Part I: Math 254A

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 1: 26 August

Professor Martin Olsson Abhishek Shivkumar

Administrative Stuff

Lectures are an hour and a half, with a break somewhere in the middle. Lectures will be recorded for (mostly) the benefit of people not in the country. Students should aim to follow the rhythm of the course and talk to their classmates so that the online learning environment doesn't just become a recitation of the textbook. Professor Olsson will aim to have office hours so that people living abroad can access them as well, but contact him if you have constraints.

If you're concerned about prerequisites, talk to Professor Olsson and speak up in class if there's something you don't recognize. Not a fatal problem if you're missing background in some area; you can catch up by reading on your own.

I asked: How much Galois Theory are we expected to know? I've learned bits and pieces of it here and there but I've never taken a full formal course in Galois Theory.

Professor Olsson says: hard to answer specifically, I'll put some notes up.

There are four recommended books for the class; we'll start with the first four chapters of Serre's Local Fields, it's very concise and terse. All four books should be accessible to Berkeley students for free; three are Springer, one is a set of free online notes.

Everyone learns math differently, the approach of this class will be lots and lots of problems and exercises. Don't worry too much about homework grades, they're really just there to measure your understanding. He'll reach out if he thinks someone is struggling. Do the survey he sent out so he can get a feel for where everyone is at, background-wise.

The remainder of the grade for this course (30%) is the term paper, which we'll discuss more when we're closer to it.

We should all work to make this a safe environment for people to learn. Treat your classmates with respect.

Note to reader: I use a Tufte style layout for my notes. The main information from lecture will be in the body of the text, the sidenotes are my comments, questions, and remarks. My only nonstandard notation that I can think of is that I use $\subset$ to mean strict subset, and $\subseteq$ when the inclusion is not necessarily strict.

Number Theory from 40,000 Feet

Question 1.2.1

What is number theory?

- Structure of $\mathbb{Q}$, $\mathbb{Z}$, prime numbers, the distribution of primes (this is more the analytic side of things)
- What are the solutions of the equation

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

  in $\mathbb{Z}$ or $\mathbb{Q}$? (Diophantine equations)

  Answer: parameterized by $\mathbb{Z}^2$ by the map

  $$(a, b) = (a^2 - b^2, 2ab, a^2 + b^2) = (x, y, z)$$

  Aside: this defines an embedding $\mathbb{P}^1 \hookrightarrow \mathbb{P}^2$.

  I'm not sure if this is injective on solutions up to permutation; I recall there being some degeneracy.

- What are the solutions of the equation

  $$x^n + y^n = z^n$$

  in $\mathbb{Z}$ or $\mathbb{Q}$ for $n \geq 3$? Answer: only the obvious solutions (due to Wiles, around 1990)

Definition 1.2.2: Algebraic Numbers

$\alpha \in \mathbb{C}$ is *algebraic* if it satisfies an equation $f(\alpha) = 0$ with $f \in \mathbb{Q}[x]$.

Lemma 1.2.3

The algebraic numbers form a field, $\overline{\mathbb{Q}}$, with $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$.

Most of this course will be dedicated to studying finite extensions of fields, namely finite extensions of $\mathbb{Q}$.

Definition 1.2.4: Number Fields

A finite field extension k of $\mathbb{Q}$ is a *number field*. $\mathcal{O}_k$, the *ring of integers* of k, is the integral closure of $\mathbb{Z}$ in k.

Given a number field k, we have the following diagram:

$$\begin{tikzcd}
k & \mathcal{O}_k \arrow[l, hook'] \\
\mathbb{Q} \arrow[u, hook] & \mathbb{Z} \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

A fundamental tool in commutative algebra which we will use is completion, which comes in two flavors. There's the algebraic version, which takes the algebraic closure of a field and allows you to fill in missing zeros of your polynomials, and there's p-adic completion, which is more local.

I need to think a little about why $\mathbb{C}$ is "global" and why $\mathbb{Q}_p$ or $\overline{\mathbb{Q}_p}$ is "local." I don't really understand that assertion.

For what follows and the rest of the course, all rings are commutative and unital.

Definition 1.2.5: Integral Closure

Let $A \hookrightarrow B$ be an inclusion of rings, then an element $b \in B$ is *integral* over A is b satisfies an equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

with $n > 0$, $a_i \in A$. The ring B is called integral over A if every element of B is integral over A.

Then, the *integral closure* of A in B is the set of all integral elements of B over A. When we speak of the integral closure or *normalization* of A without reference to some larger ring B, we mean its integral closure in its field of fractions.

Lemma 1.2.6

Given an inclusion of rings $A \hookrightarrow B$, $b \in B$ is integral over A iff there exists a finitely generated nonzero A-submodule $M \subseteq B$ such that $bM \subseteq M$.

Example 1.2.7

We have that $\mathbb{Z} \hookrightarrow \mathbb{C}$, and consider the $\mathbb{Z}$-submodule of $\mathbb{C}$ $(a + b\sqrt{-7})$. This submodule is stable under multiplication by $\sqrt{-7}$, so $\sqrt{-7}$ is integral.

We may sometimes have an example or two between a lemma or theorem and its proof. I hope this doesn't cause any confusion, as I haven't set up my proof environment to reference the result to which they belong yet.

Proof: For the forward implication, let b be integral over A, and let M be the submodule generated by b, which is of the form

$$\{a_0 + a_1 b + \cdots + a_r b^r\}$$

and finitely generated since b satisfies a monic equation in A. If

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

is the monic equation satisfied by b, then

$$b^n = -a_0 - a_1 b - \cdots - a_{n-1}b^{n-1}$$

Therefore, bM is clearly a subset of M since b^n is expressible in terms of lower powers of b.

For the converse, let $M = (v_1, \cdots, v_r)$ with $bM \subseteq M$, and consider the left multiplication map $\cdot b : M \to M$ given by

$$bv_i = \sum_j a_{ij} v_j$$

This expression is just the decomposition of bv_i into the v_i, which exists by assumption. Then we have the following diagram, where $R = (a_{ij})$ is the matrix of coefficients:

$$\begin{tikzcd}
A^r \arrow[r, two heads] \arrow[d, "R=(a_{ij})"'] & M \arrow[r, hook] \arrow[d, "\cdot b"] & B \arrow[d, "\cdot b"] \\
A^r \arrow[r, two heads] & M \arrow[r, hook] & B
\end{tikzcd}$$

Then, let

$$P(x) = \det \begin{pmatrix} x - a_{11} & \cdots & -a_{1r} \\ \vdots & \ddots & \vdots \\ -a_{r1} & \cdots & x - a_{rr} \end{pmatrix}$$

By the Cayley-Hamilton Theorem, we know that $P(R) = 0$, and since b is an eigenvalue of R, $P(b) = 0$ and therefore, b is integral. ■

We shouldn't say the submodule generated by b in the forward implication above, rather, the smallest A-submodule containing b, which is what we have described.

I really liked the Cayley-Hamilton proof of the reverse implication, but I don't really understand why we needed the commutative diagram in the proof.

Lemma 1.2.8

Let $b \in B$ be integral over A, and consider $B' \subseteq B$ the A-subalgebra generated by b. Then $A \hookrightarrow B'$ is integral, e.g, B' is integral over A.

Proof: $M = B'$ is a finitely generated A-module, stable under multiplication by anything in B' via "wraparounds," so by the above lemma, B' is integral over A. ■

Lemma 1.2.9

If B is integral over A and finitely generated as an A-algebra, then B is finitely generated as an A-module.

Example 1.2.10

$\mathbb{C}[x]$ is finitely generated as a $\mathbb{C}$-algebra, generated by x, since we can multiply x with itself, but is not finitely generated as a $\mathbb{C}$-module.

Proof: Consider the sequence

$$A \hookrightarrow A[b_1] \hookrightarrow A[b_1, b_2] \hookrightarrow \cdots \hookrightarrow A[b_1, \cdots, b_n]$$

where the b_i are the generators of B as an A-algebra. By the above lemma, each inclusion above is integral, so if we can show that $A[b_1]$ is finitely generated as an A-module, by induction, the result follows.

Then, we want to show that $A[b]$ is finitely generated as an A-module when b is integral. But, since b satisfies the equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

by assumption, we may take $1, b, \cdots, b^{n-1}$ as an A-basis for $A[b]$, from which the result follows. ■

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 2: 31 August

Professor Martin Olsson Abhishek Shivkumar

Integrality

We spent some time reviewing the relevant info from last lecture, namely, the definition of an integral element, the statement Lemma 1.2.6, and reviewing the proof of Lemma 1.2.9.

Proposition 2.1.1

If $A \hookrightarrow B \hookrightarrow C$, with C integral over B and B integral over A, then C is integral over A.

Proof: Let $c \in C$, with integral equation

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$$

with $b_i \in B$. Let $B_1 \subseteq B$ be the sub-A-algebra generated by the b_i. B_1 is finitely generated as an A-module, since B is integral over A, by Lemma 1.2.9. Define C_1 to be the subalgebra of C generated by B_1 and c. Suppose $B_1 = (d_1, \cdots, d_t)$ as an A-module, then C_1 is generated as an A-module by $d_i c^j$ for $0 \leq j \leq n-1$. $\blacksquare$

This next result is a little out of order, since we defined integral closure last week and you really need to show that this holds before that definition even makes sense.

Proposition 2.1.2

Let L be a field, $A \subseteq L$ a subring, B the integral closure of A in L. B is a subring of L containing A.

Example 2.1.3

The main example of integral closure we will be concerned with is the arrow $\mathbb{Z} \hookrightarrow \mathcal{O}_k$ in the following diagram:

$$\begin{tikzcd}
k & \mathcal{O}_k \arrow[l, hook'] \\
\mathbb{Q} \arrow[u, hook] & \mathbb{Z} \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

Proof: To see that $A \subseteq B$, note that $a \in A$ satisfies the monic equation $x - a = 0$.

If $b_1, b_2 \in B$, $M_1, M_2 \subseteq L$ the finitely generated A-submodules given by Lemma 1.2.6, satisfying $b_1 M_1 \subseteq M_1$, and $b_2 M_2 \subseteq M_2$.

Let $M := M_1 \cdot M_2$, the A-submodule of L generated by expressions $m_1 \cdot m_2$ with $m_1 \in M_1$, $m_2 \in M_2$. M is finitely generated since it is generated by the products of a set of generators for M_1 and M_2, which are themselves finitely generated.

We claim that $(b_1b_2)M \subseteq M$. To see this, note that $(b_1b_2)(m_1m_2) = (b_1m_1)(b_2m_2)$ where we can commute elements since all of these elements are contained in the field L, and since $b_1m_1 \in M_1$ and $b_2m_2 \in M_2$, it follows that $b_1b_2 \in B$.

Moreover, $(b_1+b_2)M \subseteq M$. As above, we have

$$(b_1+b_2)(m_1m_2) = b_1m_1m_2 + b_2m_1m_2 = (b_1m_1)m_2 + m_1(b_2m_2)$$

Then $b_1m_1 \in M_1$ and $b_2m_2 \in M_2$ by the above argument, so the above expression is in M, from which it follows that $b_1+b_2 \in B$. ■

This definition is also given above, in the notes to Lecture 1, because I jumped the gun a little bit.

Definition 2.1.4: Integrally Closed Domains

An integral domain A is called *integrally closed* or *normal* if the integral closure of A in the field of fractions of A is equal to A.

Example 2.1.5

$\mathbb{Z} \subset \mathbb{Q}$ and $k[x] \subset k(x)$ are integrally closed.

Proof: The proofs of these are essentially the same; the main point is that both $\mathbb{Z}$ and $k[x]$ are UFDs (unique factorization domains). Let $g \in k[x]$, which has unique decomposition

$$g(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$$

where the $p_i(x)$ are irreducible.

Then, suppose $f \in k(x)$, which can be written by the above as

$$f(x) = \frac{p_1(x)^{n_1} \cdots p_r(x)^{n_r}}{q_1(x)^{m_1} \cdots q_s(x)^{m_s}}$$

where the p_i, q_j are distinct and irreducible in $k[x]$. Suppose that f is integral over $k[x]$ with integral equation

$$f(x)^n + a_{n-1}(x)f(x)^{n-1} + \cdots + a_0(x) = 0$$

The lead term of this equation is

$$\frac{p_1(x)^{n\cdot n_1} \cdots p_r(x)^{n\cdot n_r}}{q_1(x)^{n\cdot m_1} \cdots q_s(x)^{n\cdot m_s}}$$

Multiplying through the integral equation by $q_1(x)^{n\cdot m_1} \cdots q_s(x)^{n\cdot m_s}$, we get an equation

$$p_1(x)^{n\cdot n_1} \cdots p_r(x)^{n\cdot n_r} + q_1(x)^{m_1} \cdots q_s(x)^{m_s}(\cdots) = 0$$

which implies that

$$q_1(x)^{m_1} \cdots q_s(x)^{m_s} | p_1(x)^{n\cdot n_1} \cdots p_r(x)^{n\cdot n_r}$$

which is a contradiction (since we assumed p_i, q_j distinct and irreducible) unless the denominator is equal to 1. ■

Lemma 2.1.6

All UFDs are integrally closed.

The proof is exactly as above, and is essentially a generalization of the Rational Root Theorem.

Discrete Valuation Rings

Definition 2.2.1

Principal Ideal Domains A *principal ideal domain* (PID) is an integral domain such that each ideal is principal, e.g, generated by a single element.

By convention, prime ideals are proper.

Definition 2.2.2: Discrete Valuation Ring

A *discrete valuation ring* (DVR) is a PID with a unique nonzero prime ideal. Equivalently, a DVR is a PID with a unique nonzero maximal ideal.

How I think about it: a local PID (that's not a field).

Example 2.2.3

Let $k \supseteq \mathbb{Q}$ be a number field with ring of integers $\mathcal{O}_k$, $\mathfrak{p} \subset \mathcal{O}_k$ a prime ideal, $\mathcal{O}_{k,\mathfrak{p}}$ the localization of $\mathcal{O}_k$ at $\mathfrak{p}$. $\mathcal{O}_{k,\mathfrak{p}}$ is a discrete valuation ring, and the one that we'll be concerned with for the most part.

Example 2.2.4

Consider $k[[t]]$, with

$$f(t) = a_0 + a_1 t + \cdots$$

$f \in k[[t]]^\times$ iff $a_0 \neq 0$. The way to see this is to write

$$(a_0 + a_1 t + a_2 t^2 + \cdots)(b_0 + b_1 t + b_2 t^2 + \cdots) = 1$$

and obtain equations $a_0 b_0 = 1$, $a_0 b_1 + a_1 b_0 = 0$ and so on by matching coefficients. One can inductively show that each equation is solvable if the first one, $a_0 b_0 = 1$ has a solution b_0, e.g, if $a_0 \neq 0$.

Therefore, one can see that all nonzero ideals in $k[[t]]$ are (t^r) for $r \geq 0$, from which it follows that $k[[t]]$ is a PID, with unique prime (maximal) (t).

Remark 2.2.5

As an informal organizing scheme, there are basically only two kinds of DVRs: power series over fields, and p-adic type things.

Lemma 2.2.6

Let A be a DVR, $\mathfrak{m} \subset A$ its maximal ideal, $k = A/\mathfrak{m}$. A generator $\pi \in \mathfrak{m}$ is called a *uniformizer*. Then every nonzero ideal $I \subset A$ is of the form (π^r) for unique $r \geq 0$.

Proof: Since A is a PID, $I = (\alpha)$. For the first case, $I = A$ if and only if $\alpha \in A^\times$ which in turn implies that $I = (\pi^0)$.

If $I \neq A$, $I \subseteq (\pi)$ (since, by the axiom of choice, every ideal is contained in some maximal ideal) which implies that $\alpha = \alpha_1 \pi$. Proceeding like this, we can form an ascending chain of ideals:

$$I \subset (\alpha_1) \subset (\alpha_2) \subset \cdots \subset (\alpha_n) \subset \cdots$$

where $\alpha_n \pi = \alpha_{n-1}$. If $(\alpha_n) = A$ for some n, we have

$$\alpha = \alpha_1 \pi = \alpha_2 \pi^2 = \cdots = \alpha_n \pi^n$$

where α_n is a unit (since the generator of the unit ideal must be a unit), so $(\alpha) = (\pi^n)$.

Otherwise, let $I_\infty = \bigcup_{n \geq 0} (\alpha_n)$. Since A is a PID, $I_\infty = (\beta)$, $\beta \in I_n$ for some n, so $I_\infty = I_n$. Then, the chain terminates after I_n, and we can repeat the argument above.

For the uniqueness part of the statement, suppose that $(\pi^s) = (\pi^t)$ for $ss \leq t$, that is, $\pi^s = v\pi^t$, which implies that $v\pi^{t-s} = 1$. Thus $(\pi^{t-s}) = A$, from which it follows that $t = s$, since increasing powers of (π) are *smaller*. ■

Establishing that I_∞ exists might involve the axiom of choice, I think that this may have been mentioned in passing, but no such argument was written down.

Also hidden in this proof *might* be a proof that all DVRs are Noetherian.

I may have missed a step between the I_∞ part of the proof and the uniqueness part, but this proof looks complete to me.

This result induces the valuation on discrete valuation rings.

Definition 2.2.7: Valuations on DVRs

The *valuation* on a DVR A is a function $\nu : A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ sending a to r such that $(a) = \mathfrak{m}^r$. Moreover, this function can be extended to the field of fractions K of A, e.g $\nu : K^\times \to \mathbb{Z}$ given by $\nu\left(\frac{a}{a'}\right) = \nu(a) - \nu(a')$.

ν has several nice properties which are easy to prove; $\nu : K^\times \to \mathbb{Z}$ is a surjective homomorphism with $\nu(xy) = \nu(x) + \nu(y)$. Moreover, $\nu(x + y) \geq \min(\nu(x), \nu(y))$.

Example 2.2.8

Let $A = k[[t]]$ with $\mathfrak{m} = (t)$. Then the valuation sends a power series to the exponent of its lowest degree term.

Lemma 2.2.9

$$A \setminus \{0\} = \{x \in K : \nu(x) \geq 0\}$$

and

$$\mathfrak{m} \setminus \{0\} = \{x \in K : \nu(x) > 0\}$$

We omit the proof here, but this is not difficult to show.

Example 2.2.10

$\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the prime ideal (p), is a DVR, written as a set as

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \not| b \right\}$$

The associated p-adic valuation of this DVR $\nu_p : \mathbb{Q}^\times \to \mathbb{Z}$ sends an integer to the exponent of p in its prime decomposition, with the natural extension thereof to fractions. For example, $\nu_3(9) = 2$.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 3: 2 September

Professor Martin Olsson Abhishek Shivkumar

Discrete Valuation Rings

Lemma 3.1.1

Let K be a field, $\nu : K^\times \to \mathbb{Z}$ a surjective homomorphism such that $\nu(x+y) \geq \min(\nu(x), \nu(y))$. Then

$$A = \{x \in K^\times : \nu(x) \geq 0\} \cup \{0\}$$

is a DVR.

It's an easy exercise to show that A is a ring at all.

Also, the $\cup\{0\}$ portion of the statement of this lemma can be removed if one adopts the convention that $\nu(0) = \infty$.

Proof: We will proceed by showing that for any $\pi \in A$ such that $\nu(\pi) = 1$, any ideal $I \subseteq A$ is of the form $(\pi^r) = (\pi)^r$ for some r.

Let $I \subseteq A$ be a nonzero ideal, then the set

$$\{\nu(x) : x \in I \setminus \{0\}\} \subseteq \mathbb{Z}_{\geq 0}$$

has a minimal element, r, by the well-ordering property. Let $\alpha \in I$ be an element achieving this minimum. Then for all $x \in I \setminus \{0\}$, $\nu\left(\frac{x}{\alpha}\right) = \nu(x) - \nu(\alpha) \geq 0$ by assumption, so $\frac{x}{\alpha} \in A$. Therefore, since $x = \frac{x}{\alpha}\alpha$ and x is arbitrary in $I \setminus \{0\}$, we can see that $I = (\alpha)$.

Note that $a \in A$ such that $\nu(a) = 0$ are units, since $\nu(a^{-1}) = -\nu(a) = 0$, so $a^{-1} \in A$. Let $\pi \in A$ be an element with $\nu(\pi) = 1$ (by surjectivity), with $\nu(\alpha) = r$. Then $\nu\left(\frac{\alpha}{\pi^r}\right) = 0$ whence $\frac{\alpha}{\pi^r} \in A^\times$ so that $(\alpha) = (\pi^r)$ as claimed. ■

Example 3.1.2

Consider $k[[t]] \hookrightarrow k((t))$ (where $k((t))$ is the field of fractions for $k[[t]]$, the ring of finite-tailed Laurent series); the valuation on $k((t))$ sends a Laurent series to the smallest integer with nonzero coefficient in that series. For example, $\nu\left(\frac{\pi}{t^2} - \frac{1}{t} + t^{325}\right) = -2$.

Example 3.1.3

Consider $\nu_p : \mathbb{Q}^\times \to \mathbb{Z}$ the *p-adic* valuation, which sends $a \in \mathbb{Z}$ to the power of p occurring in the prime factorization of a, with its natural extension to fractions. The corresponding DVR by the above lemma

To see that the residue field of $\mathbb{Z}_{(p)}$ is $\mathbb{Z}/(p)$ without knowing any facts or universal properties about localization, note that $(p) \in \mathbb{Z}_{(p)}$ consists of reduced fractions with numerator divisible by p, so the quotient ring $\mathbb{Z}_{(p)}/(p)$ consists of elements $\frac{a}{b}$ up to terms of the form $p\frac{c}{d}$ where p does not divide a, b, or d. Choosing $d = b$, since p is relatively prime to a, for some choice of c, $d|pc{+}a$, hence the only information of elements in the quotient is the remainder of the numerator upon division by p.

is $\mathbb{Z}_{(p)}$, with uniformizer p, and residue field $\mathbb{F}_p = \mathbb{Z}/(p)$. To see the latter point, note that

$$\mathbb{Z}_{(p)}/(p) \cong (\mathbb{Z}/(p))_{(p)}$$

by exactness of localization, and the latter is isomorphic to $\mathbb{Z}/(p)$ since localizing doesn't do anything to a field.

Remark 3.1.4

Warning:

$$\mathbb{Z}_{(p)} \neq \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/(p^n)$$

The former is the localization of $\mathbb{Z}$ at (p), the latter are the p-adic integers.

Theorem 3.1.5

Let A be a noetherian integral domain. Then A is a DVR iff the following conditions hold:

1. A is integrally closed
2. A has a unique nonzero prime ideal

Proof: For the forward direction, if A is a DVR, the second condition is obvious. The content of this direction is to show that noetherian DVRs are integrally closed.

To that end, let K be the field of fractions of A, $x_1, \cdots, x_r \in K \setminus \{0\}$, with $\nu(x_i) > \nu(x_1)$ for $i > 1$. Then,

$$x_1 + \cdots + x_r \neq 0$$

To see this, divide the sum of the x_i by x_1, and obtain

$$1 + \frac{x_2}{x_1} + \cdots + \frac{x_r}{x_1}$$

Then all of the elements $\frac{x_i}{x_1}$ have strictly positive valuation, and are therefore contained in $\mathfrak{m}$, and therefore the above sum (which is 1 plus an element of $\mathfrak{m}$) is a unit, since the maximal contains all non-units of A, else, it could be made larger by adjoining non-units. Equivalently, if there is a non-unit in the complement of $\mathfrak{m}$, by the usual Zorn's lemma argument, it must be contained in some maximal, which is a contradiction since $\mathfrak{m}$ is unique.

By Zorn's lemma argument, I'm referring to the standard ring theoretic equivalent form of the axiom of choice, that every ideal is contained in some maximal ideal.

Then, let $x \in K \setminus \{0\}$ be integral over A, with

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

If $\nu(x) = s < 0$, e.g, $x \notin A$, then $\nu(x^n) = ns$, and $\nu(a_i x^i) = \nu(a_i) + is \geq is > ns$ where $\nu(a_i) \geq 0$ since $a_i \in A$. Then, by the result above,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 \neq 0$$

from which it follows that $\nu(x) \geq 0$, e.g, $x \in A$.

This is a very clever trick, I don't see why or how anyone would ever think of doing something like this.

For the reverse direction, the second condition tells us that A is a local ring with unique nonzero maximal ideal $\mathfrak{m}$. Then consider

$$\mathfrak{m}' := \{x \in K : x\mathfrak{m} \subseteq A\}$$

which is an A-submodule of K. Fix $y \in \mathfrak{m} \setminus \{0\}$, then multiplication by y induces a map $\mathfrak{m}' \hookrightarrow A$ (this map is an embedding since y is a unit in K). Therefore, $\mathfrak{m}' \subseteq y^{-1}A$, and since $y^{-1}A$ is a finitely generated A-module, since A is noetherian, $\mathfrak{m}'$ is a finitely generated A-module.

That submodules of finitely generated noetherian modules are themselves finitely generated is a standard result in commutative algebra that we don't prove here.

Therefore, by construction, $\mathfrak{m} \subseteq \mathfrak{m} \cdot \mathfrak{m}' \subseteq A$. There are two possibilities: $\mathfrak{m} \cdot \mathfrak{m}' = \mathfrak{m}$ or A by maximality of $\mathfrak{m}$. We will prove the following:

1. If $\mathfrak{m} \cdot \mathfrak{m}' = A$, then $\mathfrak{m}$ is principal
2. If $\mathfrak{m} \cdot \mathfrak{m}' = \mathfrak{m}$, then $\mathfrak{m}' = A$
3. $\mathfrak{m}' \neq A$

From these three results, it will follow that $\mathfrak{m} = (\pi)$ is principal, and therefore that A is a PID; the final implication follows from the fact that for any $x \in A$, $(x) = (\pi^r)$ for some r. To see this, if $x \notin A^\times$, $(x) \subseteq \mathfrak{m}$ by the fact that all ideals are contained in some maximal, and there's only one maximal ideal, then $x = x_1\pi$. Then, either x_1 is a unit, or $x_1 = x_2\pi$, and so on, and this chain either terminates, or

$$x \in \bigcap_{n \geq 0} \mathfrak{m}^n = (0)$$

where the above equality is a general fact about noetherian local rings that we will not show here.

