Because $\mathfrak{b}$ is a B-module, we see that $\mathfrak{b}^\times$ is also a B-module because $x \in \mathfrak{b}^\times$ and $\alpha \in B$ will have

$$\mathrm{T}_K^L(\alpha x \mathfrak{b}) = \mathrm{T}_K^L(x \cdot \alpha\mathfrak{b}) \subseteq \mathrm{T}_K^L(x\mathfrak{b}) \subseteq A.$$

It remains to show that $\mathfrak{b}^*$ is finitely generated. Fix $\alpha_1, \dots, \alpha_n \in B$ a basis for L/K, and we set $d := \operatorname{disc}(\alpha_1, \dots, \alpha_n)$. Further, find $a \in \mathfrak{b} \cap (A \setminus \{0\})$, which exists because we can take the norm of some nonzero element of $\mathfrak{b}$.

Quickly, we claim that

$$ad\mathfrak{b}^* \overset{?}{\subseteq} B.$$

Indeed, fixing any $x \in \mathfrak{b}^* \subseteq L$, we can write

$$x = \sum_{k=1}^{n} x_k \alpha_k$$

where $x_k \in K$ for each k. Now, we note that $a\alpha_\bullet \in \mathfrak{b}$ for each $\alpha_\bullet$ because $a \in \mathfrak{b}$ and $\alpha_j \in B$, so it follows that

$$\sum_k a x_k \, \mathrm{T}_K^L(\alpha_k \alpha_\bullet) = \mathrm{T}_K^L(xa\alpha_\bullet) \in A.$$

We can view this as a system of equations to solve for the $ax_\bullet$ and everything else is a variable. Solving for this using Cramér's rule, we see that the coefficients live in A and have determinant d, where we also know that the constants are in A. So it follows

$$ax_\bullet \in \frac{1}{d} A$$

for each $x_\bullet$, so $dax_\bullet \in A$, so $dax \in B$, finishing.

But we are done because $\mathfrak{b}^*$ is a B-module where some multiple of it is contained in B. Additionally, $\mathfrak{b}^*$ is nonzero because $\mathfrak{b}$ is finitely generated (it's a fractional ideal), so surely we can find some nonzero element of L clearing the denominators. So it is supposed to follow that $\mathfrak{b}^*$ is a nonzero fractional ideal. ∎

This lets us define the following.

Definition 5.42 (Complementary ideal)**.** The *complementary ideal* $\mathcal{C}_{B/A}$ is defined as

$$B^* = \left\{x \in L : \mathrm{T}_K^L(xB) \subseteq A\right\}.$$

We note that $\mathcal{C}_{B/A}$ is a fractional ideal containing B.

Definition 5.43 (Different ideal)**.** The *different ideal* $\mathcal{D}_{A/B}$ is defined as $\mathcal{D}_{B/A} := \mathcal{C}_{B/A}^{-1}$. We might also write $\mathcal{D}_{L/K}$ depending on the phase of the Moon.

Note that $B \subseteq \mathcal{C}_{B/A}$ implies $\mathcal{D}_{B/A} \subseteq B$, so $\mathcal{D}_{B/A}$ is an integral ideal.

The different is a pretty nice ideal. We show the following.

Definition 5.44. Fix $K \subseteq L \subseteq M$ a chain of finite, separable chain of fields, where $A \subseteq K$ is a ring of integers with B and C the integral closures in L and M respectively. Then

$$\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}.$$

Proof. We refer to the book. ■

Proposition 5.45. Fix K/L a chain of finite, separable fields in the $AKLB$ set-up. Then $\mathcal{D}_{B/A}$ commutes with localization: if $S \subseteq A$ is a multiplicative subset, then

$$\mathcal{D}_{S^{-1}A/S^{-1}B} = S^{-1}\mathcal{D}_{B/A}.$$

Proof. The main idea is to show that each individual step of the construction of $\mathcal{D}_{B/A}$ is compatible with localization. We omit the proof. ■

Proposition 5.46. Fix K/L a chain of finite, separable fields in the $AKLB$ set-up. Then $\mathcal{D}_{B/A}$is commutes with completion: if $\mathfrak{p}$ is a nonzero prime of A lying below a nonzero prime $\mathfrak{q}$ of B, then

$$\mathcal{D}_{\hat{B}/\hat{A}} = \hat{B}\mathcal{D}_{B/A}.$$

Further, $(\mathcal{D}_{B/A})_{\mathfrak{q}} = \mathcal{D}_{\hat{B}/\hat{A}} \cap B$.