This is a consequence of Krull's Intersection Theorem: if I is an ideal in a noetherian ring R, and I is contained in all maximal ideals of A, then $\bigcap_{n \geq 1} I^n = 0$.

Now we can prove our triplet of assertions to complete the proof:

1. If $\mathfrak{m} \cdot \mathfrak{m}' = A$, then
$$1 = \sum_i x_i y_i$$
with $x_i \in \mathfrak{m}$, $y_i \in \mathfrak{m}'$. Since $\mathfrak{m}$ is a proper ideal, at least one of the terms in the sum must be outside of $\mathfrak{m}$, so there most exist $x \in \mathfrak{m}$, $y \in \mathfrak{m}'$ such that $xy \in A \setminus \mathfrak{m} = A^\times$. Therefore, by multiplying x by a unit in A, we may assume that $xy = 1$. If $z \in \mathfrak{m}$, then $x(yz) = z$, but $yz \in A$ by the construction of $\mathfrak{m}'$, so $\mathfrak{m} = (x)$, since z was an arbitrary element of $\mathfrak{m}$ and $z \in (x)$.

The final step of this argument, which is omitted, is that $z \in (x)$ for $z \in \mathfrak{m}$ arbitrary implies $\mathfrak{m} \subseteq (x)$, which, by maximality, implies $\mathfrak{m} = (x)$.

2. If $\mathfrak{m} \cdot \mathfrak{m}' = \mathfrak{m}$, let $x \in \mathfrak{m}'$, where $x\mathfrak{m} \subseteq \mathfrak{m}$ by assumption. It follows that $x^n\mathfrak{m} \subseteq \mathfrak{m}$ for all $n \geq 0$, so $x^n \in \mathfrak{m}'$ for all $n \geq 0$. As we noted above, $\mathfrak{m}'$ is finitely generated, so the A-submodule M generated by x^n for $n \geq 0$

is finitely generated (since submodules of finitely generated noetherian modules are finitely generated). Say M is generated by $1, x, \cdots, x^r$ for some r, then we can write an equation

$$x^{r+1} + a_r x^r + \cdots + a_0 = 0$$

Since A is integrally closed, we can conclude that $x \in A$, so $\mathfrak{m}' = A$, since x was arbitrary.

3. Let $x \in \mathfrak{m} \setminus \{0\}$, with $A \subset A_x \subseteq K$ where the first inclusion is strict since A_x is a field. To see this, note that the prime ideals of A_x are the prime ideals of A which do not intersect the set $\{1, x, x^2, \cdots\}$; since the nonzero prime ideal of A is unique and contains x, the only prime of A_x is (0), from which it follows that A_x is a field. Moreover, $A_x = K$, since the field of fractions has the universal property of being the smallest field in which a given integral domain can be embedded.

   Thus, every element of K can be written as $\frac{y}{x^n}$ for some $y \in A$, some n. Fix $z \in A \setminus \{0\}$, with $\frac{1}{z} = \frac{y}{x^n} \iff x^n = yz \in (z) \subseteq A$. This implies that there exists N s.t $\mathfrak{m}^N \subseteq (z)$ since $\mathfrak{m}$ is finitely generated (since A is noetherian). In particular, if we write $\mathfrak{m} = (x_1, \cdots, x_r)$, then $\mathfrak{m}^N$ has as generators monomials in the x_i whose exponents sum to N. By making N sufficiently large, at least one exponent in each monomial will therefore be large enough so that $x_i^n \in (z)$.

   Applying this result with $z \in \mathfrak{m}$, we can see that there exists a smallest choice of N s.t $\mathfrak{m}^N \subseteq (z)$, so $\mathfrak{m}^{N-1} \not\subseteq (z)$. Fix $y \in \mathfrak{m}^{N-1}$, $y \notin (z)$, with $y\mathfrak{m} \subseteq (z)$ by assumption. Therefore, $\frac{y}{z} \in \mathfrak{m}'$ and $\frac{y}{z} \notin A$, since $z \in \mathfrak{m}$ implies that z is a non-unit, from which it follows that $\mathfrak{m}' \neq A$.

■

Addendum

These are a couple useful results from Milne and Neukirch that I came across while doing homework; including them here for completeness.

Proposition 3.2.1

Let K be the field of fractions of A, L a field containing K. If $\alpha \in L$ is algebraic over K, then there exists nonzero $d \in A$ such that $d\alpha$ is integral over K.

Proof: Let α satisfy

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

by assumption, with $a_i \in K$. Let d be a common denominator for the a_i, so that $da_i \in A$ for all i, and multiply through by d^n:

$$(d\alpha)^n + a_{n-1}d(d\alpha)^{n-1} + \cdots + a_0 d^n = 0$$

Therefore, $d\alpha$ satisfies an integral equation with coefficients in a since $da_i \in A$. ■

Corollary 3.2.2

Let A be an integral domain with field of fractions K, B the integral closure of A in a field L containing K. If L is algebraic over K, then L is the field of fractions of B.

Proof: Since every $\alpha \in L$ is algebraic over K, by the above proposition, $d\alpha \in B$ for some nonzero $d \in A$, so each $\alpha \in L$ can be written as $\alpha = \frac{\beta}{d}$ where $\beta \in B$, which is precisely a description of the field of fractions of B (since K is the field of fractions for A, L a finite extension of K, only the denominators change for the field of fractions of B). ■

Proposition 3.2.3

Let K be the field of fractions of A integrally closed, L a finite extension of K. $\alpha \in L$ is integral over A iff its minimal polynomial over K has coefficients in A.

Proof: Let $\alpha \in L$ be integral over A satisfying

$$\mathfrak{g}(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$. Let $f \in K[x]$ be the minimal polynomial of α over K. Then, by definition, f divides g in $K[x]$, so all the zeros of f are zeros of g, and therefore, are integral over A.

Therefore, since f splits into linear factors

$$f(x) = (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_n)$$

in some field extension, with α and all the α_i integral over A by the above argument, we know that the coefficients of f are symmetric functions of the roots, e.g, sums and products of the roots. Since integral elements form a ring, the coefficients themselves are integral over A. Since A is integrally closed, the coefficients are in A, from which the forward direction follows.

Conversely, if the minimal polynomial of α over K has coefficients in A, then α is integral over A by definition. ■

The following are homework problems that we end up invoking in later proofs.

Proposition 3.2.4

Let A be an integral domain with field of fractions K, and let L/K be a finite field extension. Let B be the integral closure of A in L. If S is a multiplicative subset of A, then the integral closure of $S^{-1}A$ in L is $S^{-1}B$.

Proof: Let C be the integral closure of $S^{-1}A$ in L. It is clear that $S^{-1}B \subseteq C$, since if $b \in B$ satisfies the integral equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

$\frac{b}{s} \in S^{-1}B$ satisfies the following integral equation over $S^{-1}A$, *not* A:

$$\frac{b^n}{s^n} + \frac{a_{n-1}}{s}\frac{b^{n-1}}{s^{n-1}} + \frac{a_{n-2}}{s^2}\frac{b^{n-2}}{s^{n-2}} + \cdots + \frac{a_0}{s^n} = 0$$

Moreover, we can show that $C \subseteq S^{-1}B$; note by Corollary 3.2.2 above that L is the field of fractions of B. Let $c \in C$, with the following integral equation over $S^{-1}A$:

$$c^n + \frac{a_{n-1}}{s_{n-1}}c^{n-1} + \cdots + \frac{a_0}{s_0} = 0$$

Since $c \in L$, we can write $c = \frac{b}{a}$ with $b \in B$, $a \in A$, whence our equation becomes

$$\frac{b^n}{a^n} + \frac{a_{n-1}}{s_{n-1}}\frac{b^{n-1}}{a^{n-1}} + \cdots + \frac{a_0}{s_0} = 0$$

We want to show that $a \in S$, from which the result follows; to that end, we rearrange our equation as

$$b^n = -a\left[\frac{a_{n-1}}{s_{n-1}}b^{n-1} + \frac{a_{n-2}}{s_{n-2}}b^{n-2}a + \cdots + \frac{a_0}{s_0}a^{n-1}\right]$$

The left hand side is in B, so the right hand side must be as well. The common denominator of the bracketed expression is in S, and a must clear it so that the right hand side can be in B, so we must have that $a \in S$. Therefore $c = \frac{b}{a} \in S^{-1}B$ as claimed. ■

Proposition 3.2.5

Let A be an integrally closed domain with field of fractions K. If a monic polynomial $f(x) \in A[x]$ is reducible in $K[x]$, then $f(x)$ is reducible in $A[x]$.

Proof: Fix

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$$

which is reducible in $K[x]$, e.g, f factors (possibly non uniquely) as

$$f = g_1 \cdots g_n$$

with g_i monic irreducible polynomials by moving units among the factors. Let α be a zero of g_i in some extension of K. Since g_i is irreducible, g_i is a minimal polynomial for α; moreover, since α is a root of f, α is integral over A. Therefore, by Proposition 3.2.3 above, g_i has coefficients in A. ■

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 4: 9 September

Professor Martin Olsson Abhishek Shivkumar

Dedekind Domains

As we've discussed before, the primary focus of this course is finite extensions of $\mathbb{Q}$ (e.g, number fields) and their rings of integers. It turns out that the ring of integers for a number field is a *Dedekind domain*, satisfying the nice property that its localizations at nonzero primes are DVRs.

Definition 4.1.1: Dedekind Domains

A *Dedekind domain* is a noetherian integral domain which is integrally closed and of dimension one, e.g, every nonzero prime ideal is maximal.

Remark 4.1.2

The only "type" of Dedekind domain we're going to encounter in this course are rings of integers, another important type of Dedekind domains is given by $\Gamma(C, \mathcal{O}_C)$ where C is a smooth affine curve over a field k.

Proposition 4.1.3

For a noetherian integral domain A, A is a Dedekind domain iff for all nonzero prime ideals $\mathfrak{p} \subset A$, $A_\mathfrak{p}$ is a DVR.

Proof: Suppose A is a Dedekind domain, $\mathfrak{p}$ a nonzero prime ideal. By Proposition 3.2.4, $A_\mathfrak{p}$ is integrally closed. Therefore, by Theorem 3.1.5 we need to check only that $A_\mathfrak{p}$ has a unique prime ideal. But prime ideals in $A_\mathfrak{p}$ correspond to prime ideals in A contained in $\mathfrak{p}$ (e.g, not meeting the complement of $\mathfrak{p}$). Since A is dimension one by assumption, there can only exist one such prime, $\mathfrak{p}$ itself.

There's some discussion about why the primes in a localization are in bijection with primes in the original ring not meeting the multiplicatively closed set. This is a fairly standard result that's not hard to show, so I'm not going to discuss it here.

Also some clarification here that the complement of nonzero primes is a multiplicative subset, mostly review.

For the other direction, suppose $A_\mathfrak{p}$ is a DVR for each prime $\mathfrak{p}$. To see that A is one dimensional, suppose $\mathfrak{p} \subseteq \mathfrak{p}'$, then $\mathfrak{p}$ corresponds to a prime ideal in $A_{\mathfrak{p}'}$, hence $\mathfrak{p} = \mathfrak{p}'$.

To see that A is integrally closed, suppose $a \in K$ is integral over A, with K the field of fractions of A. Then $a \in \bigcap_\mathfrak{p} A_\mathfrak{p} \subset K$ where the intersection is taken over all primes $\mathfrak{p}$; to see this, note that since a is integral over A via a monic equation with coefficients in K, then the same equation shows that a is integral over each $A_\mathfrak{p}$. Since $A_\mathfrak{p}$ is integrally closed as above, $a \in A_\mathfrak{p}$ for each prime $\mathfrak{p}$, from which the result follows.

Then, let $I = \{x \in A : xa \in A\} \subseteq A$. This is clearly an ideal of A, and $I_\mathfrak{p} = A_\mathfrak{p}$ for all primes $\mathfrak{p}$ by the above argument, so I is not contained in any prime $\mathfrak{p}$ (else I would be a strict ideal of some $A_\mathfrak{p}$). Therefore, since A is one dimensional by the above argument, $I = A$, as every *proper* ideal must be contained in some prime (equivalently, maximal) ideal. ■

We will often omit the prefix "nonzero" when discussing prime ideals; hopefully, the correct interpretation is clear from context.

Definition 4.1.4: Fractional Ideals

Let A be a Dedekind domain, K its field of fractions. A *fractional ideal* is a finitely generated A-submodule $\mathfrak{a} \subseteq K$. Equivalently, $\mathfrak{a} \subseteq K$ is a fractional ideal of A if there exists $d \in A$ such that $d \cdot \mathfrak{a} \subseteq A$.

Given a fractional ideal $\mathfrak{a}$, define $\mathfrak{a}' = \{x \in K : x\mathfrak{a} \subseteq A\}$. If $\sigma \in \mathfrak{a}$ is nonzero, then we have a map $\mathfrak{a}' \hookrightarrow A$ given by $x \mapsto x\sigma$, from which it follows that $\mathfrak{a}'$ is finitely generated, since this map is an embedding and submodules of noetherian modules are finitely generated.

Proposition 4.1.5

With $\mathfrak{a}$ and $\mathfrak{a}'$ defined as above, $\mathfrak{a}\mathfrak{a}' = A$.

Proof: Let $\mathfrak{p} \subset A$ be a nonzero prime ideal. Then $(\mathfrak{a}_\mathfrak{p})' = (\mathfrak{a}')_\mathfrak{p}$, that is, the inverse of the localization of $\mathfrak{a}$ is the localization of the inverse. To see this, note the fact (or definition) that $\mathfrak{a}_\mathfrak{p} = A_\mathfrak{p}\mathfrak{a}' \subseteq K$; then, we have that

$$(\mathfrak{a}')_\mathfrak{p} = A_\mathfrak{p} \cdot \{x \in K : x\mathfrak{a} \subseteq A\} \quad (\mathfrak{a}_\mathfrak{p})' = \{x \in K : xA_\mathfrak{p}a \subseteq A\}$$

The latter set is clearly equal to $A_\mathfrak{p}\mathfrak{a}'$ from which the result follows.

Not super sure of the minutiae of this proof, but something like this should be the answer.

Therefore, if we can check this result at each localization, the "global" result would follow; suppose $\mathfrak{a}_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})' = A_\mathfrak{p}$ for each nonzero prime $\mathfrak{p}$, then consider $A/\mathfrak{a}'$, since $\mathfrak{a}' \subseteq A$ by construction and form an ideal since $\mathfrak{a}$ is an A-submodule. Here, we invoke an elementary result in commutative algebra: a module M over a commutative ring is zero iff $M_\mathfrak{p} = 0$ for all primes $\mathfrak{p}$ in the base ring. Applying this to $A/\mathfrak{a}'$, together with some basic lemmas about localizing quotients, the result follows.

I am not super sure of this line of reasoning either, I didn't work out all the details.

Hence, we may reduce to the case where A is a DVR; however, we know that $\mathfrak{a} = \mathfrak{m}^r = (\pi)^r$ for some r by previous results, and it is clear by our definition of $\mathfrak{a}'$ that $\mathfrak{a}' = (\pi^{-r})$, from which the result follows. ■

Corollary 4.1.6

The fractional ideals of a Dedekind domain form a group.

Note that there is a map from $K^\times$ to the group of fractional ideals, via $x \mapsto x \cdot A \subseteq K$. These ideals are called *principal.*

Note that there's a small point of concern when thinking of number fields as being embedded in $\mathbb{C}$, as the embedding is not usually unique. We can usually avoid this by regarding the number field in question as a polynomial ring over $\mathbb{Q}$ modulo minimal polynomials, thereby declining to provide an explicit embedding.

Definition 4.1.7: Ideal Class Group

The *ideal class group* or *class group* of a Dedekind domain A (denoted $\mathrm{Cl}(A)$) is the quotient of the group of fractional ideals by the group of principal fractional ideals. Equivalently, it is the cokernel of the map described above.

Example 4.1.8

Let D be a square-free integer, $k = \mathbb{Q}(\sqrt{D}) \cong \mathbb{Q}[x]/(x^2 - D) \subset \mathbb{C}$. We claim that

$$\mathcal{O}_k = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \pmod 4 \end{cases}$$

To see this, note that the minimal polynomial of $\alpha = a + b\sqrt{D}$ with b nonzero is

$$(x - (a + b\sqrt{D}))(x - (a - b\sqrt{D})) = x^2 - 2ax + (a^2 - Db^2)$$

so if $a, b \in \mathbb{Z}$, $\alpha \in \mathcal{O}_k$. However, we only need that $2a \in \mathbb{Z}$, so if $a = \frac{a'}{2}$ for $a' \in \mathbb{Z}$, then, writing $b = \frac{b'}{2}$, for $a^2 - Db^2$ to be an integer, we need $Db'^2 \equiv a'^2 \pmod 4$. Clearly, since D is square-free, $D \not\equiv 0 \pmod 4$; if $D \equiv 2, 3 \pmod 4$, since $x^2 \equiv 0, 1 \pmod 4$ for $x \in \mathbb{Z}$, by casework, one can see that the only solution is $a' \equiv b' \equiv 0 \pmod 2$ whence $a, b \in \mathbb{Z}$. The $D \equiv 1 \pmod 4$ case is similar; $a' \equiv b' \equiv 0, 1 \pmod 2$. The former case gives $\mathbb{Z} \subset \mathcal{O}_k$, the latter gives $\frac{a+b\sqrt{D}}{2} \in \mathcal{O}_k$.

There was some discussion here that I didn't completely follow of the field automorphism $\sigma : k \to k$ given by $\sqrt{D} \to -\sqrt{D}$ and using it to prove the given result on $\mathcal{O}_k$; in particular, $2a = \alpha + \sigma(\alpha)$ and $a^2 - Db^2 = \alpha\sigma(\alpha)$, so $\mathcal{O}_k$ consists of those α such that $\alpha + \sigma(\alpha)$ and $\alpha\sigma(\alpha)$ lie in $\mathbb{Z}$ (I think these are the field trace and norm, respectively).

Example 4.1.9

Let $k = \mathbb{Q}(\sqrt{-5})$; since $-5 \equiv 3 \pmod 4$, by the above example, $\mathcal{O}_k = \mathbb{Z}[\sqrt{-5}]$. What is $\mathrm{Cl}(\mathcal{O}_k)$? We can't calculate it yet, but we can show that it's nontrivial; the ideal $I = (2, 1 + \sqrt{-5}) \subset \mathcal{O}_k$ is non-principal, and $I^2 = (2)$, so $(2, 1 + \sqrt{-5})$ represents a nontrivial class in $\mathrm{Cl}(\mathcal{O}_k)$ which squares to the identity, e.g, $\mathbb{Z}/(2) \subseteq \mathrm{Cl}(\mathcal{O}_k)$. We will later see that, in fact, $\mathbb{Z}/(2) = \mathrm{Cl}(\mathcal{O}_k)$.

Note that by abuse of notation, we will often write $\mathrm{Cl}(k)$ instead of $\mathrm{Cl}(\mathcal{O}_k)$ when k is a number field. Also note that

$$\mathrm{Cl}(\mathcal{O}_k) = \mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_k))$$

where Pic denotes the Picard group of a scheme (or more generally, a ringed space).

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 5: 14 September

Professor Martin Olsson Abhishek Shivkumar

Field Norm and Trace

Example 5.1.1

Let A be a DVR with maximal $\mathfrak{m}$, then its fractional ideals are of the form $\mathfrak{m}^n$ for $n \in \mathbb{Z}$. This follows from the fact that for each fractional ideal $\mathfrak{a}$ of A, there exists $x \in A$ such that $x\mathfrak{a}$ is an ideal of A, e.g, $x\mathfrak{a} = \mathfrak{m}^k$ for some $k \in \mathbb{N}$. $x \in \mathfrak{m}^r$ for a unique $r \in \mathbb{N}$ (where $\mathbb{N}$ includes 0), from which it follows that $\mathfrak{a} = \mathfrak{m}^{k-r}$.

Note that DVRs form a sort of trivial class of Dedekind domains. DVRs do not have interesting class group, since all fractional ideals are principal.

Lemma 5.1.2

Let A be a Dedekind domain, then any fractional ideal $\mathfrak{a}$ can be written as

$$\mathfrak{a} = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}$$

where $\nu_\mathfrak{p}(\mathfrak{a}) = 0$ for all but finitely many primes $\mathfrak{p}$.

Proof: We will only sketch this result, assuming that $\nu_\mathfrak{p}(\mathfrak{a}) = 0$ for all but finitely many primes $\mathfrak{p}$; note that $\mathfrak{a}_\mathfrak{p} = A_\mathfrak{p}\mathfrak{a} = (\mathfrak{a}_\mathfrak{p}\mathfrak{p})^{\nu_\mathfrak{p}(\mathfrak{a})}$ by the example above, since $A_\mathfrak{p}$ is a DVR, with $A_\mathfrak{p}\mathfrak{p}$ its maximal ideal. Then, using the elementary commutative algebra result that a module is zero iff all of its localizations at primes are zero, the equality follows. ■

I'd like to add more to this proof at some point. I'm not sure how much more there is to it, but the $\nu_\mathfrak{p}(I) = 0$ for all but finitely many primes $\mathfrak{p}$ assertion seems nonobvious. These lecture notes (linked) have a good outline of the proof, might come back and fill in some details.

Definition 5.1.3: Trace and Norm

Let L/K be a finite extension of fields, $\alpha \in L$, and consider the map $\cdot\alpha : L \to L$ given by multiplication by L. This is a K-linear map of finite dimensional K vector spaces, so we may define

$$\mathrm{tr}_{L/K}(a) := \mathrm{tr}(\cdot a : L \to L) \in K \quad N_{L/K}(a) := \det(\cdot a : L \to L) \in K$$

the *trace* and *norm* respectively of $a \in L$ with respect to K.

Example 5.1.4

Consider $\mathbb{C}/\mathbb{R}$, with $\mathbb{C} = \mathbb{R} \oplus \mathbb{R} \cdot i$, with $a \in \mathbb{C}$, $a = \alpha + \beta i$. Then the matrix of a with the standard basis of $\mathbb{C}$ over $\mathbb{R}$ is $\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ with trace $2\alpha = a + \overline{a}$ and determinant (norm) $\alpha^2 + \beta^2 = a\overline{a}$.

Theorem 5.1.5

L/K is separable iff $\mathrm{tr}_{L/K} : L \to K$ is nonzero.

Recall that a field extension L/K is separable if, for any algebraic closure $\overline{K}$ of K, the cardinality of the set of K-linear embeddings $L \hookrightarrow \overline{K}$ is equal to $[L : K]$. With this in mind, the proof of the above theorem will follow over the course of the next few lemmas.

There are many different equivalent formulations of separable extensions, but this is the one that will help us in this proof. As a guiding example, let $L = K[x]/(p)$ with p irreducible, then this formulation of separable is equivalent to the assertion that the roots of p are distinct in in $\overline{K}$, which is the normal definition of separable extensions.

Lemma 5.1.6

Let M be a finitely generated torsion free A-module, A a PID. Then M is a free module.

Proof: Note that this follows directly from the structure theorem for finitely generated modules over a PID. Without that result, we can prove this result as follows: since M is finitely generated and torsion free, there is an inclusion $M \hookrightarrow A^r$ for some r given by picking generators for M and looking at the coefficients.

There's some business here about M embedding into $M \otimes_A K$, didn't really follow it. Doesn't seem important to the result.

Then, we can show that, in fact, $M = A^r$ by induction. When $r = 1$, $M \hookrightarrow A$ is an ideal, so $M = (\alpha)$, so there is an A-linear isomorphism $A \xrightarrow[\cdot\alpha]{\sim} M$. Assume the result holds for all $s < r$, that is, if M embeds into A^s, then M is free of rank $\leq s$. Then, let $\pi : A^r \to A^{r-1}$ be the projection onto the last $r - 1$ coordinates, e.g,

$$\pi(a_1, \cdots, a_r) = (a_2, \cdots, a_r)$$

and let $M' = \pi(M) \subseteq A^{r-1}$, $M'' = \ker(M \to M')$. With these modules defined, we have the following diagram:

Note that $\pi(M)$ is meant to mean the image of the image of M in A^r under π.

$$\begin{tikzcd}
0 \arrow[r] & M'' \arrow[r] \arrow[d, hook, dashed] & M \arrow[r] \arrow[d, hook] & M' \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & A \arrow[r] & A^r \arrow[r, "\pi"] & A^{r-1} \arrow[r] & 0
\end{tikzcd}$$

Recall that the splitting lemma states that, given a short exact sequence

$$0 \to A \to B \to C \to 0$$

having a left split (a morphism $B \to A$ composing to id_A) is equivalent to having a right split (a morphism $C \to B$ composing to id_C) which in turn is equivalent to $B \cong A \oplus C$.

The embedding in the first column is the natural one, given that $M'' \subseteq A^r$ consists of elements of the form $(a_1, 0, \cdots, 0)$. By the inductive hypothesis, $M'' = A$ or $M'' = 0$. In the latter case, $M \cong M'$ which embeds into A^{r-1}, in which case the result follows by induction. In the former case, by the splitting lemma (since $M \to M'$ has an obvious splitting morphism), we can pick a basis for M' (again by induction) and for M, from which the result follows. ■

I wonder if a five lemma argument would work for this proof; there's the small issue of the induction ensuring bounded rank without specifying the rank.

Example 5.1.7

Let k be a degree n number field, then $\mathcal{O}_k$ is a free $\mathbb{Z}$-module of rank n (we will later show that $\mathcal{O}_k$ is a finitely generated $\mathbb{Z}$-module, which we need to apply the result above). More generally, this implies that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module for a finite separable extension L/K.

Lemma 5.1.8

Let $K \hookrightarrow M \hookrightarrow L$ be a sequence of finite field extensions. Then $\operatorname{tr}_{L/K} = \operatorname{tr}_{M/K} \circ \operatorname{tr}_{L/M}$.

Proof: Let V be a finite dimensional M vector space, $a : V \to V$ an M-linear transformation. Then $\operatorname{tr}_{V,K}(a) = \operatorname{tr}_{M/K}(\operatorname{tr}_{V,M}(a))$ where the traces involving V are the ordinary trace from linear algebra. To see that the above equality holds, note that both sides are K-linear in a, so if we choose a basis (and therefore write $V = M^r$ for some r), it is suffices to prove the equality for $a = e_{ij}$ the matrix with a 1 in the i, j position, and 0s everywhere else.

This is because an arbitrary linear transformation a can be written as a finite linear combination of the e_{ij}s.

In the case where $i \neq j$, both sides are vacuously 0. If $i = j$, then the left hand side is $\operatorname{tr}_{V,K}(e_{ii}) = [M : K]$, and the right hand side is $\operatorname{tr}_{M/K}(1) = [M : K]$, from which the result follows. ■

That $\operatorname{tr}_{V,K}(e_{ii}) = [M : K]$ and $\operatorname{tr}_{M/K}(1) = [M : K]$ is obvious by picking a basis for M over K and writing out matrices; this is also probably obvious without picking bases, just not obviously obvious.

Remark 5.1.9

Note that $\operatorname{tr}_{L/K}$ is nonzero for a finite field extension L/K iff $\operatorname{tr}_{L/K} : L \to K$ is surjective (by K-linearity). Therefore, in the situation above with $K \hookrightarrow M \hookrightarrow L$, if $\operatorname{tr}_{L/M} \neq 0$ and $\operatorname{tr}_{M/K} \neq 0$, then $\operatorname{tr}_{L/K} \neq 0$.

I don't really understand the purpose of this remark.

We will use, but not prove, the following fact from field theory: all finite extensions factor as separable and purely inseparable, as in $K \hookrightarrow L$ factors as $K \hookrightarrow K^S \hookrightarrow L$ where the first inclusion is separable, the second, purely inseparable. By purely inseparable, we mean that each $\alpha \in L$ raised to some power of p is an element of K^S, where p is the characteristic of all fields being discussed. The terminology "purely inseparable" is justified; given $\alpha \in L$ with $\alpha^{p^k} \in K^S$,

$$x^{p^k} - \alpha^{p^k} = (x - \alpha)^{p^k}$$

E.g, the minimal polynomial for α over K^S has only one root: α.

There's really only one "kind" of purely inseparable extension, $L = K\left(\alpha^{\frac{1}{p}}\right)$ and chains thereof where $\alpha \in K$, p the characteristic of L and K. It's clear (I think) that one can get prime powers in the exponent of α by taking chains of such extensions.

Let's show that $\operatorname{tr}_{L/K} = 0$ if $[L : K^s] > 1$. It suffices to show by Lemma 5.1.8 that $\operatorname{tr}_{L_i/L_{i-1}}$ is zero for some i in the chain

$$K^S \subset L_1 \subset L_2 \subset \cdots \subset L_r = L$$

where $L_i = L_{i-1}(\alpha^{\frac{1}{p}})$, $\alpha \in L_{i-1}$. It is enough to show that $\operatorname{tr}\left(\left(\alpha^{\frac{1}{p}}\right)^s\right) = 0$ for each s since these powers form a basis for L_i/L_{i-1}. When $s = 0$, the corresponding matrix is the $p \times p$ identity which has trace 0 since we're working in characteristic p.

For $s > 0$, note that $x \mapsto x^s$ permutes (without fixed points) the set $\left\{\alpha^{\frac{1}{p}}, \alpha^{\frac{2}{p}}, \cdots, \alpha^{\frac{p-1}{p}}\right\}$, so the corresponding matrix is a permutation matrix with all zeros on the diagonal, whence the trace is zero.

Therefore $\mathrm{tr}_{L/K} = 0$ unless L/K is separable; then, we want to show that $\mathrm{tr}_{L/K} \neq 0$ when L/K is separable. To that end, fix $K \hookrightarrow \overline{K}$, then

$$L \otimes_K \overline{K} \cong \prod_{\sigma : L \hookrightarrow \overline{K}} \overline{K}$$

as $\overline{K}$-algebras, where the product is taken over all K-linear embeddings $\sigma : L \hookrightarrow \overline{K}$. This isomorphism follows from the fact that $L = K[x]/(p)$ by separability, so

$$L \otimes_K \overline{K} \cong \overline{K}[x]/(p)$$

and $p(x)$ splits into linear factors over $\overline{K}$ by algebraic closure. Each linear factor of this splitting defines an element of the product on the right hand side above via the Chinese remainder theorem, since there are as many roots of L in $\overline{K}$ as $\deg p = [L : K]$ which is, by separability, equal to the number of embeddings $\sigma : L \hookrightarrow \overline{K}$.

I'm not sure if there's a direct natural bijection between roots of p in $\overline{K}$ and embeddings $\sigma : L \hookrightarrow \overline{K}$. For example, with $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$, the two roots seem to naturally correspond to the identity and conjugate embeddings of $\mathbb{C}$ into itself.

Then, we claim that

$$\mathrm{tr}_{L/K}(a) = \sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(a)$$

To see this, consider $\mathrm{tr}_{L/K} \otimes_K \overline{K} : L \otimes_K \overline{K} \to \overline{K}$ the extension of $\mathrm{tr}_{L/K}$ to $\prod_{\sigma : L \hookrightarrow \overline{K}} \overline{K}$. It is an easy exercise to show that this extension is in fact the trace map on $\prod_{\sigma : L \hookrightarrow \overline{K}} \overline{K}$ over $\overline{K}$, and is given by

$$\mathrm{tr}_{L/K} \otimes_K \overline{K}(a_1, \cdots, a_n) = a_1 + \cdots + a_n$$

This is clearly nonzero in general, and therefore surjective, and since field extensions are faithfully flat, $\mathrm{tr}_{L/K}$ is surjective as well, from which it follows that $\mathrm{tr}_{L/K}$ is nonzero, which completes the proof. Moreover, since $\mathrm{tr}_{L/K} \otimes_K \overline{K}$ extends $\mathrm{tr}_{L/K}$, it follows that

$$\mathrm{tr}_{L/K}(a) = \sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(a)$$

by evaluating the trace of $a \in L$ as the trace of $a \otimes 1$ in $L \otimes_K \overline{K}$.

There are a lot of missing steps in this argument; we assume many results from field theory and about traces, and the exposition could be cleaned up a lot. I don't really understand why we tensor up to $L \otimes_K \overline{K}$. I also don't really see how we've shown that $\mathrm{tr}_{L/K} \otimes_K \overline{K}$ is nonzero.

Professor Olsson later said that what we achieve by tensoring up by $\overline{K}$ is "diagonalizing the multiplication map."

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 6: 16 September

Professor Martin Olsson Abhishek Shivkumar

Dedekind Extensions

Remark 6.1.1

If $A \subseteq K$ integrally closed in its field of fractions K, $B \subseteq L$ the integral closure of A in L a finite separable field extension of K, then $\mathrm{tr}_{L/K} : B \to A$. To see this, fix an algebraic closure $K \hookrightarrow \overline{K}$; then for any $b \in B$, any $\sigma : L \hookrightarrow \overline{K}$, $\sigma(b)$ is integral over A (since σ fixes K, the integral equation for b is the integral equation for $\sigma(b)$) so $\mathrm{tr}_{L/K}(b) = \sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(b) \in K$ is integral over A and contained in K, hence is in A itself.

Theorem 6.1.2

Let A be a noetherian integrally closed domain, K its field of fractions, L/K separable and finite; then the integral closure B of A in L is a finitely generated A-module.

Proof: The idea of this proof is to produce an inclusion $B \hookrightarrow M$ where M is finitely generated; then, since submodules of finitely generated modules over a noetherian ring are finitely generated, the result will follow. Choose $e_1, \cdots, e_d \in B$ which form a basis for L/K; to do this, first choose a basis for L over K, then, by the proof of Corollary 3.2.2, L is the field of fractions for B, and consists of elements of the form $\frac{b}{a}$, $b \in B$, $a \in A$. Then, one can "clear the denominators" of this basis (since the denominators may be absorbed into the K-coefficients) to obtain a basis in B of L. This induces in a natural way a morphism $A^d \hookrightarrow B$ given by looking at the span of the e_i with A-coefficients.

I'm not sure about this whole section, especially the last part. Is this the morphism Professor Olsson described? It's the only one I can think of.

Define

$$B^* = \{b \in L : \mathrm{tr}(b\alpha) \in A \ \forall \alpha \in B\}$$

and

$$(A^d)^* = \{b \in L : \mathrm{tr}(b\alpha) \in A \ \forall \alpha \in A^d\}$$

Note that $(b, \alpha) \mapsto \mathrm{tr}(b\alpha)$ defines a nonzero inner product from $L \times L$ to K, and induces an isomorphism $L \xrightarrow{\sim} L^*$; this was written down in our lecture notes but I don't see how it connects to anything that follows. Maybe I need to justify $(A^d)^*$ being free a little more.

Note that $B \subseteq B^*$ by the above remark on traces, so we have $A^d \subseteq B \subseteq B^* \subseteq (A^d)^*$ where $B^* \subseteq (A^d)^*$ by construction since $B \subseteq L$. However, A^d

is a free module of rank d, and therefore, so is $(A^d)^*$; then B is contained in a free (and therefore finitely generated) module, from which the result follows by the noetherian assumption.

The above is the proof that Professor Olsson covered in class; Eunice raised several points of confusion within it, so I've included the following alternative proof from Milne. What follows complements the above proof by showing that $(A^d)^*$ as described is in fact the dual of A^d.

Alternatively, we may pick a dual basis e_i^* of L/K such that $\mathrm{Tr}\big(e_ie_j^*\big) = \delta_{ij}$, and show that $A^d \subseteq B \subseteq A^d$ where the latter A^d is generated by the dual basis. To see the latter inclusion, fix $\beta = \sum_i b_ie_i^* \in B$ with $b_i \in K$. If we show that $b_i \in A$, the result follows. As the e_i are in B, so is βe_i, and so $\mathrm{Tr}(\beta e_i) \in A$. But we have that

$$\mathrm{Tr}(\beta e_i) = \mathrm{Tr}\left(\sum_j b_je_j^*e_i\right) = \sum_j b_j\,\mathrm{Tr}\big(e_j^*e_i\big) = \sum_j b_j\delta_{ij} = b_i$$

hence $b_i \in A$ for each i, from which the result follows, again by the noetherian assumption. ■

Remark 6.1.3

Note that B^* is a finitely generated A-module in L, e.g, a fractional ideal for B (assuming A Dedekind). Its inverse is called *different*, which we will revisit when we discuss ramification.

Corollary 6.1.4

Let A be a Dedekind domain, then so is B with B, L, and K as above.

Proof: Since B is a finitely generated A-module, B is noetherian, integrally closed, so we only need to show that every nonzero prime ideal is maximal. This follows from the following general fact: if $A \hookrightarrow B$ is an integral extension, $\mathfrak{p} \subseteq \mathfrak{q}$ an inclusion of prime ideals of B and $\mathfrak{p} \cap A = \mathfrak{q} \cap A$, then $\mathfrak{p} = \mathfrak{q}$. In this direction, consider the natural embedding $A/(\mathfrak{p} \cap A) \hookrightarrow B/\mathfrak{p}$; we will show that $\mathfrak{q} = 0$ in $B/\mathfrak{p}$.

To see this, if $\mathfrak{q} \neq 0$, choose $x \in \mathfrak{q} \setminus \{0\}$ and consider the integral equation

$$x^n + \cdots + a_0 = 0$$

with $a_0 \neq 0$; then we can rewrite

$$a_0 = -a_1x - \cdots - x^n \in A \cap \mathfrak{q}$$

so $A \cap \mathfrak{q} \ni a_0$. However, by assumption, $A \cap \mathfrak{q} = A \cap \mathfrak{p}$, so $a_0 = 0$, which is a contradiction, from which the result follows. ■

Exercise 6.1.5

Show that

$$(A/\mathfrak{p})_{\mathfrak{p}} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$$

and that $A/\mathfrak{p} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ for A Dedekind.

Professor Olsson solved the latter statement of this exercise via the universal property of localization; I prefer to show the former statement (which boils down to localization being an exact functor in the category of modules over A), and use it to infer the latter statement from the fact that $A/\mathfrak{p}$ must be a field anyway in Dedekind domain, since primes are maximal, so there is nothing left to localize.

Theorem 6.1.6: Fundamental Identity

Let A be a Dedekind domain, K its field of fractions, L/K a separable extension, B the integral closure of A in L (and therefore Dedekind). Then, given $\mathfrak{p} \subset A$ a nonzero prime ideal, a prime ideal $\mathfrak{q} \subset B$ *divides* $\mathfrak{p}$, denoted $\mathfrak{q}|\mathfrak{p}$ if $\mathfrak{p}B \subseteq \mathfrak{q}$ or, equivalently, $\mathfrak{p} = \mathfrak{q} \cap A$. Writing

$$\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$$

by the unique factorization of ideals in B, define $f_\mathfrak{q}$ as the degree of field extension given by the natural map $A/\mathfrak{p} \to B/\mathfrak{q}$. Then, if $[L : K] = n$,

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

Takes a little work to see that $\mathfrak{p}B \subseteq \mathfrak{q}$ is equivalent to $\mathfrak{p} = \mathfrak{q} \cap A$.

Example 6.1.7

Consider $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ with D square free, and $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$, then we want to find the ways in which we can write

$$2 = \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q}$$

where the primes are taken in the respective rings of integers.

Clearly, without choosing $\mathfrak{p}$ the only ways to obtain 2 as a sum of positive integers is as $1 + 1$ or 2, which factor as $1 \cdot 1 + 1 \cdot 1$ and $2 \cdot 1$ respectively in the above formulation (up to combinatorics).

Below, we follow the proof in Neukirch.

Proof: By the Chinese remainder theorem,

$$B/\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} B/(\mathfrak{q}^{e_\mathfrak{q}})$$

as a vector space of dimension n over $A/\mathfrak{p}$. Then, setting $k = A/\mathfrak{p}$ we want to show that

$$\dim_k B/\mathfrak{p}B = n \text{ and } \dim_k(B/(\mathfrak{q}^{e_\mathfrak{q}})) = f_\mathfrak{q} e_\mathfrak{q}$$

from which the result will follow by taking the dimension of both sides of the product decomposition for $B/\mathfrak{p}B$ via the Chinese remainder theorem.

To see that $\dim_k B/\mathfrak{p}B = n$, note that B is finitely generated as an A-module by Theorem 6.1.2, so let $b_1, \cdots, b_m \in B$ be representatives of a basis of $B/\mathfrak{p}B$ over k. It suffices to show that the b_i are a basis for L/K, from which it will follow that $m = n$.

Assume, for a contradiction, that the b_i are linearly dependent over K, and hence over A, and fix $a_i \in A$ such that

$$a_1 b_1 + \cdots + a_m b_m = 0$$

Consider the ideal $\mathfrak{a} = (a_1, \cdots, a_m)$ of A and fix $a \in \mathfrak{a}^{-1}$ such that $a \notin \mathfrak{a}^{-1}\mathfrak{p}$ (which we can choose since if $\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{p}$, then $\mathfrak{p}$ is not proper), whence $a\mathfrak{a} \not\subseteq \mathfrak{p}$. Then the elements $aa_1, \cdots, aa_m$ lie in A but not all lie in $\mathfrak{p}$ since $a\mathfrak{a} \not\subseteq \mathfrak{p}$. Then, we have

$$aa_1b_1 + \cdots + aa_mb_m \equiv 0 \pmod{\mathfrak{p}}$$

which gives a linear dependence of the b_i over k, a contradiction, so the b_i are linearly independent over K.

$B = M \oplus \mathfrak{p}B$ is essentially the assertion of a split exact sequence, although it's not immediately obvious that this should hold.

To see that they form a basis, consider the A modules $M = (b_1, \cdots, b_m)_A$ and $N = B/M$. Since $B = M \oplus \mathfrak{p}B$, $\mathfrak{p}N = N$. Moreover, since B is finitely generated and noetherian (again by Theorem 6.1.2), N is finitely generated with system of generators (say) $\alpha_1, \cdots, \alpha_s$, with

$$\alpha_i = \sum_j a_{ij}\alpha_j$$

for some $a_{ij} \in \mathfrak{p}$ via $\mathfrak{p}N = N$. Let R be the matrix with entries $(a_{ij}) - I_s$, $\tilde{R}$ the adjugate of R, whose entries are rank $s-1$ minors of R. Then, by construction

$$R \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix} = 0 \text{ and } \tilde{R}R = \det(R)I$$

by the definition of the adjugate. Hence,

$$\tilde{R}R \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix} = 0 = \det(R) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}$$

from which it follows that $\det(R)N = 0$, since the α_i generate N.

This implies that $\det(R)B \subseteq M = (b_1, \cdots, b_m)_A$, since $\det(R)$ is nonzero; to see this, by expansion, $\det(R) \equiv (-1)^s \pmod{\mathfrak{p}}$ since $a_{ij} \in \mathfrak{p}$. It therefore follows that $L = \det(R)L = (b_1, \cdots, b_m)_K$ this time over K, where the first equality follows from the fact that L is a field, and the second by the fact that L is the field of fractions of B, consisting of elements of the form $\frac{b}{a}$, $b \in B$, $a \in A$ (by Corollary 3.2.2 and its proof), so the field of fractions of $\det(R)B$ is $\det(R)L$ which must be contained in the field of fractions of $M = (b_1, \cdots, b_m)_A$, which is $(b_1, \cdots, b_m)_K$. However, it is obvious that $(b_1, \cdots, b_m)_K \subseteq L$, so they are in fact equal, and the b_i form a K-basis for L, from which it follows that $m = n$.

For the second claim, that $\dim_k(B/(\mathfrak{q}^{e_\mathfrak{q}})) = f_\mathfrak{q}e_\mathfrak{q}$, consider the descending chain

$$B/\mathfrak{q}^{e_\mathfrak{q}} \supseteq \mathfrak{q}/\mathfrak{q}^{e_\mathfrak{q}} \supseteq \mathfrak{q}^2/\mathfrak{q}^{e_\mathfrak{q}} \supseteq \cdots \supseteq \mathfrak{q}^{e_\mathfrak{q}-1}/\mathfrak{q}^{e_\mathfrak{q}} \supseteq (0)$$

of k-vector spaces. Each successive quotient between neighbors in this chain, $\mathfrak{q}^r/\mathfrak{q}^{r+1}$, is isomorphic to $B/\mathfrak{q}$; to see this, pick $\alpha \in \mathfrak{q}^r \setminus \mathfrak{q}^{r+1}$ and

I don't really get the surjectivity bit at all.

consider the homomorphism $B \to \mathfrak{q}^r/\mathfrak{q}^{r+1}$ given by $a \mapsto a\alpha$. This map clearly has kernel $\mathfrak{q}$ and is surjective since $\mathfrak{q}^r = \alpha B \oplus \mathfrak{q}^{r+1}$.

Since $f_\mathfrak{q} = [B/\mathfrak{q} : k]$, we obtain $\dim_k(\mathfrak{q}^r/\mathfrak{q}^{r+1}) = f_\mathfrak{q}$ whence

$$\dim_k(B/\mathfrak{q}^{e_\mathfrak{q}}) = \sum_{r=0}^{e_\mathfrak{q}-1} \dim_k(\mathfrak{q}^r/\mathfrak{q}^{r+1}) = e_\mathfrak{q} f_\mathfrak{q}$$

as desired. ■

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lectures 7 and 8: 21-23 September

Professor Martin Olsson Abhishek Shivkumar

Number Rings and How To Find Them

Question 7.1.1

Consider $K = \mathbb{Q}(\alpha)$ with α an algebraic integer satisfying some $f \in \mathbb{Q}[x]$ (minimal and monic). Is f irreducible? What is $\mathcal{O}_K$?

We've completely solved this problem in the quadratic setting; to study this problem in general, we want to understand the local setting e.g, if we can understand $\mathcal{O}_{K,(p)}$ for all primes $(p) \subset \mathbb{Z}$, we will hopefully be able to deduce some facts about $\mathcal{O}_K$.

To that end, let A be a DVR, K its field of fractions, $k = A/\mathfrak{m}$ the residue field, $f \in A[x]$ a monic polynomial of degree n. Define $B_f = A[x]/(f)$, $\overline{B_f} := B_f/\mathfrak{m}B_f = k[x]/(\overline{f})$ where $\overline{f} \in k[x]$ is the image of f.

Now, since $k[x]$ is a UFD we can factor

$$\overline{f} = \prod_i \overline{g_i}^{n_i}$$

with the $\overline{g_i}$ irreducible. Choose lifts $g_i \in A[x]$ of the $\overline{g_i}$.

Lemma 7.1.2

The maximal ideals of B_f (which may not be integrally closed or an integral domain) are given by $\mathfrak{m}_i := (\mathfrak{m}B_f, g_i)$ with B_f, g_i and $\mathfrak{m}$ as above.

Proof: We have a chain

$$B_f \twoheadrightarrow \overline{B_f} = k[x]/\prod_i \overline{g_i}^{n_i} \twoheadrightarrow k[x]/(\overline{g_i})$$

where $k[x]/(\overline{g_i})$ since $\overline{g_i}$ is irreducible by assumption, hence all the ideals described in the lemma are in fact maximal (as they are the kernels of these chains, and maximal ideals are precisely those ideals arising as kernels of surjections to fields).

To see that these are the only maximals, suppose $\mathfrak{n} \subset B_f$ is a maximal ideal. If $\mathfrak{m}B_f \not\subseteq \mathfrak{n}$, then $\mathfrak{m}B_f + \mathfrak{n} = B_f$ by maximality (since this would

In what follows, we will use the following formulation of Nakayama's lemma: if M is finitely generated as an R-module and the images of $m_1, \cdots, m_n$ of M in $M/J(R)M$ generate it as an R-module, they also generate M as an R-module, where $J(R)$ is the *Jacobson radical* of R, the intersection of all maximal ideals in R.

Implicit in the use of this lemma in this form is the fact that $\mathfrak{m}B_f$ is the intersection of all maximal ideals of B_f; we do not show this.

otherwise form a strictly larger ideal). Then, $\mathfrak{n}$ generates $B_f/\mathfrak{m}B_f$ as an A-module since every element of B_f can be written as a sum of elements of $\mathfrak{n}$ and $\mathfrak{m}B_f$; equivalently, we have a surjection $\mathfrak{n} \twoheadrightarrow B_f/\mathfrak{m}B_f$.

Then, by Nakayama's lemma, since B_f is finitely generated as an A-module (since f is monic), the surjection above guarantees that we can choose $n_1, \cdots, n_r \in \mathfrak{n} \subset B_f$ which generate $B_f/\mathfrak{m}B_f$; hence, they also generate B_f. Therefore, $\mathfrak{n} = B_f$, which is a contradiction, from which it follows that every maximal ideal of B_f contains $\mathfrak{m}B_f$.

This result feels right to me, but I think some work would need to be done to prove the last sentence formally.

Since all maximals containing $\mathfrak{m}B_f$ clearly arise from our chain of surjections above, the result follows. ■

We can say more about B_f if we are willing to resort to casework; the first is the so called *unramified* case.

Proposition 7.1.3

If $\overline{f}$ is irreducible then B_f is a DVR.

Proof: To see this, note that $\mathfrak{m}B_f$ is maximal, since $\overline{B_f} = B_f/\mathfrak{m}B_f = k[x]/(\overline{f})$ and $k[x]/(\overline{f})$ is a field since $\overline{f}$ is irreducible. Therefore, by the lemma, B_f is a local ring, and is noetherian since it is the quotient of A which is noetherian. Therefore, picking a uniformizer $\pi \in \mathfrak{m}$, it follows from one of our definitions of a DVR (noetherian local ring whose maximal is principal, and not a field) that B_f is a DVR. ■

Corollary 7.1.4

f as above is irreducible in $K[x]$, and B_f is the integral closure of A in $K[x]/(f)$.

Proof: That f is irreducible in $K[x]$ follows from the fact that A is a DVR and hence integrally closed, together with the contrapositive of Proposition 3.2.5. That $B_f = A[x]/(f)$ is the integral closure of A in $K[x]/(f)$ follows from irreducibility of f in $K[x]$. ■

Corollary 7.1.5

If $\overline{f}$ is separable, then $K[x]/(f)$ over K is *unramified* in the sense that $e_\mathfrak{q} = 1$ for all primes $\mathfrak{q} \subset B_f$ with respect to some $\mathfrak{p} \subset A$. Equivalently, a field extension L/K is unramified if $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a field, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_K$.

There's a remark here about how we don't really usually care about the residue field extension being separable, as it's automatic for number fields, I don't really know what residue field he's referring to here.