Proof. We again refer to the book. ■

We can also build the different by elements.

Definition 5.47 (Different for elements)**.** Fix L/K a field extension, and find some $\alpha \in L$ with f its minimal polynomial. Then we define the *different* of α as

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

The point of zeroing out so many elements is to make sure we only care about the separable ones. Next time we will show that the different ideal is generated by these elements.

5.6 December 6

As usual, we pick up the $AKLB$ picture with separable L/K and λ/κ.

5.6.1 Ramification Control: Different

We have the following lemma.

Lemma 5.48. Fix $\alpha \in L$. Then the following are true.

(a) If $A[\alpha]$ is a full, finitely generated A-submodule of L (which comes from $L = K(\alpha)$ and $\alpha \in B$), then we have that
$$(A[\alpha])^* = \frac{1}{f'(\alpha)} A[\alpha].$$

(b) If $B = A[\alpha]$, then we claim that $\mathcal{D}_{B/A}$ is the principal ideal $\delta_{L/K}(\alpha)B$.

We have that $\mathcal{D}_{B/A}$ is generated by the $\delta_{L/K}(\alpha)$ for $\alpha \in L$.

Proof. We sketch (b). Note that
$$\frac{f(x)}{x-\alpha} = b_{n-1}x^{n-1} + \cdots + b_0$$
with the $b_\bullet \in A$. We can check that
$$\mathrm{T}_K^L\left(\alpha^i \frac{b_j}{f'(\alpha)}\right) = 1_{i-j},$$
so the dual basis for $\{\alpha^\bullet\}$ comes out to
$$\frac{b_\bullet}{f'(\alpha)}.$$
In particular, it follows that
$$A[\alpha]^* = \frac{1}{f'(\alpha)} \sum_k b_k A,$$
which we can check to tbe $\frac{1}{f'(\alpha)} A[\alpha]$. From here, (a) follows directly from (b), for reasons which are not clear to me. ■

We have the following theorem.

Theorem 5.49. We have that $\mathcal{D}_{B/A}$ is generated by the $\delta_{L/K}(\alpha)$ for $\alpha \in L$.

Proof. We sketch. For each $\alpha \in B$ with minimal polynomial f, we set $b = f'(\alpha)$. We will take α so that $L = K(\alpha)$. Now, we can compute the conductor
$$\mathfrak{f} = \mathfrak{f}_{A[\alpha]} = \{x \in L : xB \subseteq A[\alpha]\},$$
so for each $x \in L$, we have $x \in \mathfrak{f}$ if and only if $xB \subseteq A[\alpha]$ if and only if $b^{-1}xB \subseteq b^{-1}A[\alpha] = A[\alpha]^*$ (by lemma) if and only if $\mathrm{T}_K^L(b^{-1}xyA[\alpha]) \subseteq B$ for each $y \in B$ if and only if $\mathrm{T}_K^L(b^{-1}xBA[\alpha]) \subseteq A$ if and only if $\mathrm{T}_K^L(b^{-1}xB) \subseteq A$ if and only if $b^{-1}x \in B^*$ if and only if $x \in b\mathcal{D}_{B/A}^{-1}$. Thus,
$$(\delta_{L/K}(\alpha)) = (b) \in \mathfrak{f}\mathcal{D}_{L/K}.$$
Now, for each nonzero prime $\mathfrak{q} \subseteq B$ lying over $\mathfrak{p} \subseteq A$, we localize: find α with $\mathfrak{q} \nmid \mathfrak{f}_{A[\alpha]}$ (check the completion in $\hat{B}$ and then find a nearby $\alpha \in B$) with $L = K(\alpha)$. We leaving verifying the existence of this α as an exercise. Everything works in the localization, so we can lift up the powers of $\mathfrak{q}$ to the general case. ■

This gives us the following control over ramification.