Example 7.1.6

Consider $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ with $f(x) = x^2 + 5$. Let p be a prime, and consider $\mathbb{Z}_{(p)}[\sqrt{-5}]$ over $\mathbb{Z}_{(p)}$. There are several cases: $\overline{f}$ factors as

I also don't know precisely what I'm supposed to understand from the following example. This probably stems from my lack of understanding on what residue field means in this context. Probably $\mathbb{Z}/(p)$, so the example shows what happens when f passes to $\overline{f}$ for various $(p) \subset \mathbb{Z}$. The cases where -5 is not a root $\pmod p$ are probably the unramified cases.

$(x+a)(x-a)$ if -5 has a square root in $\mathbb{F}_p$, and remains x^2+5 otherwise with two exceptions.

If $p=5$, $x^2+5=x^2$, and if $p=2$, $x^2+5=x^2+1\in\mathbb{F}_2[x]$, which is equal to $(x+1)^2$.

Exercise 7.1.7

Prove that $f(x)=x^3+x+1$ is irreducible over $\mathbb{Q}$ and that if $\alpha\in\mathbb{C}$ is a root of f, then for $K=\mathbb{Q}(\alpha)$, $\mathcal{O}_K=\mathbb{Z}[\alpha]$.

These random exercises are generally what he gives us during our "break," and sometimes are not meant to be solved during break. In particular, this exercise was meant to warm us up to discriminants, which we briefly discussed at the end of lecture.

It is at least clear that $\mathbb{Z}[\alpha]\subseteq\mathcal{O}_K$, but that's as far as we got.

We have thus far discussed the unramified case, where $\overline{f}$ is irreducible. The other extreme is the so-called *totally ramified* case:

Definition 7.1.8

Let A be a DVR, then $f\in A[x]$ is *Eisenstein* if

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

with $a_i\in\mathfrak{m}$ for all i, $a_0\notin\mathfrak{m}^2$.

In terms of our example above, we can say that $x^2+5\in\mathbb{Z}[x]$ is Eisenstein at (5).

Proposition 7.1.9

If f is Eisenstein, then B_f is a DVR with maximal ideal $\mathfrak{m}B_f=\mathfrak{m}_{B_f}^n$ where $n=\deg f$.

Don't really get the final step of the argument that $(\mathfrak{m}B_f,x)=(x)$.

Proof: $\overline{f}=x^n$ in $k[x]$ by assumption, since the other coefficients vanish upon modding out by $\mathfrak{m}$. Then, by Lemma 7.1.2, it is clear that B_f is local with maximal $(\mathfrak{m}B_f,x)$. Write $f\in A[x]$ as

$$x^n+a_{n-1}x^{n-1}+\cdots+a_0$$

Since $B_f=A[x]/(f)$, we have

$$x^n+a_{n-1}x^{n-1}+a_1x=-a_0$$

as elements of B_f, since $f=0\in B_f$.

Then since the $a_i\in\mathfrak{m}$ by assumption, the right hand side is in $\mathfrak{m}$, so the left hand side must be as well, which implies that $(\mathfrak{m}B_f,x)=(x)$, from which it follows that B_f is a DVR since its maximal is principal. ■

Corollary 7.1.10

f is irreducible in $K[x]$ and B_f is the integral closure of A in $L=K[x]/(f)$.

Discriminants

Recall our exercise above, where we wanted to show that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ for some specific algebraic number α. Clearly, $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_{\mathbb{Q}(\alpha)}$, how do we show that this containment is in fact equality? To this end, we will develop the theory of discriminants, which basically is a high level way to guess and check.

I have no idea what he means by guess and check here, probably because we didn't finish defining everything. I also do not know what it means for a subring $R \subseteq \mathcal{O}_K$ to "generate" K.

More generally, let $K/\mathbb{Q}$ be a number field, $\mathcal{O}_K$ its ring of integers, $R \subseteq \mathcal{O}_K$ a subring which generates K. How can we tell whether $R = \mathcal{O}_K$?

Towards answering this, we will develop the theory of discriminants. First, we have an informal "definition" for number fields: with $K = \mathbb{Q}(\alpha)$ we define the *discriminants* $\operatorname{disc}(\mathbb{Z}[\alpha])$ and $\operatorname{disc}(\mathcal{O}_K)$ by

$$\operatorname{disc}(\mathbb{Z}[\alpha]) = (\operatorname{length} \mathcal{O}_K/\mathbb{Z}[\alpha])^2 \operatorname{disc}(\mathcal{O}_K)$$

where all the values in this equality are integers.

To resolve the difficult portion of our exercise above, e.g, to show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, we can show that $\operatorname{disc} \mathbb{Z}[\alpha] = -31$ and hence cannot be equal to an integer squared times an integer unless the integer squared is 1, e.g, if $\operatorname{length} \mathcal{O}_K/\mathbb{Z}[\alpha] = 1$ which implies that $\mathbb{Z}[\alpha] = \mathcal{O}_K$, as desired.

More generally, let A be a ring, M a free finitely generated A-module (although projective suffices), $t : M \times M \to A$ a bilinear pairing (the one we will care about generally is $(x, y) \in \mathcal{O}_K \times \mathcal{O}_K$ mapping down to $\mathbb{Z}$ via $(x, y) \mapsto \operatorname{tr}(x \cdot y)$). Clearly, this is equivalent to $t : M \to M^* = \operatorname{Hom}_A(M, A)$ given by $x \mapsto t(-, x)$. This is a map of free A-modules. Take $\wedge^n M \to \wedge^n M^*$ induced by t, where n is the rank of M, whence $\wedge^n M := \det M$ is free of rank 1, and t goes to $\det t$.

For example, if $M = \bigoplus_{i=1}^n A \cdot e_i$, then $\wedge^n M = Ae_1 \cdot e_2 \cdots e_n$.

Definition 7.2.1: Discriminants

With M, A as above, we can think of the map above as $(\wedge^n M)^{\otimes 2} \to A$ (the determinant map) which defines an ideal; this ideal is called the *discriminant*, denoted $\delta_{(M,t)}$.

When $M = K$ and $A = \mathbb{Z}$, and with the pairing as above, $(x, y) \in \mathcal{O}_K \times \mathcal{O}_K \mapsto \operatorname{tr}(xy)$, the discriminant ideal $\delta_{(K/\mathbb{Q})} \subseteq \mathbb{Z}$ is clearly associated to an integer since $\mathbb{Z}$ is a PID, whence we refer to the discriminant as an integer via abuse of notation.

A quick aside on determinants, for those who haven't seen them in this form before: choose a basis e_i for M, and let $M^* = \operatorname{Hom}_A(\bigoplus_i A \cdot e_i, A) = \bigoplus_i Ae_i^*$ where e_i^* is a map

$$e_i^* : \bigoplus_i Ae_I \to A$$

which takes e_j to 1 if $i = j$, otherwise, to 0.

Then, given a map $t : M \times M \to A$, we can rewrite this as a map $M \to M^*$ with $M = \bigoplus_i Ae_i$, $M^* = \bigoplus Ae_j^*$. Without any information about this map, it must clearly take the following form (given the bases we've chosen):

$$e_i \mapsto \sum_j t(e_i, e_j)e_j^*$$

Form the matrix T whose i, j^{th} entry is $t(e_i, e_j)$. This matrix defines a map from A^r to itself, where $A^r = M = M^*$ by the bases we've chosen above (where the size of our basis is r). Then, taking the top exterior power of both sides, we have that

$$\wedge^r M = Ae_1 \wedge \cdots \wedge e_r \qquad \wedge^r M^* = Ae_1^* \wedge \cdots \wedge e_r^*$$

and the corresponding map between the top exterior powers is $\det T$; to see this, note that we must have

$$e_1 \wedge \cdots \wedge e_r \mapsto \left(\sum_j T_{1j}e_j^*\right) \wedge \cdots \wedge \left(\sum_j T_{rj}e_j^*\right)$$

Then, to rewrite this sum in terms of our chosen basis vector of $\wedge^r M^*$ (which is one-dimensional), we can see via the alternating property of the exterior power ($v \wedge w = -w \wedge v$) that we recover the alternating sum of products over permutations formulation of the determinant.

In particular, since $v \wedge v = 0$ by the alternating property, clearly we have to choose a distinct j in each of the r sums on the right hand side of the map above, which defines a permutation, and we can move $e_{\sigma(1)}^* \wedge \cdots \wedge e_{\sigma(r)}^*$ to $e_1^* \wedge \cdots \wedge e_r^*$ with $\text{sign}(\sigma)$ permutations, from which we recover the definition of the determinant.
There's some discussion here of the construction of the exterior product, which I didn't write down.

Suppose now that $M' \hookrightarrow M$ where M' and M both are free of rank n. Then $\det M' \hookrightarrow \det M$ are both free of rank 1, so this inclusion gives an ideal $\mathfrak{a} \subseteq A$ where $\mathfrak{a} = \det M' \otimes (\det M)^{-1}$. Let $t' : M' \times M' \to A$ be the restriction of t as above to M'.

Lemma 7.2.2

With M, M', t, t', and $\mathfrak{a}$ as above,

$$\delta_{(M',t')} = \mathfrak{a}^2 \delta_{(M,t)}$$

Proof: We have

$$M' \hookrightarrow M \xrightarrow{t} M^* \hookrightarrow M'^*$$

and this chain of compositions is equal to t'. Taking the determinant of this chain, we have

$$\det M' \hookrightarrow \det M \xrightarrow{\det t} \det M^* \hookrightarrow \det M'^*$$

As above, this chain of compositions is equal to $\det t'$, and the first and last inclusion both have image isomorphic to $\mathfrak{a}$, hence the image of $\det t'$ is the image of $\det t$ multiplied with $\mathfrak{a}^2$ as claimed. ■

The proof above is a little wonky, but I'm not going to worry about it.

Remark 7.2.3

Given $L' \hookrightarrow L$ an inclusion of free modules of rank 1, $L' = \mathfrak{a}L$ for some ideal $\mathfrak{a} \subseteq A$, since we can choose a basis for L and our inclusion becomes $L' \hookrightarrow A$.

Example 7.2.4

Consider $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ with D square free, and write $\mathbb{Z}[\sqrt{D}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$ which is free of rank 2 over $\mathbb{Z}$. We know that $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Recall that $\operatorname{tr}\left(a + b\sqrt{D}\right) = 2a$; rewriting the natural trace pairing as a map $\mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}]^*$, with basis $e_1 = 1$, $e_2 = \sqrt{D}$ for $\mathbb{Z}[\sqrt{D}]$, we have that $1 \mapsto \operatorname{tr}(-) = 2e_1^*$ and $\sqrt{D} \mapsto \operatorname{tr}\left(\sqrt{D} \cdot -\right) = 2De_2^*$. Then, one can see that the discriminant of $\mathbb{Z}[\sqrt{D}]$ is

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D$$

By Example 4.1.8, we know that if $D \equiv 1 \pmod 4$, $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, so

$$\mathbb{Z} \oplus \mathbb{Z}\sqrt{D} \hookrightarrow \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{D}}{2} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$$

Since this is an inclusion of free modules of the same rank, the corresponding ideal by the above discussion is $\mathfrak{a} = (2)$ (this is easy to see by drawing a lattice; $\mathbb{Z}[\sqrt{D}]$ hits half of the points of $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$), from which it follows by the lemma that $\delta_{(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}, \operatorname{tr})} = (D)$ for $D \equiv 1 \pmod 4$. Otherwise, the discriminant is $(4D)$ as above, since $\mathbb{Z}[\sqrt{D}]$ is the entire ring of integers.

Exercise 7.2.5

Consider $(5) \subset \mathbb{Z}$. What happens to (5) in the rings of integers of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{5})$?

(5) splits as $(1+2i)(1-2i)$ in $\mathbb{Z}[i]$, as $(\sqrt{5})^2$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, and stays (5) in $\mathbb{Z}[\sqrt{2}]$. These are the three possible things that can happen via the fundamental identity: the prime either splits into two different primes (as in $\mathbb{Z}[i]$), becomes a prime squared (as in $\mathbb{Z}[\sqrt{2}]$), or stays the same.

Galois Theory

Let A be a Dedekind domain, K its field of fractions, L/K a Galois extension with Galois group G, B the integral closure of A in L.

That the extension is Galois implies that

$$N_{L/K}(x) = \prod_{\sigma : L \hookrightarrow \overline{K}} \sigma(x) = \prod_{g \in G} g(x)$$

and similarly for $\mathrm{tr}_{L/K}$, so we don't need to consider an algebraic closure ($\mathbb{C}$ in all the cases we care about). The above equality is true because, fixing some $\sigma : L \hookrightarrow K$, first applying some Galois automorphism to L and then applying σ gives a set of n distinct embeddings of L into $\overline{K}$. Since the degree of the Galois extension is equal to both the size of the Galois group and the number of embeddings $L \hookrightarrow \overline{K}$, it follows that all embeddings are generated by a single embedding up to Galois automorphisms.

Moreover, G acts on B over A; given $b \in B \subset L$, b satisfies some equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

so for all $g \in G$, $g(b)$ also satisfies this equation since $g(a_i) = a_i$ by assumption. Thus $g(b) \in B$.

Now, we will state an important lemma that will be widely applicable throughout the rest of course.

Lemma 7.3.1: Approximation Lemma

Let $\mathfrak{p}_i$ be distinct prime ideals for $1 \leq i \leq k$ of A Dedekind, $x_i \in K$ the field of fractions of A, n_i integers. Then there exists $x \in K$ such that $\nu_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all i and $\nu_{\mathfrak{q}}(x) \geq 0$ for $\mathfrak{q} \neq \mathfrak{p}_1, \cdots, \mathfrak{p}_k$.

Proof: Suppose first that the x_i are in A, and we will seek a solution $x \in A$. We may assume that $x_2 = \cdots = x_k = 0$; to see this, suppose we want to find x where $x - x_1$ and $x - x_2$ have valuations bounded below as prescribed, suppose we can find y s.t $\nu_{\mathfrak{p}_1}(y - x_2)$ and $\nu_{\mathfrak{p}_2}(y)$ are sufficiently large, and similarly find z s.t $\nu_{\mathfrak{p}_2}(z - x_2)$ and $\nu_{\mathfrak{p}_1}(z)$ are sufficiently large, then set $x = y + z$. Then

$$\nu_{\mathfrak{p}_1}(x - x_1) = \nu_{\mathfrak{p}_1}(z + y - x_1) \geq \min(\nu_{\mathfrak{p}_1}(y - x_1), \nu_{\mathfrak{p}_1}(z))$$

and similarly for $\mathfrak{p}_2$, so $x = y + z$ satisfies the given requirements. Hence, by linearity and induction, it suffices to show the result when $x_2 = \cdots = x_k = 0$.

This is a little tricky to wrap my head around, should revisit to make sure I really understand what's going on here.

Then, increasing the n_i if necessary, we may assume that $n_i \geq 0$. Set

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2}\mathfrak{p}_3^{n_3} \cdots \mathfrak{p}_k^{n_k}$$

Then $\nu_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all $\mathfrak{p}$ since only the $\mathfrak{p}_i$ could have positive valuation on $\mathfrak{a}$, and clearly, by construction, none of them can. Therefore, $\mathfrak{a} = A$. It follows that $x_1 = x + y$ with $y \in \mathfrak{p}_1^{n_1}$, $x \in \mathfrak{p}_2^{n_2}\mathfrak{p}_3^{n_3} \cdots \mathfrak{p}_k^{n_k}$. Then x has the desired properties, e.g,

$$\nu_{\mathfrak{p}_1}(x - x_1) = \nu_{\mathfrak{p}_1}(y) \geq n_1$$

and

$$\nu_{\mathfrak{p}_r}(x) \geq n_r$$

for $r > 1$, and $\nu_{\mathfrak{q}}(x) \geq 0$ for $\mathfrak{q} \neq \mathfrak{p}_1, \cdots, \mathfrak{p}_k$ since $x \in A$.

Then, in the general case, write $x_i = \frac{a_i}{s}$, $a_i \in A$, $s \in A$, $s \neq 0$, $x = \frac{a}{s}$. The element a must satisfy

$$\nu_{\mathfrak{p}_i}(a - a_i) \geq n_i + \nu_{\mathfrak{p}_i}(s) \text{ and } \nu_{\mathfrak{q}}(a) \geq \nu_{\mathfrak{q}}(s)$$

Since s is fixed, we can find a satisfying the first condition for all i by the first part above, and the second condition can also be handled by the first part, since $\nu_{\mathfrak{q}}(s) > 0$ for only finitely many primes $\mathfrak{q}$, so we can just add these primes to the $\mathfrak{p}_i$. ■

Consider the set

$$S_{\mathfrak{p}} = \{\mathfrak{q} \subset B : \mathfrak{q} \cap A = \mathfrak{p}\} = \{\mathfrak{q} \subset B : \mathfrak{q} | \mathfrak{p}\}$$

for some prime $\mathfrak{p} \subset A$. $G \curvearrowright S_{\mathfrak{p}}$ via the action on B described above.

Lemma 7.3.2

$G \curvearrowright S_{\mathfrak{p}}$ is transitive, i.e, for all $\mathfrak{q}, \mathfrak{q}' \in S_{\mathfrak{p}}$, there exists $g \in G$ s.t $g\mathfrak{q} = \mathfrak{q}'$.

Proof: Fix $\mathfrak{q}|\mathfrak{p}$, and suppose there exists $\mathfrak{q}'|\mathfrak{p}$ such that $\mathfrak{q}' \neq g\mathfrak{q}$ for any $g \in G$. By Lemma 7.3.1 (the approximation lemma), there exists $x \in \mathfrak{q}'$, $x \notin g\mathfrak{q}$ for all $g \in G$ (taking $g\mathfrak{q}$ for to be our finite set of primes, with $\nu_{g\mathfrak{q}}(x-1) \geq 0$ (whence $x \notin g\mathfrak{q}$), $\nu_{\mathfrak{q}'}(x) \geq 1$).

Hence, $N(x) = \prod_{g \in G} g(x) \in \mathfrak{p} = \mathfrak{q}' \cap A$. Hence $N(x) \in \mathfrak{q}'$, $N(x) \notin \mathfrak{q}$, which is a contradiction since any element of $\mathfrak{p}$ is in $\mathfrak{q}$. ■

Define $g_{\mathfrak{p}}$ to be the number of primes $\mathfrak{q} \subset B$ such that $\mathfrak{q}|\mathfrak{p}$, $e_{\mathfrak{p}}$ the ramification index of any $\mathfrak{q}|\mathfrak{p}$, $f_{\mathfrak{p}}$ the degree of the residue field extension. Then our Fundamental Identity, Theorem 6.1.6, becomes $n = g_{\mathfrak{p}} e_{\mathfrak{p}} f_{\mathfrak{p}}$, since $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ are constant across $\mathfrak{q}|\mathfrak{p}$, since all such $\mathfrak{q}$ are equivalent by the above lemma, via the Galois action.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 9: 28 September

Professor Martin Olsson Abhishek Shivkumar

Decomposition and Inertia Groups

Consider our standard setup, e.g, A a Dedekind domain, K its field of fractions, L a Galois extension, B the integral closure of A in L, G the Galois group of L over K. Prime ideals $\mathfrak{p}$ in A factor into prime ideals $\mathfrak{q}_i$ in B by prior results, and by Lemma 7.3.2, the induced action on the prime ideals of B is transitive.

Definition 8.1.1: Decomposition Groups

Given $\mathfrak{q}|\mathfrak{p}$ as above, define $D_\mathfrak{q} \subset G$ the *decomposition group* given by

$$D_\mathfrak{q} = \{g \in G : g\mathfrak{q} = \mathfrak{q}\}$$

the stabilizer in G of $\mathfrak{q} \in S_\mathfrak{p}$.

Note that for $h \in G$, $D_{h\mathfrak{q}} = hD_\mathfrak{q}h^{-1}$, so the choice of representative of an orbit of primes doesn't matter, up to conjugation. Consider the following diagram:

$$\begin{tikzcd}
L & B \arrow[l, hook'] \arrow[r, two heads] & l = B/\mathfrak{q} \\
K \arrow[u, hook] & A \arrow[l, hook'] \arrow[u, hook] \arrow[r, two heads] & k = A/\mathfrak{p} \arrow[u, hook]
\end{tikzcd}$$

We assume that k is perfect, i.e, its finite extensions are separable. From this diagram, we obtain a map $\epsilon : D_\mathfrak{q} \to \mathrm{Aut}(l/k)$, since $D_\mathfrak{q} \curvearrowright B$ descends to $D_\mathfrak{q} \curvearrowright B/\mathfrak{q}$, and $D_\mathfrak{q}$ fixes A and therefore fixes k.

Proposition 8.1.2

l/k is Galois, and ϵ is surjective.

Proof: Since k is perfect, l is finite over k since L is finite over K, so l/k is separable. We need to show that l/k is normal, e.g, irreducible polynomials in k either split into linear factors in l or don't split at all. Fix $\overline{a} \in l$, $\overline{f} \in k[x]$ its minimal polynomial. Fix $k \hookrightarrow \overline{k}$, in which $\overline{f}$ factors as

$$\overline{f}(x) = (x - \overline{a})(x - \gamma_1) \cdots (x - \gamma_d)$$

For posterity, recall that an extension is Galois if it is separable and normal. L/K is separable if for every $\alpha \in L$, the minimal polynomial of α over F is separable, it doesn't have any repeated roots. L/K is normal if every polynomial that is irreducible over K either has no roots in L or splits into linear factors in L.

We wish to show that the γ_i lie in l.

Fix $a \in B$ mapping to $\overline{a} \in l$, and consider

$$g(x) = \prod_{\sigma \in G} (x - \sigma(a)) \in A[x]$$

To see that $g \in A[x]$, note that $A = B^G$, the set of G-invariant elements of B. It follows that $A = L^G \cap B$ where $L^G = K$ since L/K is Galois. Then

$$\tau g(x) = \prod_{\sigma \in G} (x - \tau\sigma(a)) = g(x)$$

where the last equality is from the fact that τ just reorders our product, so $g \in A[x]$ since τ was arbitrary in G and preserves g.

Then, $\overline{g}(x)$ is a product of linear factors with $\overline{a}$ as a root, so $\overline{f}(x)$ divides $\overline{g}(x)$, so all roots of $\overline{f}$ are among the roots of $\overline{g}$, from which it follows that $\overline{f}$ splits into linear factors. Since $\overline{a}$ was arbitrary in l, it follows that l/k is Galois.

There's a discussion in the middle of this about showing that if

$$\overline{f}(x) = \prod_{S \subseteq G} (x - \overline{\sigma(a)})$$

then $S = D_{\mathfrak{q}}$. I can't tell why this would be essential to showing that l/k is Galois, and I don't know which part of our argument implies this.

It remains to show that $\epsilon : D \to \mathrm{Aut}(l/k)$ is surjective. To that end, we will use Lemma 7.3.1: choose $a \in B \setminus \mathfrak{q}$ such that $a \in \sigma(\mathfrak{q})$ for all $\sigma \in G \setminus D_{\mathfrak{q}}$. Consider

$$g(x) = \prod_{\sigma \in G} (x - \sigma(a))$$

Then

$$\overline{g}(x) = x^k \prod_{\sigma \in D_{\mathfrak{q}}} (x - \overline{\sigma(a)})$$

for some k, where some of the linear terms in g become factors of the x^k (e.g, for $\sigma^{-1} \in G \setminus D_{\mathfrak{q}}$ in the product for g, $\sigma^{-1}(a) \in \mathfrak{q}$ and collapses to 0 in the quotient). Thus, every conjugate of $\overline{a}$ is of the form $\epsilon(\sigma)(\overline{a})$ for some $\sigma \in D_{\mathfrak{q}}$, since the surviving terms in the expansion of $\overline{g}(x)$ contain precisely those σ in the image of ϵ. Since all conjugates of $\overline{a}$ are achievable by the action of $\mathrm{Aut}(l/k)$ (by definition of the Galois group), it follows that ϵ is surjective as claimed. ■

In the language of the Approximation Lemma, $a \in \sigma(\mathfrak{q})$ translates to $\nu_{\sigma(\mathfrak{q})}(a) \geq 1$, and $a \notin \mathfrak{q}$ translates to $\nu_{\mathfrak{q}}(a-1) \geq 1$. Since $a - 1 \in \mathfrak{q}$, $a \notin \mathfrak{q}$.

The kernel of ϵ is the *inertia group*, e.g, we have an exact sequence

$$0 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \to \mathrm{Aut}(l/k) \to 0$$

Therefore, by the Galois correspondence, we have a sequence of subfields

$$K \hookrightarrow L^{D_{\mathfrak{q}}} \hookrightarrow L^{I_{\mathfrak{q}}} \hookrightarrow L$$

where L/K has Galois group G, $L/L^{I_{\mathfrak{q}}}$ has Galois group $I_{\mathfrak{q}}$, and $L/L^{D_{\mathfrak{q}}}$ has Galois group $D_{\mathfrak{q}}$.

Most of what follows is completely opaque to me. I tried to resuscitate this section by reading section I.9 in Neukirch, but I wasn't able to completely reconstruct it. I've tried to just say what was said in class, which I think was not a complete proof of everything asserted. Might revisit this later.

Fix some prime $\mathfrak{p} \subset A$, which factors into the product of some primes $\mathfrak{q}_i^{D_{\mathfrak{q}}} \subset B^{D_{\mathfrak{q}}}$. The induced Galois action of $D_{\mathfrak{q}}$ on $B^{D_{\mathfrak{q}}}$ fixes $\mathfrak{q}_i^{D_{\mathfrak{q}}}$ by assumption, so there is exactly one prime in B over each $\mathfrak{q}_i^{D_{\mathfrak{q}}}$, $\mathfrak{q}$ itself.

Therefore, since $D_{\mathfrak{q}}$ is the Galois group for $L/L^{D_{\mathfrak{q}}}$, we have that

$$|D_{\mathfrak{q}}| = [L : L^{D_{\mathfrak{q}}}] = 1 \cdot e(\mathfrak{q}/\mathfrak{q}^{D_{\mathfrak{q}}}) \cdot f(\mathfrak{q}/\mathfrak{q}^{D_{\mathfrak{q}}})$$

What this tells us is that the identity $[L : K] = e_{\mathfrak{q}} f_{\mathfrak{q}} g_{\mathfrak{q}}$ factor into a sequence of maps: $L \hookrightarrow L^{D_{\mathfrak{q}}}$ gives us $g_{\mathfrak{q}}$, and each prime is unramified and has inertia degree 1. $L^{D_{\mathfrak{q}}} \hookrightarrow L^{I_{\mathfrak{q}}}$ gives us $f_{\mathfrak{q}}$ with a single unramified prime, and $L^{I_{\mathfrak{q}}} \hookrightarrow L$ gives us $e_{\mathfrak{q}}$. Hence, the decomposition group allows us to "factor" our fundamental identity into three separate embeddings.

Exercise 8.1.3

Let $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{5})$ over $\mathbb{Q}$, with Galois group $(\mathbb{Z}/(2))^3$. Factor $\mathbb{Q} \hookrightarrow L$ as above to obtain $e_{\mathfrak{q}}$, $f_{\mathfrak{q}}$, and $g_{\mathfrak{q}}$ for $\mathfrak{p} = (5)$.

Complete Fields

This section seems to have been a quick aside at the end of lecture to make sure we're all on board for p-adic numbers and completions in general, probably in preparation for next lecture.

Recall that the p-adic integers are defined as

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/(p^n)$$

which is the *completion* of $\mathbb{Z}$ with respect to the ideal (p), or the p-adic completion. The inverse limit can be described explicitly as elements $(a_1, a_2, \cdots)$ with $a_k \in \mathbb{Z}/(p^k)$ and $a_{k+1} \mapsto a_k$ under the natural map $\mathbb{Z}/(p^{k+1}) \to \mathbb{Z}/(p^k)$.

Equivalently, there is a categorical definition of the inverse limit (which is in fact a categorical limit, for reasons passing understanding) as the limit of the diagram of projections $\mathbb{Z}/(p^m) \to \mathbb{Z}/(p^n)$ for $m > n$ (with the obvious generalization to general I-adic completions).

Our guiding principle for completion is meant to be $k[x]$ completed with respect to (x), which produces the power series ring $k[[x]]$.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 10: 30 September

Professor Martin Olsson Abhishek Shivkumar

Completions

We've discussed localizations both concretely (in terms of the inverse limit construction) and abstractly (in terms of categorical limits). We now offer an intermediary conception: $\mathbb{Z}_p$ is the equalizer of the following diagram:

$$\prod_{n\geq 1}\mathbb{Z}/(p^n) \rightrightarrows \prod_{n\geq 1}\mathbb{Z}/(p^n)$$

where the top arrow is the identity, and the bottom arrow is the shift map, taking $(a_1, a_2, \cdots,)$ to $(a_2 \mod p, a_3 \mod p^2, \cdots)$. It can be seen with some work that the equalizer condition encodes the compatibility data of the inverse limit, e.g, that the a_i form a "compatible collection" of elements.

Lemma 9.1.1

$\mathbb{Z}_p$ is a discrete valuation ring.

Proof: First note that the ideals in $\mathbb{Z}/(p^n)$ are (p^k) for $0 \leq k \leq n$, since ideals in $\mathbb{Z}/(p^n)$ are ideals in $\mathbb{Z}$ containing (p^n), and ideals in $\mathbb{Z}$ containing (p^n) correspond to divisors of p^n, which are precisely p^k for $0 \leq k \leq n$ as above.

In what follows, we show that $\mathbb{Z}_p$ is a local PID, but a DVR is additionally not a field. It's slightly nontrivial to see that there are non-units in $\mathbb{Z}_p$, I assume this step is what is handled by Proposition 2 on page 7 of Serre's Local Fields; Professor Olsson points us to this result at the end of his proof.

Also, the final stage where the sequence of ideals stabilizing implies that $I = p^k\mathbb{Z}_p$ is not entirely clear to me.

Moreover, if $I \subset \mathbb{Z}_p$ is an ideal, and $I_n \subset \mathbb{Z}/(p^n)$ its image, then we have the following diagram:

$$\begin{tikzcd}
\cdots \arrow[r] & I_{n+1} \arrow[r] \arrow[d, hook] & I_n \arrow[r] \arrow[d, hook] & I_{n-1} \arrow[r] \arrow[d, hook] & \cdots \\
\cdots \arrow[r] & \mathbb{Z}/(p^{n+1}) \arrow[r] & \mathbb{Z}/(p^n) \arrow[r] & \mathbb{Z}/(p^{n-1}) \arrow[r] & \cdots
\end{tikzcd}$$

Since for each n $I_n = (p^k)$ for $k \leq n$, there are two options: if $I_n = (p^n)$ for each n, then $I = (0)$. Otherwise, for some n, $I_n = (p^k)$ with $k < n$, in which case $I_m = (p^k)$ for all $m > n$ (keep in mind that these ideals appear to be the same, but they live in different rings and are not equal as sets). In this case, clearly $I = p^k\mathbb{Z}_p$. Therefore, the ideals of $\mathbb{Z}_p$ are of the form (p^k) and clearly the only maximal ideal is $(p) = p\mathbb{Z}_p$ itself, so $\mathbb{Z}_p$ is a local PID, and therefore a DVR. ■

There's some discussion at the end of this proof of how $\cdot p : \mathbb{Z}_p \to \mathbb{Z}_p$ is injective, but I didn't follow it or see why it is necessary to show that $\mathbb{Z}_p$ is a DVR. That paragraph of my notes is omitted, at least until Professor Olsson posts his lecture slides.

Definition 9.1.2: *p*-adic Numbers

With $\mathbb{Z}_p$ as above, fix $\mathbb{Q}_p$ as its field of fractions, the field of *p-adic numbers*. Since $\mathbb{Z}_p$ is a DVR, we have $\nu_p : \mathbb{Q}_p^\times \to \mathbb{Z}$. We may use this valuation to define the so-called *p-adic norm*,

$$|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_{\geq 0}$$

given by $|x|_p = p^{-\nu_p(x)}$ and $|0|_p = 0$.

It is easy to check the usual norm properties for $|\cdot|_p$, which inherit from the familiar properties of the p-adic valuation. For what follows, note that when we discuss norms in general, we will exclude the trivial norm given by $|x| = 1$ for all $x \in \mathbb{Q}_p^*$, $|0| = 0$.

From this norm, we can construct in the normal way a metric ($d(x, y) = |x - y|_p$) which provides a topology on $\mathbb{Q}_p$. Recall that a sequence $(x_n)_{n\geq 1}$ in $\mathbb{Q}_p$ is Cauchy if for every $\epsilon > 0$ there exists N such that $|x_n - x_m|_p < \epsilon$ for all $n, m \geq N$.

Proposition 9.1.3

Every Cauchy sequence is convergent in $\mathbb{Q}_p$, e.g, $\mathbb{Q}_p$ is a complete metric space.

Proof: Fix a Cauchy sequence $(x_n)_{n\geq 1}$ in $\mathbb{Q}_p$. Recall that $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ which just says that $\nu_p(x) \geq 0$, precisely the condition for $x \in \mathbb{Z}_p$. If $|x_n - x_m|_p \leq 1$, then $x_n = x_m + y$ for some $y \in \mathbb{Z}_p$, hence $x_n \in \mathbb{Z}_p \iff x_m \in \mathbb{Z}_p$. Via the Cauchy property, we may assume that $|x_n - x_m| \leq 1$ for all m, n by choosing some tail of our original sequence associated to $\epsilon = 1$ (since convergence does not care about any finite number of lead terms). Multiply this new sequence by p^r for some r, and we can therefore assume that $x_n \in \mathbb{Z}_p$ for all n; this follows from the fact that now, $x_n \in \mathbb{Z}_p$ if and only if $x_1 \in \mathbb{Z}_p$, so we can multiply x_1 by some power of p such that $p^r x_1 \in \mathbb{Z}_p$, from which it follows that the entire sequence is in $\mathbb{Z}_p$.

For every s, consider the sequence $\overline{x_n} := x_n \pmod{p^s}$ in $\mathbb{Z}/(p^s)$. Each of these sequences is eventually constant by the Cauchy property, since for $x, y \in \mathbb{Z}_p$, $|x - y|_p < p^{-s} \iff \nu_p(x - y) > s$, which implies that $\overline{x} = \overline{y}$ in $\mathbb{Z}/(p^s)$. Call the limit of this sequence a_s, and form $a = (a_s)_{s\geq 1}$. We claim a is the limit of our sequence $(x_n)_{n\geq 1}$, from which the result follows. ■

Need to check: that a is in fact a well-defined element of $\mathbb{Z}_p$ and that it is the limit of $(x_n)_{n\geq 1}$.

This result gives us an alternate description of $\mathbb{Q}_p$: let $\mathcal{C}$ be the ring of Cauchy sequences (with respect to $|\cdot|_p$) in $\mathbb{Q}$, whose ring structure arises from element-wise addition and multiplication. Consider $I \subset \mathcal{C}$ the ideal of Cauchy sequences converging to 0.

Before we can prove the following lemma, we need a quick aside on the formal power series formulation of $\mathbb{Z}_p$ and the formal Laurent series formulation of $\mathbb{Q}_p$. In particular, given $a = (a_1, a_2, \cdots) \in \mathbb{Z}_p$, we may represent a as a power series in p, with coefficients between 0 and $p-1$ (inclusive). This is easy to see via construction: suppose

$$a = b_0 + b_1 p + b_2 p^2 + \cdots$$

Then we need the projection of a to $\mathbb{Z}/(p^n)$ to be a_n. When $n = 1$, this gives us $b_0 = a_1$ (choosing a_1 between 0 and $p-1$), $n = 2$ gives us $b_1 = \frac{a_2 - a_1}{p}$, and so on, with $b_n = \frac{a_n - (b_0 + b_1 p + \cdots + b_{n-1} p^{n-1})}{p^n}$.

If p does not divide n, then n is invertible in $\mathbb{Z}_p$, since the class of n is invertible in each $\mathbb{Z}/(p^k)$. One could also see this by noting that $\mathbb{Z}_p$ is local with maximal (p). Therefore, for nonzero elements a of $\mathbb{Z}_p$, only finitely many of the lead terms a_i can be 0, so $p^{-k}a \in \mathbb{Z}_p^\times$ for some k. Therefore, writing a as a power series in p, p^{-k} is a formal Laurent series in p as claimed, from which it follows (since a is an arbitrary nonzero nonunit) that $\mathbb{Q}_p$ consists of formal Laurent series in p, with coefficients as above.

Lemma 9.1.4

I is a maximal ideal, and $\mathcal{C}/I \cong \mathbb{Q}_p$.

I filled in my own argument for this proof because I really didn't understand what Professor Olsson was saying. It's not a very complicated result, unless this proof is wrong, in which case it is Fields Medal-level stuff.

Proof: Consider the map $\mathcal{C} \to \mathbb{Q}_p$ taking (x_n) to its limit (which exists by the above proposition). Clearly, the kernel of this map is I, and the map is surjective; to see this, fix $a \in \mathbb{Q}_p$ and write its Laurent series as

$$a_{-n}p^{-n} + a_{-n+1}p^{-n+1} + \cdots + a_0 + a_1 p + \cdots$$

with $0 \leq a_i < p$. Then take the Cauchy sequence of partial sums of the above Laurent series in $\mathcal{C}$ which clearly maps to a. This sequence is Cauchy since for sufficiently large m, n, the valuation of the difference $\nu_p(a_{n+1}p^{n+1} + \cdots + a_m p^m) \geq n+1$, so $\left|a_{n+1}p^{n+1} + \cdots + a_m p^m\right|_p \leq \frac{1}{p^{n+1}}$.

The kernel of this map is clearly I, and so by the first isomorphism theorem, $\mathcal{C}/I \cong \mathbb{Q}_p$, from which it follows that I is maximal since $\mathbb{Q}_p$ is a field. ■

Exercise 9.1.5

Let p, q be prime numbers. Show that $|\cdot|_p$ and $|\cdot|_q$ define the same topology on $\mathbb{Q} \iff p = q$.

Only the forward direction is nontrivial, so consider the sequence $(p^k)_{k\geq 1}$ which goes to 0 in $|\cdot|_p$, but $\left|p^k\right|_q = 1$ for all k, since p^k is a unit for $p \neq q$, so (p^k) cannot go to zero with respect to $|\cdot|_q$ unless $p = q$. It follows that $|\cdot|_p$ and $|\cdot|_q$ define inequivalent topologies when $p \neq q$ since some sequences converge in one and not the other.

Moving away from the p-adic norm for a moment, consider a more general story: let K be a field, with a nontrivial norm $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying $|x| = 0 \iff x = 0$, $|xy| = |x||y|$, and $|x+y| \leq |x| + |y|$. As always, the norm gives a metric on K, and we say that two norms on K are equivalent if they define the same topology.

Definition 9.1.6

$|\cdot| : K \to \mathbb{R}_{\geq 0}$ is *non-archimedean* if it satisfies the strong triangle inequality, $|x+y| \leq \max(|x|, |y|)$.

In particular, $|\cdot|_p$ on $\mathbb{Q}$ is non-archimedean, but the regular norm on $\mathbb{Q}$ is archimedean.

Theorem 9.1.7

Every norm on $\mathbb{Q}$ is equivalent to the usual norm (often denoted $|\cdot|_\infty$) or one of the p-adic norms.

Proof: Fix some non-archimedean nontrivial norm $|\cdot|$ on $\mathbb{Q}$. Since $|1 \cdot 1| = |1| \cdot |1|$, $|1| = 1$, so $|n| = |1 + \cdots + 1| \leq 1$ by the non-archimedean property. Since our norm is nontrivial, there exists $\alpha \in \mathbb{Q}^\times$ such that $|\alpha| \neq 1$, so picking either its numerator or denominator, there exists $n \in \mathbb{Z}$ such that $|n| < 1$. Moreover, looking at the prime factorization of n, we can see that there exists a prime p such that $|p| < 1$.

Fix $\mathfrak{a} = \{n \in \mathbb{Z} : |n| < 1\} \subset \mathbb{Z}$. By the non-archimedean property, $\mathfrak{a}$ is closed under addition, and is closed under multiplication by elements of $\mathbb{Z}$ since $|n| \leq 1$ for all $n \in \mathbb{Z}$ by our arguments above, therefore, $\mathfrak{a}$ is an ideal of $\mathbb{Z}$. $\mathfrak{a}$ is proper, since $|1| = 1$, and $(p) \subseteq \mathfrak{a}$ for some p by the arguments above, so since (p) is maximal, we can conclude that $\mathfrak{a} = (p)$. Therefore, the unit ball with respect to our norm $|\cdot|$ is equal to the unit ball with respect to $|\cdot|_p$.

So for $n \in \mathbb{Z}$, $n = bp^m$ with p not dividing b. Since b is an integer, $|b| \leq 1$ by arguments made above. However, by construction, $b \notin \mathfrak{a}$, so $|b| \not< 1$, from which it follows that $|b| = 1$. Therefore,

$$|n|_p^{-\log_p |p|} = (p^{-m})^{-\log_p |p|} = p^{\log_p |p|^m} = |p|^m = |n|$$

where the last equality follows from the fact that $|b| = 1$. Hence, for any n, $|n| = |n|_p^s$ where $s = -\log_p |p|$, so $|\cdot| \sim |\cdot|_p$. ■

The archimedean case is more technical, and is available to those who seek it in Neukirch.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lectures 11 and 12: 5-7 October

Professor Martin Olsson — Abhishek Shivkumar

Completions

Recall that $\mathbb{Q}_p$ can be regarded either as the field of fractions of $\mathbb{Z}_p$ or as the completion (in the sense of Cauchy sequences) of $\mathbb{Q}$ with respect to $|\cdot|_p$. This situation generalizes more generally for K a number field, $\mathfrak{p} \subset \mathcal{O}_K$, e.g, $\varprojlim_n \mathcal{O}_K/\mathfrak{p}^n$ is a DVR with field of fractions $K_\mathfrak{p}$, which is also given by the completion (again in the sense of Cauchy sequences) of K with respect to $|\cdot|_\mathfrak{p}$ given by

$$|x|_\mathfrak{p} = \left(\frac{1}{|\mathcal{O}_K/\mathfrak{p}|}\right)^{\nu_\mathfrak{p}(x)}$$

A notational warning: $K_\mathfrak{p}$ can mean either the localization or the field of fractions of the $\mathfrak{p}$-adic completion depending on context.

Lemma 10.1.1

Any extension of $|\cdot|_p$ on $\mathbb{Q}$ to a number field K is equal to $|\cdot|_\mathfrak{p}$ for some prime $\mathfrak{p} \subset \mathcal{O}_K$ over (p).

Also, this lemma was left as an exercise for us to prove.

The idea of the proof is to start with some extension $|\cdot|$ on K, and consider $A = \{x \in K : |x| \leq 1\}$; we want to show that $A = \mathcal{O}_{K,\mathfrak{p}}$ for some $\mathfrak{p}$ since $|x|_\mathfrak{p} \leq 1 \iff \nu_\mathfrak{p}(x) \geq 0$. Consider also $\mathfrak{a} = \{x \in K : |x| < 1\}$, which we want to show is the maximal ideal of $\mathcal{O}_{K,\mathfrak{p}}$. $\mathfrak{a}$ is an ideal (assuming $|\cdot|$ is non-archimedean, via the relevant section of the proof of Theorem 9.1.7) and we can show that $\mathfrak{a}$ is in fact maximal, and it's a general fact that all prime ideals in $\mathcal{O}_K$ contain (p) for some rational prime p.

Lemma 10.1.2

Let K be a field complete with respect to a norm $|\cdot|$, and V a finite dimensional vector space over K. A norm on V extending $|\cdot|$ is a norm on V which agrees with $|\cdot|$ on scalar multiplication; two norms $|\cdot|_1$, $|\cdot|_2$, on V extending $|\cdot|$ on K define the same topology on V iff there exists $\mathbb{R} \ni c_1, c_2 > 0$ such that $c_1|v|_1 \leq |v|_2 \leq c_2|v|_1$.

For what follows, a norm without a subscript refers to the field norm.

Proof: For the reverse direction, note that the topology on a vector space is determined by the open neighborhoods around 0, since the translates of these neighborhoods are all the open neighborhoods in the topology. Therefore, for the two norms to define the same topology, it suffices to show that in every ball around 0 of one norm, a ball of the other norm fits inside it and vice versa, which is precisely what our pair of inequalities above show.

For the forward direction, choose $c > 0$ such that $B_{c,|\cdot|_1}(0) \subseteq B_{1,|\cdot|_2}(0)$ e.g, $|v|_1 \le c \implies |v|_2 \le 1$. Choose $a \in K$ such that $0 < |a| < 1$; then for all $v \in V$ nonzero, there exists a unique integer s such that $c|a| < |a^s v|_1 \le c$. To see this, note that taking the logarithm of these inequalities yields

$$\log c + \log |a| < s \log |a| + \log |v|_1 \le \log c$$

Geometrically, this corresponds to dividing $\mathbb{R}$ into half open segments of length $\log |a|$ based at $\log c$, so that the above inequalities just say that there exists a unique integer s such that $s \log |a| + \log |v|_1 \in (\log c + \log |a|, \log c]$. This much is clear visually.

Then, since $|a^s v|_1 \le c$, $|a^s v|_2 \le 1$ so

$$|v|_2 \le |a|^{-s} < c^{-1}|a|^{-1}|v|_1$$

Therefore, we may set $c_2 = c^{-1}|a|^{-1}$; since v is arbitrary, we have the upper bound on $|v|_2$ we desired. Interchanging $|\cdot|_1$ and $|\cdot|_2$ and running this argument again, we obtain the requisite inequality in the other direction, from which the result follows. ■

Theorem 10.1.3

Fix a norm $|\cdot|_V$ on V over K a field equipped with a norm $|\cdot|_K$, and choose a basis $v_1, \cdots, v_d$ for V. Under the induced identification $V \xrightarrow{\sim} K^d$, the topology on V is the product topology.

Proof: Concretely, given a sequence $(x_n)_{n\in\mathbb{N}}$ in V, write $x_n = x_n^1 v_1 + \cdots + x_n^d v_d$ where the $x_n^i \in K$. Then x_n is Cauchy with respect to $|\cdot|_V$ iff each x_n^i is Cauchy with respect to $|\cdot|_K$.

The strategy we use in this proof has a clear geometric picture: Cauchy convergence of (x_n) corresponds to a ball getting smaller, whereas simultaneous Cauchy convergence of the coefficients corresponds to a cuboid getting smaller. To show, for example, that the product and ordinary topologies on $\mathbb{R}^2$ are equivalent, it suffices to find an open ball around every point in every open box, and vice versa; this is precisely what we are doing by our iff statement about Cauchy sequences.

For the reverse direction,

$$|x_n - x_m|_V \le \sum_{j=1}^{d} \left|x_n^j - x_m^j\right|_K |v_j|_V$$

by the triangle inequality, and if each x_n^i is Cauchy (by assumption), each term on the right hand side can be made arbitrarily small simultaneously, since there are finitely many terms.

The forward direction follows by induction on d, with the $d = 1$ case obvious. Suppose this holds up to $d - 1$; then, replace (x_n) with $(x_n - x_m)_{n,m}$ where the latter is a sequence via the "snake" identification of $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$. Therefore, we can assume that (x_n) tends to 0. Suppose (x_n^j) does not tend to 0 for some j (WLOG $j = 1$ by permuting the basis). Replacing (x_n) again by a subsequence, we can also assume that $\left|x_n^1\right|_K > \epsilon$ for some ϵ, all n. Consider the sequence $\left(\frac{x_n}{x_n^1}\right)_{n\in\mathbb{N}}$ which converges to 0 since (x_n)

does, and the denominator is bounded below. Writing

$$\frac{x_n}{x_n^1} - v_1 = \frac{x_n^2}{x_n^1} v_2 + \cdots + \frac{x_n^d}{x_n^1} v_d$$

The left hand side converges to $-v_1$ by assumption, and each of the coefficients on the right hand side converge by induction, so v_1 is in the span of $v_2, \cdots, v_d$, which contradicts the basis property, from which the result follows. ■

Exercise 10.1.4

Show that $\mathbb{Q}_p$ is totally disconnected, that is, its connected components are its points.

Let K be a number field, $\nu_\mathfrak{p}$ a discrete valuation defined by $\mathfrak{p} \subset \mathcal{O}_K$, L/K a finite extension. Completing with respect to $\nu_\mathfrak{p}$ we obtain $K_\mathfrak{p}$, and fixing an algebraic closure $\overline{K_\mathfrak{p}}$, we have the following diagram:

$$\begin{tikzcd} L \arrow[rr, dashed] & & \overline{K_\mathfrak{p}} \\ K \arrow[u, hook] \arrow[r, hook] & K_\mathfrak{p} \arrow[ur, hook] & \end{tikzcd}$$

Any embedding $\sigma : L \hookrightarrow \overline{K_\mathfrak{p}}$ gives rise to norm on L; specifically, the norm $\omega = \overline{\nu} \circ \sigma$ where $\overline{\nu}$ is the norm on $\overline{K_\mathfrak{p}}$.

Implicit in this discussion is the fact (unknown to me) that a normed field retains its norm under completion with respect to a prime (or its corresponding valuation) and subsequent algebraic closure.

Theorem 10.1.5

With, K, L, $\mathfrak{p}$ etc. as above, two embeddings $\sigma, \tau : L \hookrightarrow \overline{K_\mathfrak{p}}$ give rise to the same absolute value on L iff they are conjugate over $K_\mathfrak{p}$.

We will prove this result later on, after we have developed some general theory.

Fix K a field complete with respect to a norm given by a discrete valuation ν, $|x|_\nu = a^{\nu(x)}$ for some fixed $0 < a < 1$. Let $A \subset K$ be the corresponding valuation ring, e.g, $A = \{x \in K : \nu(x) \geq 0\} \cup \{0\}$. Furthermore, let L/K be a finite separable extension, and B the valuation ring for some extension of ν to L.

I don't think it's clear that such extensions always exist unless we can just extend the norm to some algebraic closure and restrict from there as we did above, but that too is non-obvious. It is clear, I think, that valuations extend to completions, simply by taking the limit.

Proposition 10.1.6

B is a DVR defining a norm on L for which L is complete.

We will sketch the proof of this result: for all $\mathfrak{q} \subset B$ prime over $\mathfrak{p} \subset A$ (with $\mathfrak{p}$ the unique maximal of A), we have that $\varprojlim_n B/\mathfrak{q}^n B$ is a DVR in L. Hence, since B is free over A by Lemma 5.1.6 and the remarks following its proof, we may write $B = Ae_1 \oplus \cdots \oplus Ae_n$. Since different primes all give the same topology on L, by the approximation lemma, only one prime $\mathfrak{q}$ lies above $\mathfrak{p}$.

This is missing quite a bit, especially the last sentence.

Therefore, $\mathfrak{p}B = \mathfrak{q}^e$ for some e. Let ω be the valuation on L defined by B (and $\mathfrak{q}$); then $\omega|_K = e\nu$. Setting $|y|_\omega = a^{\omega(y)/e}$ gives a norm on L extending $|\cdot|_\nu$ on K.