Theorem 5.50. We have the following. Fix $\mathfrak{q}$ of L lying over $\mathfrak{p}$ of K.

(a) A prime $\mathfrak{q}$ of L is ramified over K if and only if $\mathfrak{q} \mid \mathcal{D}_{B/A}$.

(b) Fix $s := \nu_{\mathfrak{q}}(\mathcal{D}_{B/A})$ and $e := e(\mathfrak{q}/\mathfrak{p})$. Then

$$\begin{cases} e \le s \le e - 1 + \nu_{\mathfrak{q}}(e) & \mathfrak{q} \text{ is wildly ramified,} \\ e \le s \le e - 1 + \nu_{\mathfrak{q}}(e) & \mathfrak{q} \text{ is tamely ramified.} \end{cases}$$

Proof. We refer to the book. The main point is to localize at $\mathfrak{q}$ and set α to be a uniformizer, finishing by the previous theorem. ■

5.6.2 Ramification Control: Discriminant

We have the following definition.

Definition 5.51. The *discriminant ideal* $D_{B/A}$ of A (living downstairs) is the ideal generated by the discriminants $d(\alpha_1, \dots, \alpha_n)$ for $\alpha_\bullet \in B$.

Example 5.52. Taking K to be a number field, $D_{K/\mathbb{Q}} = (\operatorname{disc} \mathcal{O}_K)$.

It happens that the discriminant essentially comes from the different.

Proposition 5.53. We have that $D_{B/A} = \mathrm{N}_K^L \mathcal{D}_{L/K}$.

Proof. The main point is that both sides commute with localizations by subsets $S \subseteq A$, so we may take A to be a local and hence principal ring. It follows that there is an integral basis for B over A, which we name $\{\alpha_1, \dots, \alpha_n\} \subseteq B$. Now, it follows that

$$D_{B/A} = (\operatorname{disc}(\alpha_1, \dots, \alpha_n))$$

because changing to any other basis only multiplies by a square of the determinant of the change-of-basis matrix.

Now, $\mathcal{C}_{B/A}$ is generated by some dual basis $\alpha_1', \dots, \alpha_n'$. Noting that B will only have finitely many primes while being a Dedekind ring, we see that B is a principal ideal domain, so we can find some $b \in L$ such that $\mathcal{C}_{B/A}$ has a basis $b\alpha_1, \dots, b\alpha_n$ over A. It follows that

$$(1) = \left(\det[\mathrm{T}_K^L \, \alpha_i \alpha_j']\right) = \left((\mathrm{N}_K^L \, b) \cdot \det[\mathrm{T}_K^L \, \alpha_i \alpha_j]\right) = \mathrm{N}_K^L \, b \cdot D_{L/K},$$

I guess. Anyways, it's supposed to follow that $D_{L/K} = \mathrm{N}_K^L \, \mathcal{D}_{L/K}$ by tracking through the δs. ■

So we get the following corollary.

Proposition 5.54. A prime $\mathfrak{p}$ of K ramifies up in L if and only if $\mathfrak{p} \mid D_{L/K}$.

Proof. Norm the primes dividing $\mathcal{D}_{B/A}$ down to primes dividing $D_{L/K}$. ■

In particular, we have that a prime p of $\mathbb{Z}$ will ramify up in some number field K if and only if $p \mid \operatorname{disc} \mathcal{O}_K$.

We also have the following tower law.

Proposition 5.55. For a tower $K \subseteq L \subseteq K$, we have that

$$D_{M/K} = D_{L/K}^{[M:L]} D_{M/L}.$$

Proof. Taking the tower law for the different and norm everything downwards. The exponent of $[M : L]$ comes from norming elements of L downwards. ∎

While we're here, we pick up the following statement.

Theorem 5.56 (Hermite–Minkowski)**.** There are only finitely many number fields of given discriminant $\operatorname{disc} \mathcal{O}_K$.

Proof. See the book. ∎

5.6.3 Zeta and L-functions

Here is our main character.

Definition 5.57 (Riemann ζ-function)**.** We define

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for all $s \in \mathbb{C}$ such that $\operatorname{Re} s > 1$.

We note that this does indeed converge (absolutely!) for each $s \in \mathbb{C}$ such that $\operatorname{Re} s > 1$ because

$$\sum_{n=1}^{\infty} \left| \frac{1}{n^s} \right| = \sum_{n=1}^{\infty} \frac{1}{n^{\operatorname{Re} s}} < \infty.$$

We also have uniform absolute convergence on any set $\{s \in \mathbb{C} : \operatorname{Re} s > 1 + \delta\}$ for each $\delta > 0$.

The reason we care about this function in number theory is the following.

Proposition 5.58 (Euler product)**.** We have that

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

again for each $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$.

Proof. The point is to use unique prime factorization. We have that

$$\begin{aligned} 1 - p^{-s} \\ = \end{aligned} \sum_{k=0}^{\infty} \frac{1}{p^{ks}}.$$

Now, for any finite set T of primes, we have that

$$\prod_{p \in T} \frac{1}{1 - p^{-s}} = \prod_{p \in T} \sum_{\nu_p = 0}^{\infty} \frac{1}{p^{-s\nu_p}},$$

which will expand out to a sum of $\frac{1}{n^{-s}}$ such that s only contains primes in T. Setting T to be the primes up to N, we can bound

$$\left|\zeta(s) - \prod_{p\in T}\frac{1}{1-p^{-s}}\right| = \left|\sum_{p|n \implies p\notin T}\frac{1}{n^s}\right| < \sum_{n=N+1}^{\infty}\left|\frac{1}{n^s}\right|.$$

Taking $N\to\infty$ causes this to go to 0, so we get the result we want. ■

To continue our story, we have the following definition.

Definition 5.59 (The Γ function)**.** We define

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

for $s\in\mathbb{C}$ such that $\operatorname{Re} s > 0$.

Example 5.60. We have that $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$.

The function Γ can be meromorphically continued to all of $\mathbb{C}$ as follows.

Proposition 5.61. We have that $\Gamma(s+1) = s\Gamma(s)$ for each s where Γ happens to be defined.

Proof. Apply integration by parts. ■

Corollary 5.62. We have that $\Gamma(n) = (n-1)!$ for each $n\in\mathbb{Z}^+$.

Proof. Start with $\Gamma(1) = 1$ and induct using the above proposition. ■

Formally speaking, we get an analytic continuation of $\frac{1}{\Gamma(s)}$ to all of $\mathbb{C}$ by simply applying the identity repeatedly, which is giving us our meromorphic continuation to all of $\mathbb{C}$ with poles at exactly the non-positive integers $s\in\{0,-1,-2,\dots\}$.

5.7 December 8

The speedrun continues.

5.7.1 Riemann ζ-function

We quickly recall the definition we had

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

for $\operatorname{Re} s > 1$. We also defined

$$\Gamma(s) := \int_0^\infty e^{-y}y^s\frac{dy}{y},$$

for $\operatorname{Re} s > 0$, and we had an analytic continuation of $\frac{1}{\Gamma(s)}$ to all of $\mathbb{C}$. We now define

$$\Xi(s) := \pi^{-3/s}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

for $\operatorname{Re} s > 1$. We now have the following theorem.

Theorem 5.63. The function $\Xi(s)$ extends to a meromorphic function on all of $\mathbb{C}$, with simple poles at $s = 0$ and $s = 1$ with residues -1 and 1 respectively. In fact, Ξ satisfies

$$\Xi(s) = \Xi(1 - s).$$

Proof. We won't prove all of this, but we will prove a bit. So far we only have Ξ only defined to the right of $\operatorname{Re} s = 1$. We start with a trick: we extend ζ to $\operatorname{Re} s > 0$ so that Ξ will also be defined over there.

Definition 5.64. A *Dirichlet series* is a sum of the form $\sum_n a_n n^{-s}$, where $a_n \in \mathbb{C}$.

Lemma 5.65. Fix $\sum_n a_n n^{-s}$ be a Dirichlet series and define, for $n \in \mathbb{N}$,

$$A_n = \sum_{k=1}^{n} a_k.$$

If we can find $c > 0$ and $\sigma > 0$ such that $|A_n| < cn^\sigma$ for each n, then the full series will converge with $\operatorname{Re} s > \sigma$.