Proposition 10.1.7

Let K be a field, $|\cdot|_1, |\cdot|_2$ two norms on it. They define the same topology on K iff there exists $\lambda > 0$ s.t $|x|_1 = |x|_2^\lambda$ for all $x \in K$.

No proof was offered of this result, but it is available in Neukirch as Proposition 3.3, on page 117.

From this result, and the above discussion on $|\cdot|_\omega$ we can conclude that there exists a unique extension of $|\cdot|_\nu$ on K to L. In fact, this result passes to towers of extensions and (for K perfect) implies that there exists a unique extension of $|\cdot|_\nu$ to $\overline{K}$.

Example 10.1.8

Consider a finite extension $L/\mathbb{Q}_p$ of degree n with B the ring of integers of L ($\mathbb{Z}_p$ the ring of integers of $\mathbb{Q}_p$); by the results above, $pB = \mathfrak{m}_B^e$ for some e, and one can show that $B/\mathfrak{m}_B B \cong \mathbb{F}_{p^f}$ where $n = ef$.

The natural norm on L is given by $|y|_\omega = \frac{1}{q^{\omega(y)}}$ where $q = p^f$, ω as above an extension of ν_p. Therefore, $|\cdot|_\omega^{\frac{1}{n}}$ extends $|\cdot|_p$.

Not entirely sure what we have shown here; we know that the cardinality of the residue field takes the place of p in converting a valuation to a norm (with our guiding example being the p-adic valuation and its associated norm), so the norm we defined above is what we would expect. Then we see that since it's a power of "the" extension norm, they define the same topology. That's my best guess.

Remark 10.1.9

The existence of the unique extension of $|\cdot|_K$ to $\overline{K}$ gives an alternate way to think about the absolute value on L/K; in particular, given $|\cdot|_{\overline{K}}$, pick any embedding $\sigma : L \hookrightarrow \overline{K}$, and restrict $|\cdot|_{\overline{K}}$ to $\sigma(L) \cong L$. This does not depend on σ, since the extension $|\cdot|_{\overline{K}}$ is unique, and therefore fixed by $\mathrm{Gal}(\overline{K}/K)$.

Global to Local

Given K a number field, ν a discrete valuation on K, K_ν the corresponding completion (in either sense). Let $A \subset K$ be the valuation ring of ν, L/K a finite extension, B the integral closure of A in L, $\hat{A}$ the completion of A with respect to the unique maximal.

Note that K_ν/K is almost always transcendental; for example consider $\mathbb{C}((t))$ over $\mathbb{C}(t)$, where $\mathbb{C}((t))$ is the completion of $\mathbb{C}(t)$ with respect to the degree valuation. This is a transcendental extension.

Proposition 10.2.1

$B \otimes_A \hat{A} \cong \prod_{\mathfrak{q}_i | \mathfrak{p}} \hat{B}_i$ where B_i is the completion of B at $\mathfrak{q}_i$.

Proof: First, note that $B \otimes_A \hat{A} \cong \varprojlim_n B/\mathfrak{p}^n B$; since $B = A^d$ for some d by Lemma 5.1.6 and the subsequent discussion, we have that

$$B \otimes_A \hat{A} \cong \hat{A}^d = \varprojlim_n (A/\mathfrak{p}^n)^d = \varprojlim_n B/\mathfrak{p}^n B$$

by various basic results about tensors and completions, and categorical limits commuting. Then, by the Chinese remainder theorem,

$$\prod_{\mathfrak{q}_i \mid \mathfrak{p}} \hat{B}_i = \varprojlim_n B/\mathfrak{q}_1^n \cdots \mathfrak{q}_g^n \cong \varprojlim_n B/\mathfrak{q}_1^n \times \cdots \times B/\mathfrak{q}_g^n$$

Then, since $\mathfrak{q}_1^{rn} \cdots \mathfrak{q}_g^{r_n} \subseteq \mathfrak{p}^n B \subseteq \mathfrak{q}_1^n \cdots \mathfrak{q}_g^n$ for some r (say, $r = \max_i e_i$) since $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$, and $\mathfrak{p}^n B \subseteq \mathfrak{p}B$. Then, we have the following diagram:

$$\begin{tikzcd}
\varprojlim_n B/\mathfrak{p}^n B \arrow[r] & \varprojlim_n B/\mathfrak{q}_1^n \cdots \mathfrak{q}_g^n \\
\varprojlim_n B/\mathfrak{q}^{rn} \cdots \mathfrak{q}_g^{rn} \arrow[u] \arrow[ur, "\cong"'] &
\end{tikzcd}$$

where

$$\varprojlim_n B/\mathfrak{q}_1^{rn} \cdots \mathfrak{q}_g^{rn} \cong \varprojlim_n B/\mathfrak{q}_1^n \cdots \mathfrak{q}_g^n$$

since one is a reindexing of the other. Therefore, the isomorphism we have claimed follows. ■

There are about a thousand details to be checked here, but I think the basic structure is fine. "Reindexing" has to be a misnomer here, the point probably being that looking at every r^{th} element in the inverse limit (in the product form) is enough data to infer the entire element. In fact, we show in this week's homework that

$$\mathbb{Z}_n \cong \prod_{p \mid n} \mathbb{Z}_p$$

so that, in particular, $\mathbb{Z}_{p^r} \cong \mathbb{Z}_p$. We didn't use any special facts about $\mathbb{Z}$ to show this, just the Chinese remainder theorem, so some analogous result holds generally.

Exercise 10.2.2

Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, with $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$. Describe the splitting of (5) in this extension.

$f(x) = x^3 - 2$ is the minimal polynomial for 2, and factors in $\mathbb{F}_5[x]$ as $(x-3)(x^2+3x-1)$, and the quadratic factor is irreducible by exhaustive search (since a quadratic is irreducible iff it has no roots). This tells us that (5) splits without ramification into two primes in $\mathbb{Z}[\sqrt[3]{2}]$.

Consider the following setup, synthesized from our discussions thus far:

$$\begin{tikzcd}
L & B \arrow[l, hook'] \arrow[r, hook] & B \otimes_A \hat{A} & \\
K \arrow[u, hook] \arrow[dr, hook] & A \arrow[l, hook'] \arrow[r, hook] \arrow[u, hook] \arrow[d, hook] & \hat{A} \arrow[u, hook] & \overline{K_\nu} \\
& K_\nu \arrow[urr, hook] & &
\end{tikzcd}$$

Note that the primes $\mathfrak{q} \subset B$ over $\mathfrak{p} \subset A$ are in bijection with valuations ω on L extending ν, leading to the notation $\omega|\nu$.

This analysis follows from the following general procedure: suppose L/K is separable with $L = K(\theta)$ for some $\theta \in \mathcal{O}_L$ with minimal polynomial $p \in \mathcal{O}_K[x]$. Then, fixing $\mathfrak{p}$ prime in $\mathcal{O}_K$ and relatively prime to the conductor of $\mathcal{O}_K[\theta]$, defined as $\{y \in \mathcal{O}_L : y\mathcal{O}_L \subseteq \mathcal{O}_K[\theta]\}$, if

$$\overline{p}(x) = \overline{p_1}(x)^{e_1} \cdots \overline{p_r}(x)^{e_r}$$

where $\overline{p}(x) \equiv p(x) \pmod{\mathfrak{p}}$, then $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + p_i(\theta)\mathcal{O}_L$ are the different prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}$, where the inertia degree f_i of $\mathfrak{q}_i$ is the degree of $\overline{p}_i(x)$ and $\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$. This follows from the fundamental identity.

Note that if $\mathcal{O}_L = \mathcal{O}_K[\theta]$, the conductor restriction does not matter; as such, this is the best case scenario for calculating the primes above a given prime.

Corollary 10.2.3

For all $\omega|\nu$, there exists $\sigma : L \hookrightarrow \overline{K_\nu}$ over K such that L_ω is isomorphic to $\sigma(L)K_\nu$.

Proof: Note that $L \otimes_K K_\nu = \prod_{\omega|\nu} L_\omega$ embeds into $\overline{K_\nu}$, so we can conclude that this map in fact factors through one of the L_ω (since injections out of a product of fields are actually maps out of one of the factors, as otherwise there would be a nontrivial kernel) so that this embedding is in fact an embedding of L_ω into $\overline{K_\nu}$. Then, the composite $L \hookrightarrow L \otimes_K K_\nu \hookrightarrow \overline{K_\nu}$ is an embedding of L into $\overline{K_\nu}$. Since we may embed K_ν into $\overline{K_\nu}$ either directly (by some fixed embedding) or by first embedding it into $L \otimes_K K_\nu$, the result follows by Galois theory. ■

Needs fixing, don't understand the lecture proof. Ditto below, why is $\mathrm{Gal}(\overline{K_\nu}/K_\nu)$ the relevant Galois group?

We are now ready to prove Theorem 10.1.5.

Proof: It is clear that conjugate embeddings give rise to the same absolute value. For the other direction, note again that $L \hookrightarrow \prod_{\omega|\nu} L_\omega \hookrightarrow \overline{K_\nu}$ factors through some specific E_{ω_0}. Then, with σ and τ defining the same absolute values, we have the following diagram

$$E \hookrightarrow \prod_{\omega|\nu} \to E_{\omega_0} \rightrightarrows \overline{K_\nu}$$

where the parallel arrows are σ and τ. By Galois theory, these two embeddings then differ by an element of $\mathrm{Gal}(\overline{K_\nu}/K_\nu)$. ■

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 13: 12 October

Professor Martin Olsson Abhishek Shivkumar

Completions

Given K a number field, ν a discrete valuation on K, E/K a finite extension. By previous results, we know that $E \otimes_K K_\nu \cong \prod_{\omega|\nu} E_\omega$.

Corollary 11.1.1

If $n = [E : K]$, and $n_\omega = [E_\omega, K_\nu]$, then

$$n = \sum_{\omega|\nu} n_\omega = \sum_{\omega|\nu} e_\omega f_\omega$$

Proof: We know that n is equal to the number of embeddings $E \hookrightarrow \overline{K_\nu}$. In turn, via the factorization of embeddings $E \hookrightarrow \overline{K_\nu}$ through $\prod_{\omega|\nu} E_\omega$, it is clear that n is equal to the sum of the n_ω, since we can partition all embeddings $E \hookrightarrow \overline{K_\nu}$ via which E_ω they factor through. ■

One needs to check that embeddings $E \hookrightarrow \overline{K_\nu}$ have image inside a subfield of $\overline{K_\nu}$ isomorphic to $\overline{K}$. In fact, given a finite separable extension E/K, and any embedding $K \hookrightarrow \Omega$ where Ω is an algebraically closed field, then the number of embeddings of E into Ω over K is equal to $[E : K]$. To see this, let $E = K(\alpha)$, f the minimal polynomial of α so that $E \cong K[x]/(f)$. Then K-embeddings of E into some algebraically closed Ω are determined by the image of x, and for this map to be well-defined, x must be a root of f in Ω, of which there are exactly $[E : K]$.

Corollary 11.1.2

If E/K is Galois with Galois group G, then E_ω/K_ν is Galois with group $D_\omega \subset G$.

Theorem 11.1.3: Structure of complete DVRs (equal char.)

Suppose A is a complete discrete valuation ring whose fraction field and residue field have equal characteristic. Then $A = k[[t]]$ where $k = A/\mathfrak{m}$ is the residue field.

The proof is available in Serre II.4., but the idea is to find k inside A. Once you have a section $k \to A$, fix $t \in \mathfrak{m}$ a generator which gives a map $k[t] \to A$, which descends to a map $k[t]/(t^n) \to A/\mathfrak{m}^n$ which is in fact an isomorphism by induction. We have a diagram

$$\begin{tikzcd}
0 \arrow[r] & k(t^{n-1})/(t^n) \arrow[r] \arrow[d, "\cong"] & k[t]/(t^n) \arrow[r] \arrow[d] & k[t]/(t^{n-1}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathfrak{m}^{n-1}/\mathfrak{m}^n \arrow[r] & A/\mathfrak{m}^n \arrow[r] & A/\mathfrak{m}^{n-1} \arrow[r] & 0
\end{tikzcd}$$

The first vertical map is an isomorphism since both are one dimensional

k-vector spaces, and it follows by induction and the five lemma that the map $k[t]/(t^n) \to A/\mathfrak{m}^n$ is an isomorphism. Then we have that

$$k[[t]] = \varprojlim_n k[t]/(t^n) \xrightarrow{\sim} \varprojlim_n A/\mathfrak{m}^n \cong A$$

Theorem 11.1.4: Structure of complete DVRs (mixed char.)

Let A be a complete discrete valuation ring, with characteristic 0 fraction field and characteristic $p > 0$ residue field k, and suppose that k is perfect. Then there is an endofunctor W (where $W(k)$ is called the ring of Witt vectors) on the category of rings with the universal property that $W(k)$ has a unique map to A agreeing the surjection $A \twoheadrightarrow k$, where $W(k) \to A$ is a map of complete DVRs of mixed characteristic with residue field k.

Note that the other mixed characteristic is not possible: if the field of fractions has characteristic p, then $p = 0$ in A, so $p = 0$ in k since k is a quotient of A.

Since k is perfect of positive characteristic, the Frobenius map $\sigma_k : k \xrightarrow{\sim} k$ given by $x \mapsto x^p$ is an automorphism. Then, by functoriality of W, we have $\sigma : W(k) \to W(k)$ an automorphism lifting Frobenius.

Example 11.1.5

Let $E/\mathbb{Q}_p$ be a finite extension; then since $\mathbb{Q}_p$ is of characteristic 0 (as it contains a copy of $\mathbb{Z}$), it follows by the following diagram that we are in the setting of mixed characteristic, whence we have $W(k)$ as below:

$$\begin{tikzcd}
E & \mathcal{O}_E \arrow[l, hook'] \arrow[rr, two heads] & & k \\
& & W(k) \arrow[ul] & \\
\mathbb{Q}_p \arrow[uu] & \mathbb{Z}_p \arrow[l, hook'] \arrow[uu] \arrow[ur] \arrow[rr, two heads] & & \mathbb{F}_p \arrow[uu]
\end{tikzcd}$$

Exercise 11.1.6

Suppose A is a complete DVR, $x \in \mathfrak{m}$, $u = 1 + x \in A^\times$. Then for all $m \in \mathbb{Z}_{\geq 1}$ coprime with the characteristic of k, u has an m^{th} root in A.

This is an easy application of the corollary to Hensel's lemma that we prove below.

Theorem 11.1.7: Hensel's Lemma

Let K be complete with respect to a norm induced by a discrete valuation, the corresponding DVR $\mathcal{O} = \{x \in K | |x| \leq 1\}$ with maximal $\mathfrak{m} = \{x \in K | |x| < 1\}$. Let $f \in \mathcal{O}[x]$, $\alpha_0 \in \mathcal{O}$ s.t $|f(\alpha_0)| < \left|f'(\alpha_0)^2\right|$. Then the sequence $\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$ converges to a root α of f in $\mathcal{O}$ and $|\alpha - \alpha_0| \leq \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1$.

Proof: We will sketch this result, the reference is Lang's Algebraic Number Theory. Fix $c = \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1$. Show by induction that the following results hold:

1. $|\alpha_i| \leq 1$, e.g, the α_i remain in $\mathcal{O}$
2. $|\alpha_i - \alpha_0| \leq c$
3. $\left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leq c^{2^i}$ and $|f'(\alpha_i)| = |f'(\alpha_0)|$

This implies the theorem, as the third condition implies that

$$|\alpha_{i+1} - \alpha_i| = \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| |f'(\alpha_i)| \leq c^{2^i} |f'(\alpha_0)| \to 0$$

so the limit α exists via completeness of K. Moreover, by the fact that $|f'(\alpha_i)|$ is a constant sequence, $|f'(\alpha)| = |f'(\alpha_0)| \neq 0$, so it follows that $|f(\alpha)| = 0 \iff f(\alpha) = 0$. ■

Corollary 11.1.8

If $f(x) \in \mathcal{O}[x]$ has a root $\overline{\alpha} \in k$ the residue field of $\mathcal{O}$, with $f'(\overline{\alpha}) \neq 0$, then f has a root in K.

Proof: Let $\alpha_0 \in \mathcal{O}$ be any lift of $\overline{\alpha}$, so $f(\alpha_0) \in \mathfrak{m}$ by assumption, so $|f(\alpha_0)| < 1$, $f'(\alpha_0)$ a unit since it is nonzero in the residue field, so $|f'(\alpha_0)| = 1$. Then, apply Hensel's lemma, from which the result follows. ■

Note that Taylor's theorem is true for polynomials in any ring, that is,

$$f(x) = \sum_{k \geq 0} \frac{f^{(k)}(a)}{k!}(x-a)^k$$

holds where $\frac{f^{(k)}(a)}{k!}$ is in fact integral and the infinite sum makes sense since f is a polynomial and its derivatives eventually all vanish.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lectures 14 and 15: 14-19 October

Professor Martin Olsson Abhishek Shivkumar

Different and Discriminant

Our setup is the usual one: A Dedekind, K its field of fractions, L/K a degree n separable extension, B the integral closure of A in L. Recall the trace map $\mathrm{tr}_{L/K} : L \times L \to K$ given by $(x, y) \mapsto \mathrm{tr}(xy)$ (where the separability condition guarantees that the map $\mathrm{tr}_{L/K}$ is non-degenerate), which induces an isomorphism $L \xrightarrow{\sim} L^* = \mathrm{Hom}_K(L, K)$. Recall that this induces a map $B \to B^* = \mathrm{Hom}_A(B, A)$, from which we obtain a map

$$\wedge^n B \to \wedge^n B^* = (\wedge^n B)F^* \iff (\wedge^n B)^{\otimes 2} \hookrightarrow A$$

where the map is an embedding since the top exterior power of B is a rank one A-module, so $(\wedge^n B)^{\otimes 2}$ is again rank one, and its image in A is therefore an ideal.

Then, recalling again that $B^* = \{x \in L : \mathrm{tr}(xy) \in A \; \forall y \in B\} \subset L$ is a fractional ideal, we set its inverse $\mathcal{D}_{B/A} \subseteq B$ the "*different*" ideal; equivalently, B^* is the "*codifferent*" ideal.

Let I_L and I_K represent the groups of fractional ideals in L and K respectively, then the norm map can be realized as $N^I_{L/K} : I_L \to I_K$ given by $\beta \mapsto (\beta \cap A)^{f_\beta}$ which we call a norm map because the following diagram commutes:

$$\begin{tikzcd}
L^\times \arrow[r, "N_{L/K}"] \arrow[d] & K^\times \arrow[d] \\
I_L \arrow[r, "N^I_{L/K}"] & I_K
\end{tikzcd}$$

where the map $L^\times \to I_L$ is given by $x \mapsto xB$ and similarly for K.

This requires a proof, which we will sketch; first assume that L/K is Galois with Galois group G, then for $\beta \subset B$, $\mathfrak{p} = \beta \cap A$, by Lemma 7.3.2 and the subsequent discussion, we can write $\mathfrak{p}B = \beta_1^{e_\mathfrak{p}} \cdots \beta_g^{e_\mathfrak{p}}$. Therefore, since $N^I_{L/K}(\beta) = \prod_{\sigma \in G} \sigma(\beta)$ again by Lemma 7.3.2, it follows that $N_{L/K}(\beta) = (\beta_1 \cdots \beta_g)^{e_\mathfrak{p} f_\mathfrak{p}}$ since the size of the decomposition group D_β is $e_\mathfrak{p} f_\mathfrak{p}$.

I'm not entirely sure what we've shown here. We want to show that $AN_{L/K}(x) = N^I_{L/K}(Bx) = (Bx \cap A)^{f_{Bx}}$ for all $x \in L^\times$ (e.g, commutativity of the above diagram). Perhaps this follows by the discussion here, but I don't see how.

For the general case (L/K not Galois), take the Galois closure $E/L/K$, and noting that $N^I_{E/K} = N^I_{L/K} \circ N^I_{E/L}$ and $N_{E/K} = N_{L/K} \circ N_{E/L}$, we have the following diagram:

$$\begin{tikzcd}
E^\times \arrow[r, two heads, "N_{E/L}"] \arrow[d] & L^\times \arrow[r, "N_{L/K}"] \arrow[d] & K^\times \arrow[d] \\
I_E \arrow[r, "N^I_{E/L}"] & I_L \arrow[r, "N^I_{L/K}"] & I_K
\end{tikzcd}$$

The outer rectangle commutes via the Galois case above, as does the left square again by the Galois case. The key observation is that $N_{E/L} : E^\times \twoheadrightarrow L^\times$ is surjective, from which it follows that the right triangle commutes via pulling elements in $L^\times$ back to $E^\times$ then mapping them to $K^\times$ along the outer rectangle, which we know commutes.

By the arguments made above, we can omit the superscript I when talking about norms, since the two notions are equivalent via taking the fractional ideal generated by an element. It's not clear to me why $N_{E/L}$ specifically is surjective. Does this have to do with Galois extensions specifically?

Theorem 12.1.1

$N_{L/K}(\mathcal{D}_{B/A}) = \delta_{B/A}$ where $\delta_{B/A}$ is the discriminant.

Proof: It suffices to consider the case when A is a DVR; to see this, note that $N_{L/K}(\mathcal{D}_{B/A})$ and $\delta_{B/A}$ both live in a Dedekind domain and therefore factor uniquely into prime ideals of B, so showing this equality is the same as showing that the two ideals have equal prime decomposition, and one way to do this is to show that the ramification of each prime is equal in both ideals. Then, consider the following diagram:

$$\begin{tikzcd}
L & S^{-1}B \arrow[l, hook'] & B \arrow[l, hook'] \\
K \arrow[u, hook] & S^{-1}A \arrow[l, hook'] \arrow[u, hook] & A \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

One can show that $S^{-1}\mathcal{D}_{B/A} = \mathcal{D}_{B/A}S^{-1}B = \mathcal{D}_{S^{-1}B/S^{-1}A}$, from which we restrict to the case where A is a DVR.

I do not understand this claim at all, mainly the relevance of the above diagram. The posted lecture notes reference Serre, page 51.

Then B is a free A-module, with basis $e_1, \cdots, e_n$, and $\delta_{B/A} = \det(\mathrm{tr}(e_ie_j))$ by construction of the discriminant. Let $\sigma_1, \cdots, \sigma_n : L \hookrightarrow \overline{K}$ be the embeddings of L into $\overline{K}$ which fix K; it follows by previous results that

$$\mathrm{tr}(e_ie_j) = \sum_{k=1}^{n} \sigma_k(e_ie_j)$$

So, via this identity, the matrix $\mathrm{tr}(e_ie_j)$ can be written as the product of transpose matrices

$$\mathrm{tr}(e_ie_j) = (\sigma_j(e_i))(\sigma_i(e_j)) = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix} \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(e_1) & \cdots & \sigma_n(e_n) \end{pmatrix}$$

Therefore, $\det(\mathrm{tr}(e_ie_j)) = \det(\sigma_i(e_j))^2$.

This is an important result in its own right, and generally the most effective way to calculate discriminants in practice (at least that I have seen thus far).

Now consider a dual basis e_i^* for B^* via the trace pairing; note that B has finitely many prime ideals since all of its primes are above the unique prime of A, so by an easy application of the approximation lemma (7.3.1), we can see that B is a PID. If $\mathfrak{q}$ is a prime of B, then by the approximation lemma, there exists $b \in B$ such that $\nu_{\mathfrak{q}}(b) = 1$ and $\nu_{\mathfrak{p}}(b) = 0$ for all $\mathfrak{p} \neq \mathfrak{q}$, so $xA = \mathfrak{q}$. Therefore, the codifferent fractional ideal B^* can be written as $B^* = B\beta \subset L$ for some $\beta \in L$.

We seem to be implicitly assuming that fractional ideals over a PID are themselves principal, which sounds familiar, but I can't find a reference earlier in my notes.

Therefore

$$\delta_{B^*/A} = \det\big(\sigma_i(e_j^*)\big)^2 = N_{L/K}(\beta)^2 \delta_{B/A}$$

where $N_{L/K}(\beta) = N_{L/K}(B^*) = N_{L/K}(\mathcal{D}_{B/A}^{-1})$ by the definition of the different and our observation above. From this, we can see that

$$N_{L/K}(\mathcal{D}_{B/A})^2 = \delta_{B/A}\delta_{B^*/A}^{-1}$$

and the result will follow if we can show that $\delta_{B/A}\delta_{B^*/A}^{-1} = A$. This follows essentially from matrix multiplication, as it is easy to show that the product of the matrices whose squared determinants give the discriminants in question is the identity matrix. ■

Exercise 12.1.2

Let ζ a p^{th} root of unity for p a prime. Calculate the discriminant of $\mathbb{Z}[\zeta]/\mathbb{Z}$.

Recall from homework that the discriminant can be realized (up to sign) as the field norm of $f'(\zeta)$ where f is the minimal polynomial for ζ, so, since $f = \frac{x^p - 1}{x-1} = 1 + x + \cdots + x^{p-1}$, $f'(\zeta) = \frac{p\zeta^{p-1}}{\zeta - 1}$, so we want to calculate $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\left(\frac{p\zeta^{p-1}}{\zeta-1}\right)$.

Clearly, since the norm is multiplicative, the norm of the numerator is p^{p-1} since the norm of ζ^k is 1, as the corresponding matrix is a permutation matrix for the power basis, and there are $p-1$ rows since $\left[\mathbb{Q}\left(e^{2\pi i/p}\right) : \mathbb{Q}\right] = p-1$ (more generally $\left[\mathbb{Q}\left(e^{2\pi i/m}\right) : \mathbb{Q}\right] = \varphi(m)$) since the "last" basis element we might expect to need is given by the equation

$$\zeta^{p-1} = -(1 + \zeta + \cdots + \zeta^{p-2})$$

e.g in terms of the previous basis elements. It remains to form the norm of the denominator, $\zeta - 1$. Since

$$N(\zeta - 1) = \prod_k (\zeta^k - 1) = \prod_k (1 - \zeta^k) = p$$

in the Galois group formulation of the norm, where the second equality follows from the fact that $p-1$ is even for odd primes, and the final equality from the factorization of $1 + x + \cdots + x^{p-1}$ evaluated at $x = 1$. Therefore, the discriminant (up to sign, since that is implicit in the way in which we are calculating the discriminant) is p^{p-2}.