Proof. We refer to Lang's *Algebraic Number Theory*, Chapter VIII, Theorem 2. ∎

And now we use the lemma.

Proposition 5.66. The function $\zeta(s)$ has a meromorphic continuation to $\operatorname{Re} s > 0$, with a simple pole at $s = 1$.

Proof. We can use the lemma. Set

$$\zeta_s(s) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}$$

to be the alternating version of ζ. Then we see that $|A_n| \le 1$ always, so ζ_2 will converge on $\operatorname{Re} s > \sigma$ for each $\sigma > 0$, so ζ_2 will converge on $\operatorname{Re} s > 0$ by pushing σ back to 0.

But now we can compute that

$$\frac{2}{2^s}\zeta(s) + \zeta_2(s) = \sum_{n=1}^{\infty} \frac{2}{(2n)^s} + \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s),$$

so

$$\zeta(s) = \frac{\zeta_2(s)}{1 - 2^{1-s}}.$$

Because both functions here agree on $\operatorname{Re} s > 1$, the right-hand side will provide a continuation for ζ to $\operatorname{Re} s > 0$. Tracking our poles, we see that ζ_2 will have no poles here, but $1 - 2^{1-s}$ will have a zero at $s = 1 + \frac{2\pi ni}{\log 2}$ for each n.

We would like to get rid of these poles. For this, we define

$$\zeta_3(s) := \zeta(s) - \frac{3}{3^s}\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^2} - \frac{2}{6^s} + \cdots.$$

Again by lemma, ζ_3 will continue to $\operatorname{Re} s > 0$, and we now find that

$$\zeta(s) = \frac{\zeta_3(s)}{1 - 3^{1-s}}$$

for $\operatorname{Re} s > 1$, so we have a continuation for ζ to $\operatorname{Re} s > 0$. But tracking our poles like last time, now our poles will occur at $s = 1 + \frac{3\pi ni}{\log 3}$ for each n, but the intersection is

$$\left\{1 + \frac{3\pi ni}{\log 3} : n \in \mathbb{Z}\right\} \cap \left\{1 + \frac{3\pi ni}{\log 3} : n \in \mathbb{Z}\right\} = \{1\}$$

because $\frac{\log 2}{\log 3}$ is irrational. So our only possible pole is at $s = 1$, which we can verify does indeed exist by looking at $\zeta(s)$ as $s \to 1^+$. ■

From here, we have extended Ξ to $\operatorname{Re} s > 0$, and we can prove the functional equation (with some effort), which provides a continuation of Ξ to all of $\mathbb{C}$. ■

5.7.2 The Riemann Hypothesis

It is known that, for each positive integer n, we have

$$\zeta(1-n) = \frac{-B_n}{n!},$$

where B_n are the Bernoulli numbers, given by the generating function

$$\frac{t}{1-e^{-t}} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

In particular, ζ has zeroes at the negative even integers. In fact, ζ has no other zeroes outside of the strip $0 < \operatorname{Re} s < 1$.

Conjecture 5.67. The Riemann hypothesis is the conjecture that

$$\zeta(s) = 0 \implies s \in -2\mathbb{Z}_{>0} \text{ or } \operatorname{Re} s = \frac{1}{2}.$$

This might appear abstract, but it has many implications to analytic number theory. To state this, we have the following definitions.

Definition 5.68 (Prime-counting functions)**.** Fix $x > 0$. Then define $\pi(x)$ to be the number of primes less than x; define

$$\operatorname{Li}(x) := \int_0^x \frac{dx}{\log x}.$$

Define

$$\psi(x) := \sum_{p^m \le x} \log p.$$

Theorem 5.69. Fix $\varepsilon \ge 0$. The following are equivalent.

(i) The function $\zeta(s)$ has no zeroes $\operatorname{Re} s > \frac{1}{2} + \varepsilon$.

(ii) We have that $\psi(x) = x+) \left(x^{1/2+\varepsilon}(\log x)^2\right)$.

(iii) We have that $\pi(x) = \operatorname{Li}(x) + O\left(xe^{-a\sqrt{\log x}}\right)$, for some $a > 0$.

We remark that it is known that $\psi(x) = x + O\left(xe^{-c\sqrt{\log x}}\right)$, which is the Prime number theorem.