That A a complete DVR implies that B is a complete DVR is not a result I can see easily, nor is it one I can find reference to earlier in my notes. A proof I found online uses a version of Hensel's lemma.

Theorem 12.1.3

Let β be a prime over $\mathfrak{p}$ in our standard $AKLB$ setup (with L/K finite and separable). Then β is unramified iff $\beta \not| \mathcal{D}_{B/A}$.

Proof: First, we will handle a special case, when A is a complete DVR with unique prime $\mathfrak{p}$. Note that this implies that B is a complete DVR with unique prime β s.t $\beta^e = \mathfrak{p}B$ for some e.

Note that B is a free A-module by Lemma 5.1.6 and the subsequent example, so we may choose a basis over A $e_1, \cdots, e_n$, and consider $\delta_{B/A} = \det(\mathrm{tr}(e_ie_j))$. Note that

$$\delta_{B/A} \equiv \delta_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} \pmod{\mathfrak{p}}$$

since

$$\delta_{B/A} = \begin{cases} A & B/\mathfrak{p}B \text{a separable field extension over } A/\mathfrak{p} \\ \mathfrak{p}^r & \text{else} \end{cases}$$

As an example, consider $k[x]/(x^2)/k$ whose discriminant is the determinant of the matrix

$$\begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(x) \\ \mathrm{tr}(x) & \mathrm{tr}(x^2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

via the obvious basis for $k[x]/(x^2)$ over k. Therefore, $\delta_{(k[x]/(x^2))/k} = 0$.

In either case, $\mathcal{D}_{B/A} = \beta^h$ for $h \geq 0$ with $h = 0$ in the first case and $h > 0$ in the second case above, via the identity $N_{L/K}(\mathcal{D}_{B/A}) = \delta_{B/A}$. In the $h = 0$ case, $\mathfrak{p}B = \beta$ so we have a separable field extension, and the $h > 0$ case is similar.

This assertion is also nonobvious to me, especially that the residue fields forming a separable extension implies that the discriminant is A, or that this implies what we claimed above.

No part of this last part makes any sense to me.

For the general case, note the following property of the different: given field extensions $K \hookrightarrow L \hookrightarrow M$ with rings of integers A, B, and C respectively, then $\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}$ (we will not show this; a reference is Serre, page 51). Moreover, we have as in the proof of Theorem 12.1.1, that $S^{-1}\mathcal{D}_{B/A} = \mathcal{D}_{S^{-1}B/S^{-1}A}$ e.g, the different is compatible with localization. Finally, the different is compatible with completion: given $\mathfrak{p} \subset A$, $\beta \subset B$ over $\mathfrak{p}$, $\hat{B}_\beta$ over $\hat{A}_\mathfrak{p}$ the completions, then $\hat{\mathcal{D}}_{B/A} = \mathcal{D}_{B/A} \cdot \hat{B}_\beta = \mathcal{D}_{\hat{B}_\beta/\hat{A}_\mathfrak{p}}$. The idea of the proof for this property is that, using the localization compatibility again, we may assume that A is local with maximal ideal $\mathfrak{p}$.

We have the following diagram:

$$\begin{tikzcd}
L \otimes_K \hat{K} & B \otimes_A \hat{A}_p \arrow[l, hook'] \\
\hat{K} \arrow[u, hook] & \hat{A}_\mathfrak{p} \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

Then, one can show that there is a trace map $\mathrm{tr}_{L\otimes_K\hat{K}/\hat{K}} : L \otimes_K \hat{K} \to \hat{K}$ which induces pairings as before. Then, again using a basis, one may show that $B^* \otimes_A \hat{A}_\mathfrak{p} = (B \otimes_A \hat{A}_p)^*$ where this duality is in reference to $\mathrm{tr}_{L\otimes_K\hat{K}/\hat{K}}$. Essentially, this result shows that the formation of the codifferent commutes with completion.

Recall also that $B \otimes_A \hat{A}_{\mathfrak{p}} = \prod_{\beta|\mathfrak{p}} \hat{B}_\beta$ by Proposition 10.2.1, so $\mathcal{D}_{B/A}^{-1} \cdot (B \otimes_A \hat{A}_{\mathfrak{p}}) = \prod_{\beta|\mathfrak{p}} \mathcal{D}^{-1}_{\hat{B}_\beta/\hat{A}_{\mathfrak{p}}}$.

Then, applying these facts reduces the general case to the special case; write $\mathcal{D}_{B/A} = \prod_{\text{primes } \beta} \beta^{h_\beta}$. We claim that $h_\beta > 0$ iff β is ramified. Pass to the completions, $\hat{B}_\beta/\hat{A}_{\mathfrak{p}}$ and $h_\beta > 0$ iff $\mathcal{D}_{\hat{B}_\beta/\hat{A}_{\mathfrak{p}}} \neq \hat{B}_\beta$ so it is enough to consider the complete local case. ■

Lots to check here, I can barely follow the logic.

Corollary 12.1.4

There are only finitely many ramified primes in B.

Ramified primes divide $\mathcal{D}_{B/A}$ and only finitely many primes divide a given fractional ideal.

Corollary 12.1.5

$\mathfrak{p} \subset A$ does not divide $\delta_{B/A}$ iff $\mathfrak{p}$ is unramified in B; we say $\mathfrak{p}$ is unramified if all the primes above $\mathfrak{p}$ are unramified.

Exercise 12.1.6

What primes ramify in the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$?

We've previously stated that $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$, which has integral basis $1, \sqrt[3]{2}, \sqrt[3]{4}$. Then, $\delta_{\mathbb{Z}[\sqrt[3]{2}]/\mathbb{Z}} = -2^2 3^3$ by a straightforward calculation, from which it follows that only (2) and (3) ramify in this extension.

Equivalently, without knowing the ring of integers for this extension, one can see that 2 is ramified immediately, and that 3 is ramified since if it is unramified, it is unramified in the Galois closure, which adjoins roots of unity e.g $\frac{1+\sqrt{-3}}{2}$ from which it follows that 3 ramifies in the Galois closure. Unsure how this rules out other primes.

Theorem 12.1.7

Fix $\mathfrak{q} \subset B$ over $\mathfrak{p} \subset A$ in our usual $AKLB$ setup, with L/K finite and separable and $A/\mathfrak{p}$ perfect, and e the ramification of $\mathfrak{q}$ over $\mathfrak{p}$. Then, there are three cases:

1. $\mathfrak{q}^{e-1} | \mathcal{D}_{B/A}$ and the multiplicity of $\mathfrak{q}$ in $\mathcal{D}_{B/A}$ is exactly $e-1$ if the characteristic of $A/\mathfrak{p}$ does not divide e. This is the so-called *tamely ramified* case.
2. If the characteristic of $A/\mathfrak{p}$ does divide e, then $\mathfrak{q}^e | \mathcal{D}_{B/A}$. This is the *wildly ramified* case.
3. If $\mathfrak{q}$ is unramified, then $\mathfrak{q} \nmid \mathcal{D}_{B/A}$.

We will prove this result in the next lecture, a reference is Serre Proposition 13 on page 58.

Example 12.1.8

Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Notice that completing with respect to (3) gives $\mathbb{Q}_3(\sqrt[3]{2})/\mathbb{Q}_3$ which is a degree three extension with $f = 1$; to see that $f = 1$, note that $x^3 - 2 \pmod 3 \equiv x^3 + 1 \pmod 3 = (x+1)^3 \pmod 3$ which implies that the residue field extension is trivial.

To see that the degree of the extension is three, note that cubic polynomials are either irreducible or have a root, which implies that $x^3 - 2$ is irreducible in $\mathbb{Q}_3(\sqrt[3]{2})$ by Hensel's lemma, from which the result follows.

$x^3 - 2 \pmod 9$ has no solutions, and note that this does not contradict Hensel's lemma since the derivative vanishes.

Therefore, $3\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathfrak{q}^3$ so $\mathfrak{q}^3$ divides the different (since we are in the wildly ramified case).

I missed the last bit of this example, which explains how to use this to calculate the discriminant of $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lectures 16 and 17: 21-26 October

Professor Martin Olsson Abhishek Shivkumar

Finishing Theorem 12.1.7

Consider our standard $AKLB$ setup with L/K finite and separable, $A/\mathfrak{p}$ perfect for some prime $\mathfrak{p} \subset A$, e.g, the setting where Theorem 12.1.7 applies. Note that Theorem 12.1.3 suffices to show the third part of Theorem 12.1.7. For the first two parts, we will provide a sketch: the main idea is reduction to the case where A is a complete DVR. Consider $\hat{B}_\mathfrak{q}$ over $\hat{A}_\mathfrak{p}$, and note that $\mathfrak{q}\hat{B}_\mathfrak{q}$ is the unique maximal of $\hat{B}_\mathfrak{q}$ lying over $\mathfrak{p}\hat{A}_\mathfrak{p}$ the unique maximal of $\hat{A}_\mathfrak{p}$, with ramification e. Then, as we have stated previously, $\mathcal{D}_{B/A} \cdot \hat{B}_\mathfrak{q} = \mathcal{D}_{\hat{B}_\mathfrak{q}/\hat{A}_\mathfrak{p}}$.

Note that the ramification index e doesn't change upon completion because $\mathfrak{p}B = \mathfrak{q}^e(\text{other primes})$ and so $(\mathfrak{p}\hat{A}_\mathfrak{p})\hat{B}_\mathfrak{q} = (q^e(\text{other primes}))\hat{B}_\mathfrak{q}$ and the other primes become the unit ideal upon completion, so in fact $(\mathfrak{p}\hat{A}_\mathfrak{p})\hat{B}_\mathfrak{q} = \mathfrak{q}^e\hat{B}_\mathfrak{q}$.

After reducing to the complete DVR case, we want to reduce to the totally ramified case. To that end, consider the following diagram:

$$\begin{tikzcd}
L & & B \arrow[ll, hook'] \\
& K^{\mathrm{un}} \arrow[ul, hook] & A^{\mathrm{un}} \arrow[l, hook'] \arrow[u, hook] \\
K \arrow[uu, hook] \arrow[ur, hook] & & A \arrow[ll, hook'] \arrow[u, hook]
\end{tikzcd}$$

where $A \hookrightarrow A^{\mathrm{un}}$ is unramified, and $A^{\mathrm{un}} \hookrightarrow B$ is totally ramified, K^{un} the field of fractions of A^{un}. Then, we have $A \hookrightarrow W(B/\mathfrak{q}) \hookrightarrow B$ where W represents the Witt vector functor.

I don't really know what role the Witt vectors play here, I'll try to update once slides are posted. I don't know which of the identities for the different we have actually shown and which we are just invoking.

So K^{un} is the field of fractions of $W(B/\mathfrak{q}) \cdot K \subseteq L$ with ring of integers $W(B/\mathfrak{q}) \otimes_{W(A/\mathfrak{p})} A$. Then, from the fact that $\mathcal{D}_{L/K} = \mathcal{D}_{L/K^{\mathrm{un}}} \cdot \mathcal{D}_{K^{\mathrm{un}}/K} = \mathcal{D}_{L/K^{\mathrm{un}}}$, we can conclude that it suffices to prove the theorem in the case where A is a complete DVR and L/K is totally ramified.

In this case, $B = A[\alpha]$ where α satisfies an Eisenstein polynomial.

Proposition 13.1.1

Let A be a complete DVR with maximal $\mathfrak{p}$, B/A as above with only one prime $\mathfrak{q} \subset B$ over $\mathfrak{p}$, and with $B/\mathfrak{q}$ separable over $A/\mathfrak{p}$. Then there exists $\alpha \in B$ such that $B = A[\alpha]$ and α satisfies an Eisenstein polynomial.

Proof: Choose $\beta \in B$ such that $\overline{\beta} \in B/\mathfrak{q}$ generates $B/\mathfrak{q}$ over $A/\mathfrak{p}$ (since L/K is totally ramified). Let $f \in A[x]$ be a monic polynomial reducing to the irreducible polynomial of $\overline{\beta}$ over $A/\mathfrak{p}$, and let $\gamma \in \mathfrak{q}$ be a uniformizer.

Then $f(\beta+\gamma) \equiv f(\beta) + f'(\beta)\gamma \pmod{\mathfrak{q}^2}$, and $f'(\beta) \not\equiv 0 \pmod{\mathfrak{q}}$ since the residue extension is separable by assumption. Therefore, $f'(\beta)\gamma$ is not in $\mathfrak{q}^2$ so for $\alpha = \beta$ or $\beta + \gamma$, there exists an element in $A[\alpha] \subseteq B$ of order 1 at $\mathfrak{q}$. We claim, then, that $B = A[\alpha]$. By Nakayama's lemma, it suffices to show that $\mathfrak{p}B + A[\alpha] = B$, or, equivalently, that $A[\alpha]/\mathfrak{p}A[\alpha] \to B/\mathfrak{q}^e$ is surjective. To see this, consider the following diagram:

Don't follow the invocation of Nakayama's lemma here or why the two things we claim are equivalent above are equivalent, will try to update when I can take a look at the lecture slides.

$$\begin{tikzcd}
 & & A[\alpha] \arrow[d] \arrow[dr] \arrow[drrr, two heads] & & & \\
0 \arrow[r] & \mathfrak{q}^{e-1}/\mathfrak{q}^e \arrow[r] & B/\mathfrak{q}^e \arrow[r] & B/\mathfrak{q}^{e-1} \arrow[r] & \cdots \arrow[r, two heads] & B/\mathfrak{q}
\end{tikzcd}$$

We know that $A[\alpha] \to B/\mathfrak{q}$ is surjective, so we want to show that all downward arrows are surjective. Suppose we have shown that $A[\alpha] \to B/\mathfrak{q}^{e-1}$ is surjective, with kernel $\tau \subset A[\alpha]$. Then, note that $\mathfrak{q}^{e-1}/\mathfrak{q}^e$ is a one dimensional space over $B/\mathfrak{q}$ with basis $[\omega^{e-1}]$ for any uniformizer $\omega \in \mathfrak{q}$, so if we can show that $\tau \to \mathfrak{q}^{e-1}/\mathfrak{q}^e$ is surjective, then the result follows by a diagram chase.

To show that we can choose f to be Eisenstein, fix an algebraic closure and write $f(x) = \prod(x - \sigma(\alpha))$. Now notice that norm of $\sigma(\alpha)$ is the same for all σ by unique extension of norm $|\cdot|_{\mathfrak{p}}$ to the algebraic closure, so via Viète;s relations, the coefficients are in $\mathfrak{p}$ via the non-archimedean property of the norm. To show that $a_0 \notin \mathfrak{p}^2$, note that L/K is separable and totally ramified so $|a_0| = |\alpha|^e$ which implies $a_0 \notin \mathfrak{p}^2$ due to the chosen normalization: $a_0 \in \mathfrak{q}^e$ which implies that $\nu_{\mathfrak{q}}(a_0) = e$ so the valuation of a_0 is 1 with respect to $\mathfrak{p}$. ■

I didn't follow large sections of this, I'll try to post a more detailed proof when the lecture slides are up. Another resource is Serre, page 20.

Finally, with the above result, we claim that $\mathcal{D}_{B/A} = (f'(\alpha))$. To see this, let f be the required polynomial from the above argument, and write

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

with

$$f'(\alpha) = e\alpha^{e-1} + (e-1)a_{e-1}\alpha^{e-2} + \cdots + a_1$$

There's some discussion at the beginning of Lecture 17 about the term paper that I didn't transcribe. General idea: term paper should have a clear goal from the outset, then build towards that as opposed to a sequence of lemmas and propositions.

Recall that α has order one in $\mathfrak{q}$ by the above proof, so if the characteristic of $A/\mathfrak{p}$ does not divide e, then all the coefficients of $f'(x)$ are in $\mathfrak{p}B = \mathfrak{q}^e$ except for e, and $e\alpha^{e-1} \in \mathfrak{q}^{e-1}$ so $f'(\alpha)$ is the sum of a nonzero element (e.g, a generator) of $\mathfrak{q}^{e-1}$ and elements in $\mathfrak{q}^e$. This implies that $(f'(\alpha)) = \mathfrak{q}^{e-1}$. If the characteristic of $A/\mathfrak{p}$ *does* divide e, then $f'(\alpha)$ is the nonzero sum of elements in $\mathfrak{q}^e$, so $(f'(\alpha)) \subseteq \mathfrak{q}^e$ (since the lead term vanishes).

It remains to show that the different is in fact equal to $(f'(\alpha))$; in fact we can show something stronger:

Lemma 13.1.2

Let $E = K(\alpha)$, f a *separable* irreducible minimal polynomial of α over K, and

$$\frac{f(x)}{x-\alpha} = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$$

Then the dual basis of $1, \alpha, \cdots, \alpha^{n-1}$ is $\frac{b_0}{f'(\alpha)}, \cdots, \frac{b_{n-1}}{f'(\alpha)}$, i.e,

$$\operatorname{tr}\left(\alpha^i \frac{b_j}{f'(\alpha)}\right) = \delta_{ij}$$

Proof: Let $\alpha_1, \cdots, \alpha_n$ be the distinct roots of f in some algebraic closure of $K(\alpha)$, then

$$\sum_{i=1}^{n} \frac{f(x)}{x-\alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)} = x^r$$

for all $0 \leq r \leq n-1$. To see this, subtract the left hand side from the right hand side to obtain a polynomial of degree $n-1$ (for any choice of r) with roots $\alpha_1, \cdots, \alpha_n$. Plug in $\alpha_1 = \alpha$:

$$\left[\frac{f(x)}{x-\alpha_1}\right](\alpha_1)\frac{\alpha_1^r}{f'(\alpha_1)} = \alpha_1^r$$

from which it follows that $\left[\frac{f(x)}{x-\alpha_1}\right](\alpha_1)\frac{1}{f'(\alpha_1)} = 1$. This implies that

$$\operatorname{tr}\left(\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}\right) = x^r$$

where the trace is taken coefficient-wise on the polynomial, so noting that

$$\frac{f(x)}{x-\alpha} = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$$

we have that

$$\operatorname{tr}\left(b_i \frac{\alpha^r}{f'(\alpha)}\right) = \delta_{ir}$$

as claimed. ■

Finally, we may conclude that $B^* = \frac{1}{f'(\alpha)}B$; the above lemma shows that B^* is the B-submodule of L generated by $\frac{b_j}{f'(\alpha)}$, so if we may write the b_i

in terms of $1, \alpha, \cdots, \alpha^{n-1}$, the result would follow. This is an elementary observation, again from

$$\frac{f(x)}{x-\alpha} = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$$

Since f is monic, $b_{n-1} = 1$. For the other coefficients, note that $b_{n-2} - \alpha b_{n-1} = a_{n-1}$, $b_{n-3} - \alpha b_{n-2} = a_{n-2}$ and so on, which follows by multiplying the above identity by $x - \alpha$ and identifying coefficients, and the result follows.

Cyclotomic Fields

Let n be an integer, ζ_n a primitive n^{th} root of unity (e.g, $\zeta_n^n = 1$, $\zeta_n^m \neq 1$ for $m < n$). A good standard choice is $\zeta_n = e^{2\pi i/n}$. Consider $K_n = \mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, with $n = p^r$, p prime, $r \geq 1$ which is equipped with a natural action by $(\mathbb{Z}/(p^r))^\times$, where i acts by sending ζ_n to ζ_n^i.

Lemma 13.2.1

For all $i \in (\mathbb{Z}/(p^r))^\times$, $\frac{1-\zeta_{p^r}^i}{1-\zeta_{p^r}} \in \mathcal{O}_{K_n}^\times$.

Proof:

$$\frac{1-\zeta_{p^r}^i}{1-\zeta_{p^r}} = 1 + \zeta_{p^r} + \cdots + \zeta_{p^r}^{i-1} \in \mathcal{O}_{K_n}$$

Note that $\zeta_{p^r}^i$ is also a primitive p^r-th root of unity since $i \in (\mathbb{Z}/(p^r))^\times$, so there exists j minimal such that $\left(\zeta_{p^r}^i\right)^j = \zeta_{p^r}$. By repeating the above argument, we have that

$$\frac{1-\left(\zeta_{p^r}^i\right)^j}{1-\zeta_{p^r}^i} = \frac{1-\zeta_{p^r}}{1-\zeta_{p^r}^i} \in \mathcal{O}_{K_n}$$

e.g, $\frac{1-\zeta_{p^r}^i}{1-\zeta_{p^r}}$ is invertible in $\mathcal{O}_{K_n}$ as claimed. ■

Note the expansion

$$\frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}} = \prod_{i \in (\mathbb{Z}/(p^r))^\times} (x - \zeta_{p^r}^i)$$

where the latter equality is via the fact (which we have used above) that $(\mathbb{Z}/(p^r))^\times$ indexes *primitive* roots of unity.

Setting $x = 1$, we have that $p\mathcal{O}_{K_n} = \prod_{i \in (\mathbb{Z}/(p^r))^\times}(1 - \zeta_{p^r}^i)$ which we can write as a unit times $(1-\zeta_{p^r})^{\varphi(p^r)}$ where $\varphi(p^r)$ is defined to be the size of $(\mathbb{Z}/(p^r))^\times$ the group of units of $\mathbb{Z}/(p^r)$ (more generally, this is how we define $\varphi(n)$, Euler's totient function).

It follows that $[K_n : \mathbb{Q}] = \varphi(p^r)$ since (p) is totally ramified in K_n, and $e_{(p)} = \varphi(p^r)$. Moreover, one can show (though we will not) that the discriminant of $\mathbb{Z}[\zeta_{p^r}]$ is $p^{p^{r-1}(p^r-r-1)}$, and that all other primes are unramified.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 17: 28 October

Professor Martin Olsson Abhishek Shivkumar

Cyclotomic Fields

Recall our setup with $K_n = \mathbb{Q}(\zeta_n)$, ζ_n a primitive n^{th} root of unity, equipped with an action $(\mathbb{Z}/(n))^\times \curvearrowright \mathbb{Q}(\zeta_n)$ where i acts by $\zeta_n \mapsto \zeta_n^i$.

Proposition 14.1.1

Let $n = p^r$ for some $r \geq 1$. Then $\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n]$.

Proof: As always, we know that $\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_{K_n}$, we just need to show equality.

It suffices to show that, for all primes l, the inclusion $\mathbb{Z}[\zeta_n] \hookrightarrow \mathcal{O}_{K_n}$ becomes an isomorphism upon localization by l: $\mathbb{Z}[\zeta_n]_l \xrightarrow{\sim} \mathcal{O}_{K_n,l}$ (it is a well known result in commutative algebra that checking if a map if an isomorphism is the same as checking if all of its localizations are isomorphisms). To check this, we complete with respect to l, since this allows us to apply Proposition 13.1.1:

There's some discussion in here about showing this result via showing that two codifferent ideals are equal, which I have excised to a margin note since it seems sort of unrelated to the way we end up proving the result (localizations).

It suffices to show that $\mathcal{D}_{\mathbb{Z}[\zeta_n]/\mathbb{Z}} = \mathcal{D}_{\mathcal{O}_{K_n}/\mathbb{Z}}$, since if we have $\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_{K_n} \subseteq \mathcal{O}_{K_n}^* \subseteq \mathbb{Z}[\zeta_n]^*$ via the trace pairing, the inclusion $\mathbb{Z}[\zeta_n] \subseteq \mathbb{Z}[\zeta_n]^*$ gives us the codifferent $\mathcal{D}^{-1}_{\mathbb{Z}[\zeta_n]/\mathbb{Z}}$ and the inclusion $\mathcal{O}_{K_n} \subseteq \mathcal{O}_{K_n}^*$ gives us the codifferent $\mathcal{D}^{-1}_{\mathcal{O}_{K_n}/\mathbb{Z}}$ so these two are equal iff $\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_{K_n}$ is an equality.

$$\begin{tikzcd}
\mathbb{Q}_l(\zeta_n) & \mathbb{Z}_l[\zeta_n] \arrow[l, hook'] \\
\mathbb{Q}_l \arrow[u, hook] & \mathbb{Z}_l \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

We know from Proposition 13.1.1 that $\mathcal{O}_{\mathbb{Q}_l(\zeta_n)} = \mathbb{Z}_l[\alpha]$, and we may take α to be ζ_n.

Not sure why we can take α to be ζ_n; something about the proof of Proposition 13.1.1? Order 1 at the maximal etc. Really did not understand the $l = p$ localization comment.

The only nontrivial case is when we localize and complete at $l = p$; in this case, one can check that $1 - \zeta_n$ has order 1, which suffices. ■

This discussion is useful in determining the corresponding facts for general cyclotomic fields.

Theorem 14.1.2

Let $n = p_1^{r_1} \cdots p_s^{r_s}$. Then $[K_n : \mathbb{Q}] = \varphi(n) := |(\mathbb{Z}/(n))^\times|$, the only primes ramified in K_n are the p_i, and $e_{p_i} = (p_i - 1)p_i^{r_i - 1}$. K_n is Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/(n))^\times$.

A fact which was mentioned (from Lang's Algebraic Number Theory) but which didn't really fit in with the flow of the proof above: $\mathcal{D}_{B/A}$ is the greatest common divisor of ideals $(f'(\alpha))$ for $\alpha \in B$, f the irreducible polynomial of α.