5.7.3 Class Field Theory

As we must, we begin with a little abstraction.

Definition 5.70 (Restricted direct product)**.** Fix $\{G_\alpha\}_{\alpha\in\lambda}$ be a collection of groups, and fix subgroups $\{H_\alpha\}_{\alpha\in\lambda}$ so that $H_\alpha \subseteq G_\alpha$. Now we define the *restricted direct product* defined as

$$\prod_{\alpha\in\lambda}{}' G_\alpha := \left\{ (g_\alpha)_{\alpha\in\lambda} \in \prod_{\alpha\in\lambda} G_\alpha : g_\alpha \in H_\alpha \text{ all but finitely often} \right\},$$

with operation inherited from the product.

This lets us define the following two objects.

Definition 5.71 (Idéles)**.** Fix K a global field. Then the group of *idéles* I_K of K is the restricted product

$$\prod_{\mathfrak{p}\in M_K}{}' K_\mathfrak{p}^\times$$

where our subgroups are $\mathcal{O}_\mathfrak{p}^\times$, which is the unit group of the valuation ring associated to the place $\mathfrak{p} \in M_K^\circ$. If $\mathfrak{p}$ is real, then take $\mathbb{R}_{>0}^\times$; if $\mathfrak{p}$ is complex, take $\mathbb{C}^\times$.

To codify the above subgroups, we have the following definition.

Definition 5.72 (Valuation rings)**.** Fix K a global field and $\mathfrak{p}$ a place. Then

$$U_\mathfrak{p} := \begin{cases} \mathcal{O}_\mathfrak{p}^\times & \mathfrak{p} \text{ finite}, \\ \mathbb{R}_{>0}^\times & \mathfrak{p} \text{ real}, \\ \mathbb{C}^\times & \mathfrak{p} \text{ complex}. \end{cases}$$

We wold like to be able to kill some finite set of places, so given a set $S \subseteq M_K$ of places, we define

$$I_K^S := \left\{ (a_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K_\mathfrak{p}^\times : a_\mathfrak{p} \in U_\mathfrak{p} \text{ for } \mathfrak{p} \notin S \right\}$$

so that

$$I_K^S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}.$$

In particular, $S \subseteq S'$ implies $I_K^S \subseteq I_K^{S'}$ and $I_K = \bigcup I_K^S$ so that $I_K^S \subseteq I_K$.

What makes the idéles usable is that we have a diagonal map

$$K^\times \subseteq I_K$$

by taking $\alpha \mapsto (\alpha)_\mathfrak{p}$. We can see that, indeed, only finitely many places $\mathfrak{p}$ will have $\alpha \notin U_\mathfrak{p}$.

Definition 5.73 (Principal idéle)**.** An idéle is *principal* if it is in $K^\times \subseteq I_K$.

Example 5.74. If K is a number field, then

$$K^\times \cap I_K^{M_K^\infty} = \mathcal{O}_K^\times$$

More generally, if $M_K^\infty \subseteq S$, then $K^\times \cap I_K^S = \mathcal{O}_{K,S}^\times$, which are the S-units of $\mathcal{O}_K$.

The above example leads us to the next definition.

Definition 5.75 (General S-integers)**.** Fix K a global field. Given a finite set S of places, we set $K^S := K^\times \cap I_K^S$.

The addition of infinite places being able to add restrictions really only matters for real places ρ, where we are requesting that the image under $\rho : K \hookrightarrow \mathbb{R}^\times$ be positive.

5.8 December 10

And so it ends.

5.8.1 Idéle Class Group

We continue our story of class field theory. Today we will be modest enough to take K to be a number field.

Definition 5.76 (Idéle class group)**.** The *idéle class group* is defined as the quotient $C_K := I_K/K^\times$, where $K^\times \subseteq I_K$ using the usual embedding.

We would like to relate C_K with our usual ideal class group Cl_K .

Remark 5.77. We have that C_K is uncountable.

There is a homomorphism $I_K \to J_K$, where J_K are the fractional ideals by taking

$$(\alpha_\mathfrak{p})_\mathfrak{p} \longmapsto \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\nu_\mathfrak{p}(\alpha_\mathfrak{p})},$$

which is a legal, finite product because all but finitely many of the $\alpha_\mathfrak{p}$ have $\nu_\mathfrak{p}(\alpha_\mathfrak{p}) = 0$ by definition of the restricted product. We note that the above map is surjective because look at it, and its kernel essentially consists of the infinite places:

$$I_K^{M_K^\infty} = \prod_{\mathfrak{p}\mid\infty} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\nmid\infty} \mathcal{O}_\mathfrak{p}^\times.$$

Thus, $I_K/I_K^{M_K^\infty} \cong J_K$ and modding out by $K^\times$ on both sides gives us a surjective map $C_K \to \mathrm{Cl}_K$ with kernel $K^\times I_K^{M_K^\infty}/K^\times$. Putting this all together, we get the following exact sequence.

$$0 \to K^\times \to K^\times I_K^{M_K^\infty} \to C_K \to \mathrm{Cl}_K \to 0$$

Of course, the above story does not have to be for just infinite places/

Proposition 5.78. For any finite subset S which contains M_K^∞, we have the following exact sequence.

$$0 \to K^\times \to K^\times I_K^S \to \mathrm{Cl}_K^S \to 0,$$

where Cl_K^S is the class group of our S-integers.

Proof. Imitate the above discussion. ∎

We note that if S is sufficiently large, namely to contain a generating set for Cl_K, we will have that $\mathrm{Cl}_K^S = 0$, so we get the short exact sequence

$$0 \to K^\times \to K^\times I_K^S \to C_K \to 0.$$

By drawing the following diagram, the five lemma tells us that $K^\times I_K^S \cong I_K$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^\times & \longrightarrow & K^\times I_K^S & \longrightarrow & C_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & K^\times I_K & \longrightarrow & C_K & \longrightarrow & 0 \end{array}$$

This is sufficiently cute.

5.8.2 Topological Groups

We have the following definition.

Definition 5.79 (Topological group)**.** A *topological group* G is a group G together with a topology such that the maps

$$(x,y) \mapsto xy \qquad \text{and} \qquad x \mapsto x^{-1}$$

are continuous maps.

Example 5.80. Everyone's favorite fields give topological groups: $(\mathbb{Q},+), \mathbb{R}^\times, \mathbb{C}^\times$, and so on.

We remark that if G is a topological group, then given $g \in G$, the maps $x \mapsto gx$ and $x \mapsto xg$ are both continuous by the first condition, so they are homeomorphisms $G \to G$ by noting the inverse maps are from g^{-1}.

We note that this implies we can create a topology on G using only the open sets around the identity of G. Namely, if U is a nonempty open subset with $g \in U$, then $g^{-1}U$ will be an open subset containing e.

We pick up the following facts.

Proposition 5.81. Fix G a topological group with $H \subseteq G$ a subgroup.

(a) If H is open, then H is closed.

(b) If H is closed and of finite index, then H is open.

(c) If $H_1 \subseteq H_2 \subseteq G$ and H_1 is open, then H_2 is also open.

Proof. For (a) and (b), we simply look at G/H. For (a), all cosets in G/H are open, so H is closed by considering the union of all the cosets not equal to H. For (b), all cosets in G/H are closed, so H is now open. For (c), tile H_2 by H_1s as in H_2/H_1 and then union them together. ■

With this notation in mind, we observe that we can build a basic set of open sets around $1 \in I_K$ by

$$\prod_{\mathfrak{p} \in S} W_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} U_\mathfrak{p},$$

where $S \subseteq M_K$ is finite and $W_\mathfrak{p}$ is an open neighborhood of 1 in $K_\mathfrak{p}^\times$. We can also view this as the coarsest group topology that we can give I_K while requiring the projections

$$I_K \to K_\mathfrak{p}^\times$$

to be continuous while maintaining $I_K^S \subseteq I_K$ being open.

One can show that this topology makes $K^\times \subseteq I_K$ into a discrete subgroup and so closed. Additionally, we get that is C_K a topological group by modding.

5.8.3 Norms

To continue using our embedding $K^\times \subseteq I_K$, we pick up the following definition.

Definition 5.82 (Absolute norm)**.** Given some idéle $a := (a_\mathfrak{p})_\mathfrak{p} \in I_K$, we define the *absolute norm* as

$$\mathrm{N}(a) = \prod_\mathfrak{p} |\|a_\mathfrak{p}\|_\mathfrak{p}^{-1}.$$

It happens that this is a continuous homomorphism $I_K \to \mathbb{R}_{>0}$, it is surjective, and it has kernel $K^\times$ (by the product formula on $K^\times$). Thus, the absolute norm in fact descends to a map $C_K \twoheadrightarrow \mathbb{R}_{>0}^\times$.

The norm is a good way to measure size of the idéle class group, but we would like to make the idéle class group smaller to be able to handle it more properly. This gives us the following definition.

Definition 5.83 (C_K^0)**.** We define $C_K^0 := \ker C_K$.

It is a theorem that C_K^0 has now been made small enough: namely, C_K^0 is compact.

There is also a relative norm to accompany our absolute norm.

Definition 5.84 (Relative norm)**.** Fix L/K an extension of number fields. Then we define the *relative norm* $\mathrm{N}_K^L : I_L \to I_K$ by taking $\beta \in I_L$ to

$$\left(\mathrm{N}_K^L \beta\right)_\mathfrak{p} := \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathrm{N}_{K_\mathfrak{p}}^{L_\mathfrak{q}} B_\mathfrak{q}.$$

This norm is also functorial, making the following diagram commute.

$$\begin{array}{ccc} L^\times & \hookrightarrow & I_L \\ {\scriptstyle \mathrm{N}_K^L}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_K^L} \\ K^\times & \hookrightarrow & I_K \end{array}$$

Hooray.

5.8.4 Global Class Field Theory

We are now ready to state the main theorem of global class field theory.

Theorem 5.85. Fix K a number field. There exists a canonical bijection between finite abelian extensions L/K and open subgroups $H \subseteq C_K$ of finite index. In fact, $\mathrm{Gal}(L/K) \cong C_K/H$.

We would like to further extend this correspondence, in the way that Galois theory does.

Theorem 5.86. Fix K a number field. Then the correspondence in Theorem 5.85 is inclusion-reversing.

(a) If the extensions L and L' correspond to the subgroups H and H', then $L \supseteq L'$ if and only if $H \subseteq H'$.

(b) Further, LL' corresponds to $H \cap H'$, and $L \cap L'$ correspond to HH'.

We also have some control over prime-splitting.

Theorem 5.87. Fix K a number field. Then the correspondence in Theorem 5.85 controls prime-splitting.

(a) For all finite places $\mathfrak{p} \in M_K^\circ$, we have that $\mathfrak{p}$ is unramified in L if and only if $H \supseteq K^\times U_\mathfrak{p}/K^\times$.

(b) For all places $\mathfrak{p} \in M_K^\circ$, then $\mathfrak{p}$ splits completely in L if and only if $H \supseteq K^\times K_\mathfrak{p}^\times/K^\times$.

Let's do some applications.

Definition 5.88 (Hilbert class field)**.** Fix K a number field. Then the *Hilbert class field* of K is the extension L/K which corresponds to $H = K^\times I_K^{M_K^\infty}/K^\times \subseteq C_K$.

The Hilbert class field has some magic associated with it. Fix K a number field and set $H := K^\times I_K^{M_K^\infty}/K^\times$ corresponding to L the Hilbert class field. We have the following.

(a) We have that $C_K/H \cong I_K/K^\times I_K^{M_K^\infty} \cong J_K/K^\times = \mathrm{Cl}_K$. In particular, $\mathrm{Gal}(L/K) \cong \mathrm{Cl}_K$.

(b) Noting that $H \supseteq K^\times K_\mathfrak{p}/K^\times$ for each infinite place $\mathfrak{p}$ and $H \supseteq K^\times U_\mathfrak{p}/K^\times$ for each finite place $\mathfrak{p}$, it follows that L is unramified at all finite places and splits completely at all infinite places.

(c) In fact, we can see that L is the largest abelian extension of K unramified at all finite places.

As an aside, we remark that we can recover the Kronecker–Weber theorem from global class field theory by essentially showing $\mathrm{Gal}\left(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}\right) \cong \widehat{\mathbb{Z}}$.