Proof: The key idea of the proof is the following diagram:

$$\begin{tikzcd}
 & K_n & \\
\mathbb{Q}(\zeta_{p_1^{r_1}}) \arrow[ur, hook] & \cdots \arrow[u, hook] & \mathbb{Q}(\zeta_{p_s^{r_s}}) \arrow[ul, hook] \\
 & \mathbb{Q} \arrow[ul, hook] \arrow[u, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Each $\mathbb{Q}(\zeta_{p_i^{r_i}})$ is contained in $K_n = \mathbb{Q}(\zeta_n)$ since

$$\zeta_n = e^{\frac{2\pi i}{p_1^{r_1}\cdots p_s^{r_s}}} \implies \zeta_n^{p_1^{r_1}\cdots p_{i-1}^{r_{i-1}} p_{i+1}^{r_{i+1}}\cdots p_s^{r_s}} = \zeta_{p_i^{r_i}}$$

Then, we may proceed via induction on s, where the $s = 1$ case is the prime power case we have discussed above. For the inductive step, consider $n' = p_1^{r_1} \cdots p_{s-1}^{r_{s-1}}$, with the following diagram:

$$\begin{tikzcd}
 & K_n & \\
K_{n'} \arrow[ur, hook, "\varphi(p_s^{r_s})"] & & \mathbb{Q}(\zeta_{p_s^{r_s}}) \arrow[ul, hook] \\
 & \mathbb{Q} \arrow[ul, hook, "(\mathbb{Z}/(n'))^\times"] \arrow[ur, hook] &
\end{tikzcd}$$

The result follows by inspection of this diagram and from the fact that the two extensions in this diagram are disjoint. ■

I didn't really understand the end of this proof, I'll fix this part when notes are uploaded.

Quadratic Reciprocity

For what follows, let p be an odd prime.

Definition 14.2.1: Legendre Symbol

Given p an odd prime, $a \in \mathbb{F}_p^\times$, we define the *Legendre symbol* as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & x^2 \equiv a \pmod{p} \text{ for some } x \in \mathbb{F}_p \\ -1 & \text{else} \end{cases}$$

In fact, $\left(\frac{-}{p}\right)$ defines a homomorphism from $\mathbb{F}_p$ to $\mathbb{Z}/(2)$ presented as $\{1, -1\}$, e.g, the Legendre symbol is multiplicative. This follows from the following more general result:

This wasn't in lecture, I added it in.

Proposition 14.2.2: Euler's Criterion

Let p be an odd prime, $a \in \mathbb{F}_p^\times$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Proof: This result follows by analysis of the polynomial $x^{p-1} - 1 \in \mathbb{F}_p[x]$. Since $p-1$ is even, we can write

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

Note that Fermat's Little Theorem implies that every element of $\mathbb{F}_p^\times$ is a root of this polynomial, so each element of $\mathbb{F}_p^\times$ is in fact a root of exactly one of the factors (since a degree $p-1$ polynomial has at most $p-1$ roots). Clearly, $a \in \mathbb{F}_p^\times$ is a square iff there exists x s.t

$$x^2 \equiv a \pmod{p} \iff x^{2\frac{p-1}{2}} = x^{p-1} = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$$

E.g, a is a square iff $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$. Therefore, if a is not a square, then a is a root of the right factor of our polynomial, e.g, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, from which the result follows. ■

Note that this result also shows that exactly half of $\mathbb{F}_p^\times$ are squares and half are non-squares, since each factor must have $\frac{p-1}{2}$ distinct roots.

Proposition 14.2.3

Let

$$S = \sum_{\nu \in (\mathbb{Z}/(p))^\times} \left(\frac{\nu}{p}\right) \zeta^\nu \in \mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta)$$

for an odd prime p. Then $S^2 = \left(\frac{-1}{p}\right)p$.

Proof: By observation, we can write

$$S^2 = \sum_{\nu,\mu} \left(\frac{\nu\mu}{p}\right) \zeta^{\nu+\mu}$$

Then, reindexing ν as $\nu\mu$ since both are units and this just permutes the sum, we have that

$$S^2 = \sum_{\nu,\mu} \left(\frac{\nu\mu^2}{p}\right) \zeta^{\mu(\nu+1)} = \sum_{\nu,\mu} \left(\frac{\nu}{p}\right) \zeta^{\mu(\nu+1)}$$

where the second equality is from the fact that $\nu\mu^2$ is a square iff ν is. We may split the above sum into two sums:

$$S^2 = \sum_{\nu \neq -1} \left(\frac{\nu}{p}\right) \sum_{\mu} \zeta^{\mu(\nu+1)} + \sum_{\mu} \left(\frac{-1}{p}\right)$$

The latter sum is equal to $(p-1)\left(\frac{-1}{p}\right)$; moreover, $\sum_\nu \left(\frac{\nu}{p}\right) = 0$ from the fact shown above that precisely half of $\mathbb{F}_p^\times$ are nonsquares, and half are squares, so $\sum_{\nu\neq -1}\left(\frac{\nu}{p}\right) = -\left(\frac{-1}{p}\right)$. Finally,

$$\sum_{\mu}\zeta^{\mu(\nu+1)} = \sum_{\mu}\xi^{\mu} = \xi + \xi^2 + \cdots + \xi^{p-1} = -1$$

where $\xi = \zeta^{\nu+1}$, so we may conclude that

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

as claimed. ■

Lemma 14.2.4

Every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Proof: Consider $\mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free. We want to show that $\sqrt{d} \in \mathbb{Q}(\zeta_n)$ for some n, from which the result would follow. It suffices to show this for $d = p$ prime, since the composite extension of cyclotomic extensions is itself cyclotomic by taking the least common multiple of the indices involved. For p odd, if $p \equiv 1 \pmod 4$, then

$$\sqrt{p} = \sum_{k=0}^{p-1}\zeta_p^{k^2}$$

and similarly if $p \equiv 3 \pmod 4$, then

$$i\sqrt{p} = \sum_{k=0}^{p-1}\zeta_p^{k^2}$$

It follows that $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_n)$ for $n = p$ and $n = 4p$ respectively. To see that the quadratic Gauss sums above sum to $\sqrt{p}$ and $i\sqrt{p}$, note that

$$\sum_{k=0}^{p-1}\zeta_p^{k^2} = \sum_{k=0}^{p-1}\left(1 + \left(\frac{k}{p}\right)\right)\zeta_p^k$$

since in the former sum, squares in $\mathbb{F}_p^\times$ are counted twice in k^2, so we may instead sum over all of $\mathbb{F}_p$ and allow $\left(1 + \left(\frac{k}{p}\right)\right)$ to set non-square terms to zero, and scale square terms by 2. By inspection, the latter sum is the sum S of Proposition 14.2.3, and therefore squares to $\left(\frac{-1}{p}\right)p$. By Euler's criterion, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, from which our mod 4 analysis and conclusions follow.

Finally, for $p = 2$, it is clear that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ since $(1+i)^2 = 2i \iff \frac{1+i}{\sqrt{i}} = \sqrt{2}$. ■

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lectures 18-20: 2-9 November

Professor Martin Olsson Abhishek Shivkumar

Quadratic Reciprocity

I asked about optional lectures during dead week, Professor Olsson says he's open to the idea if people have topics they want to hear about.

Theorem 15.1.1: Quadratic Reciprocity

Let p, q be odd primes. Then

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

Before we prove this theorem, a few remarks; first, note that we can extend the Legendre symbol $\left(\frac{-}{p}\right)$ from $\mathbb{F}_p^\times$ to $\mathbb{Z}$ by setting $\left(\frac{n}{p}\right) = 0$ when $p|n$. This implies, then, that $x^2 - n$ has $1 + \left(\frac{n}{p}\right)$ roots modulo p by inspection. **Proof:** The proof is a direct application of Proposition 14.2.3; we may write

There were some remarks in here that I didn't quite understand about the discriminant of $\mathbb{Q}(\sqrt{p})$ and the values of f_q for some extension being related to the Legendre symbol.

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

where the final equality is via two applications of Euler's criterion (Proposition 14.2.2). On the other hand, since raising a sum to the q^{th} power mod q is the same as raising each summand to the q^{th} power,

$$S^q = \sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right)^q \zeta^{\nu q} \equiv \left(\frac{q}{p}\right)\sum_{n=1}^{p-1}\left(\frac{\nu q}{p}\right)\zeta^{\nu q} \equiv S\left(\frac{q}{p}\right) \pmod{q}$$

where $\left(\frac{\nu}{p}\right)^q = \left(\frac{\nu}{p}\right)$ since raising ± 1 to an odd power does not alter it, and where the final equality is just the fact that νp is a reindexing of ν since p is a unit mod q. Finally, multiplying by S, we have

$$S^{q+1} \equiv S^2(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv S^2\left(\frac{q}{p}\right)$$

The claim follows by dividing by S^2, which we can do since $S^2 = \left(\frac{-1}{p}\right)p$ is nonzero. ■

Someone asks: this proof is all well and good but why would anyone write down the sum S in the first place? Professor Olsson says: I think of S as a kind of Fourier transform. Unclear what this means.

Minkowski's Bound

Let $K/\mathbb{Q}$ be a number field, $\mathrm{Cl}(K)$ its class group, and recall that any element of $\mathrm{Cl}(K)$ can be represented by an ideal of $\mathcal{O}_K$ (by clearing denominators).

Proposition 15.2.1

Let $n = [K : \mathbb{Q}]$, then $n = r_1 + 2r_2$ where r_1 is the number of embeddings $K \hookrightarrow \mathbb{R}$ and r_2 is the number of embeddings (up to complex conjuation) of embeddings $K \hookrightarrow \mathbb{C}$ whose image is not contained in $\mathbb{R}$.

Proof: We know that $K/\mathbb{Q}$ is separable so n is equal to the number of embeddings $K \hookrightarrow \overline{\mathbb{Q}}$, which we think of as sitting inside of $\mathbb{C}$. Then, a given embedding either lies inside $\overline{Q} \cap \mathbb{R}$, or does not. If we have r_1 embeddings of the former type, then each embedding of the latter type up to conjugation is in fact 2 distinct embeddings when we remove the "up to conjugation" requirement, from which the result $n = r_1 + 2r_2$ follows. ■

We've discussed the norm of an ideal before, but I'm adding a definition here because previously it was just sort of thrown in in the fog of war.

Definition 15.2.2: Norm of an ideal

In our standard $AKLB$ setup, we have a map $N_{B/A}$ from the set of fractional ideals of L to the fractional ideals of K given by

$$N_{B/A}(\mathfrak{b}) = (\{N_{L/K}(x) : x \in \mathfrak{b}\})$$

e.g, the ideal generated by the norms of the elements of $\mathfrak{b}$.

$N_{B/A}$ is the unique homomorphism satisfying $N_{B/A}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{p}}$ for $\mathfrak{p} = \mathfrak{q} \cap A$ the prime ideal of A below $\mathfrak{q}$. Additionally, the two notions of a norm are well-behaved with respect to each other in the sense that the following diagram commutes:

$$\begin{tikzcd}
L^\times \arrow[r, "N_{L/K}"] \arrow[d, "y \mapsto (y)"] & K^\times \arrow[d, "x \mapsto (x)"] \\
\mathcal{I}_B \arrow[r, "N_{B/A}"] & \mathcal{I}_A
\end{tikzcd}$$

where $\mathcal{I}$ denotes the set of fractional ideals.

It is important to note that in the special case of $AKLB$ where $K = \mathbb{Q}$, $A = \mathbb{Z}$, the norm $N_{\mathcal{O}_L/\mathbb{Z}}$ of an integral ideal $I \subseteq \mathcal{O}_L$ is simply the size of the quotient ring $\mathcal{O}_L/I$. We will not show this.

The nomenclature $N_{B/A}$ is weird to me, it seems like it should also be $N_{L/K}$ here. Also I'm not sure if this descends to a morphism of class groups, but I'm pretty sure this was mentioned. In the case we care about, $K = \mathbb{Q}$ and L is a number field, since the fractional ideals of $\mathbb{Z}$ are all principal (e.g $\text{Cl}(\mathbb{Z})$ is trivial) via finding a common denominator of generators, we may take the codomain of $N_{\mathcal{O}_L/\mathbb{Z}}$ to be the positive rational numbers.

Theorem 15.2.3: Minkowski's Bound

Let $M_K = \sqrt{|D_K|}\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$ where D_K is the discriminant. Then every element of $\text{Cl}(K)$ can be represented by an ideal $I \subset \mathcal{O}_K$ with $N_{\mathcal{O}_K/\mathbb{Z}}(I) = |\mathcal{O}_K/I| \leq M_K$.

Note that the norm of an integral (meaning non-fractional) ideal must be integral via a result stating that the norm restricts to the ring of integers. Moreover, note that if $M_K < 2$ for $K/\mathbb{Q}$ a number field, then each fractional ideal is represented by some integral ideal $\mathfrak{a}$ with $N_{\mathcal{O}_K/\mathbb{Q}}(\mathfrak{a}) < 2$, so $N_{\mathcal{O}_K/\mathbb{Q}}(\mathfrak{a}) = 1$ and $\mathcal{O}_K/\mathfrak{a}$ is trivial, so $\mathfrak{a} = \mathcal{O}_K$ and $\mathrm{Cl}(K)$ is trivial.

Example 15.2.4

Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$, $n = 2$, $|D_K| = 4$, $r_2 = 1$. Then $M_K = \frac{4}{\pi} < 2$, so we can conclude that every fractional ideal is equivalent to an ideal of norm 1, which implies that $\mathrm{Cl}(\mathbb{Q}(i))$ is trivial.

More generally, to calculate $\mathrm{Cl}(K)$ for $K/\mathbb{Q}$ a number field, we need only to consider the primes p with $p \leq M_K$; this follows from the fact that fractional ideals factor into prime ideals in Dedekind domains (such as $\mathcal{O}_K$), so $\mathrm{Cl}(K)$ is generated by the primes. Moreover, since the norm of a prime ideal is the size of the residue field (where the quotient ring is a field since Dedekind domains are one-dimensional), the norms of prime ideals are prime powers p^n. Therefore, every prime of $\mathcal{O}_K$ is above exactly one prime $p \in \mathbb{Z}$, so we can find all the primes of $\mathrm{Cl}(K)$ by looking at the primes $p \leq M_K$ and the primes above them.

Exercise 15.2.5

Let $K = \mathbb{Q}(\sqrt{10})$; calculate $\mathrm{Cl}(K)$.

It is clear that $r_1 = 2$, so $r_2 = 0$, and by previous calculations $|D_K| = 40$, so the Minkowski bound gives $M_K = \sqrt{40}\frac{2}{4} = \sqrt{10} < 4$, so to determine $\mathrm{Cl}(K)$, we need only look at the primes above 2 and 3. Some analysis in this direction shows that $\mathrm{Cl}(K) = \mathbb{Z}/(2)$.

Though there are other ways to prove the following result, it is certainly implied by Minkowski's bound:

Corollary 15.2.6

$\mathrm{Cl}(K)$ is finite.

The key point is that each prime has finitely many primes above it, and primes in $\mathcal{O}_K$ are finite order as fractional ideals.

Don't really understand why my latter claim here is obvious.

To prove Minkowski's bound, we need another result of Minkowski's on lattices, which we will develop after a few definitions.

Definition 15.2.7: Lattices

A *lattice* in $V = \mathbb{R}^n$ is an abelian subgroup $A \subset V$ with $A \cong \mathbb{Z}^n$ and $A \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} V$, e.g, a $\mathbb{Z}$-basis for A is an $\mathbb{R}$-basis for V.

The quotient V/L of V by a lattice L is a compact manifold; one can see this most easily in the two-dimensional case by drawing the lattice, picking a fundamental domain, and identifying edges which gives the fundamental polygon for the torus. We want to compute the volume of V/L which can be defined abstractly as

$$\mathrm{vol}(V/L) = \int_{V/L} dx_1 \wedge \cdots \wedge dx_n$$

but more concretely can be concreted via a determinant. Let $b_1, \cdots, b_n \in \mathbb{R}^n$ be the standard basis, then L is given by some matrix A in the standard basis, and $\mathrm{vol}(V/L) = |\det A|$.

Definition 15.2.8: Convex Subsets

A subset $S \subseteq V = \mathbb{R}^n$ is *convex* if for all $x, y \in S$, the line $tx+(1-t)y$ for $t \in [0,1]$ is contained in S.

Theorem 15.2.9: Minkowski's Theorem

Let $L \subseteq V = \mathbb{R}^n$ be a lattice, and let $S \subseteq V$ be a bounded closed convex measurable subset of V that is symmetric about the origin (e.g, $x \in S \implies -x \in S$). If $\mathrm{vol}(S) \geq 2^n \,\mathrm{vol}(V/L)$ then S contains a nonzero element of L.

Proof: Suppose first that $\mathrm{vol}(S) > 2^n \,\mathrm{vol}(V/L)$, then the quotient map $\frac{1}{2}S \to V/L$ is not injective, where $\frac{1}{2}S \subseteq S$ since S is convex and symmetric. This map cannot be injective, since if it were, then the volume of $\frac{1}{2}S$ which is $\frac{1}{2^n}\,\mathrm{vol}(S)$ would be less than or equal to $\mathrm{vol}(V/L)$ which contradicts the assumption. This implies that there exists $P_1 \neq P_2 \in \frac{1}{2}S$ such that $P_1 - P_2 \in L$, and $-P_2 \in \frac{1}{2}S$ by symmetry, so by convexity, $\frac{1}{2}(P_1 - P_2) \in \frac{1}{2}S$, so $P_1 - P_2 \in S \cap L$, e.g, $S \cap L$ contains a nonzero element.

Professor Olsson called this Blichfield's lemma but that seems to refer to a very slightly different lemma or formulation of the lemma; in particular, Blichfield's lemma says that $\mathrm{vol}(S) > \det(L)$ implies that there exist distinct $z_1, z_2 \in S$ s.t $z_1 - z_2 \in L$. This implies Minkowski's Theorem.

Also, I think convex should imply measurable, so that hypothesis might be unnecessary.

The second case is when $\mathrm{vol}(S) = 2^n \,\mathrm{vol}(V/L)$. Then for all $\epsilon > 0$, there exists a nonzero $Q_\epsilon \in L \cap (1+\epsilon)S$ by the first part. If $\epsilon < 1$, then $Q_\epsilon \in L \cap 2S$, and $L \cap 2S$ is finite since L is discrete and $2S$ is bounded; therefore, there exists $Q \neq 0$ such that $Q = Q_\epsilon \in L \cap (1+\epsilon)S$ for all $\epsilon > 0$, therefore $Q \in L \cap S$. Equivalently, if we suppose $L \cap S$ has no nonzero points, for some ϵ, $|L \cap (1+\epsilon)S \setminus \{0\}| = 1$ so $Q_\epsilon = Q$ as above. ∎

We are now ready to prove Minkowski's bound:

Proof: Let $\sigma_1, \cdots, \sigma_{r_1}$ be the real embeddings of K, and $\eta_1, \cdots, \eta_{r_2}$ the complex embeddings (e.g picking one of each conjugate pair). Then we have an embedding $\sigma : K \hookrightarrow \mathbb{R}^n$ given by

$$x \mapsto (\sigma_1(x), \cdots, \sigma_{r_1}(x), \mathrm{Re}(\eta_1(x)), \cdots, \mathrm{Re}(\eta_{r_2}(x)), \mathrm{Im}(\eta_1(x)), \cdots, \mathrm{Im}(\eta_{r_2}(x)))$$

Note that $V = \mathbb{R}^n$ here is also given by $V = K \otimes_{\mathbb{Q}} \mathbb{R}$ by a result from commutative algebra (since we may pick a basis for K and write $K = \mathbb{Q}^n$). Then, for any $I \subset K$ a fractional ideal, $\sigma(I) \subset V$ is a lattice, which we will discuss further and justify later on. Minkowski's bound will follow by studying the volume of $V/\sigma(I)$; in particular, we will use Minkowski's Theorem to pick a representative of I in the class group that has some good properties.

There's a cool geometric argument to the first part that is basically the same proof as given, but more motivated. First, take L to $\mathbb{Z}^n$ by a linear transformation, which preserves convexity and symmetry of S (and affects the volume of S and V/L by the same factor, taking $\mathrm{vol}(V/L)$ to 1), and consider the lattice consisting of "cubes" centered at points all of whose coordinates are even; this partitions $\mathbb{R}^n$ into cubes of edge length 2. Clearly, $\mathrm{vol}(S)$ is equal to the sum of the volumes of intersections of S with each such cube, and there is a unique translate taking each such intersection to the central cube centered at the origin. The volume of each cube is 2^n, so if $\mathrm{vol}(S) > 2^n$, these translates cannot all be disjoint in the central cube, so two points $x, y \in S$ coincide in the central cube. Thus, $x - y$ is in the lattice of edge length 2, and as above, we can use the given adjectives to show that $\frac{x-y}{2}$ is in S and intersects with $\mathbb{Z}^n$.

One can also run through this argument without first moving to the standard lattice, but I've already typed it up like this.

Note first that $\sigma(\mathcal{O}_K)$ is a lattice since $\mathcal{O}_K \cong \mathbb{Z}^n$ and σ is an embedding; further note that if $L_1, \cap L_2$ are two lattices in $V = \mathbb{R}^n$, $A : V \to V$ a linear map, then $\mathrm{vol}(V/L_2) = \mathrm{vol}(V/L_1)|\det(A)|$. This follows from a basic geometric property of either determinants or of the top differential form which we used to define vol. We claim that $\mathrm{vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|D_K|}$. To see this, let $w_1, \cdots, w_n \in \mathcal{O}_K$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and write the matrix A whose i^{th} row is

$$(\sigma_1(w_i), \cdots, \sigma_{r_1}(w_i), \mathrm{Re}(\eta_1(w_i)), \cdots, \mathrm{Re}(\eta_{r_2}(w_i)), \mathrm{Im}(\eta_1(w_i)), \cdots, \mathrm{Im}(\eta_{r_2}(w_i)))$$

Then, one can see that $\sigma(\mathcal{O}_K) = A^t(\mathbb{Z}^n)$ so $\mathrm{vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K)) = \det A$ by the above. To calculate $\det A$, viewing A as an element of $M_n(\mathbb{C})$ for ease of calculation, we may perform the following operations:

1. Add i times the column $\mathrm{Im}(\eta_j(w_*))$ to the column $\mathrm{Re}(\eta_j(w_*))$
2. Multiply all columns $\mathrm{Im}(\eta_j(w_*))$ by $-2i$ (which changes the determinant by $(-2i)^{r_2}$)
3. Add each column $\eta_j(w_*)$ (created in the first step) to the column $-2i\,\mathrm{Im}(\eta_j(w_*))$ to produce a column $\overline{\eta_j(w_*)}$

This matrix is now clearly the matrix of all embeddings into $\overline{Q}$ (no longer up to conjugation), and hence its determinant is $(-2i)^{r_2}\sqrt{|D_K|}$ by the determinant squared of the matrix of embeddings formulation of the discriminant. Therefore, the claim that $\mathrm{vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K)) = |\det A| = 2^{-r_2}\sqrt{|D_K|}$ follows.

Given $I \subset K$ a fractional ideal, note that $\sigma(I)$ is a lattice with $\mathrm{vol}(V/\sigma(I)) = 2^{-r_2}\sqrt{|D_K|}N_{\mathcal{O}_K/\mathbb{Z}}(I)$. To see that $\sigma(I)$ is a lattice, note that there exists $m \in \mathbb{Z}$ such that $m\mathcal{O}_K \subseteq I \subseteq \frac{1}{m}\mathcal{O}_K$ which one can check prime by prime by decomposing I into a product of primes; therefore, $\sigma(I)$ is a lattice since it is between these two lattices (this is a sketch). For the latter point, $I = I_1 I_2^{-1}$ where $I_1, I_2 \subset \mathcal{O}_K$ are integral ideals (this is achieved by taking I_1 to be the product of primes with positive exponent, I_2^{-1} the negative exponents), and note that if $L_1 \subset L_2 \subset \mathbb{R}^n$ are full rank lattices, then $\mathrm{vol}(\mathbb{R}^n/L_1) = \mathrm{vol}(\mathbb{R}^n/L_2)[L_2 : L_1]$ by a linear algebra argument which amounts to a tiling of a fundamental domain for $\mathbb{R}^n/L_1$ by the squares of L_2. Then, since $I_1 \hookrightarrow I_1 I_2^{-1}$ (since $I_2^{-1} \supseteq \mathcal{O}_K$) and $I_1 \hookrightarrow \mathcal{O}_K$, we can calculate

$$\mathrm{vol}(\mathbb{R}^n/\sigma(I)) = \mathrm{vol}(\mathbb{R}^n/\sigma(I_1))[I_2^{-1} : \mathcal{O}_K]^{-1}$$

which by the discussion above is equal to

$$\mathrm{vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K))[\mathcal{O}_K : I_1][I_2^{-1} : \mathcal{O}_K]^{-1} = 2^{-r_2}\sqrt{|D_K|}N_{\mathcal{O}_K/\mathbb{Z}}(I)$$

Don't immediately see why $N_{\mathcal{O}_K/\mathbb{Z}}(I) = [\mathcal{O}_K : I_1][I_2^{-1} : \mathcal{O}_K]^{-1}$

Then, consider $f : \mathbb{R}^n \to \mathbb{R}$ given by

$$f(x_1, \cdots, x_n) = x_1 \cdot x_2 \cdot \cdots x_{r_1-1} \cdot x_{r_1} \cdot (x_{r_1+1}^2 + x_{r_1+1+r_2}^2) \cdots (x_{r_1+r_2}^2 + x_{r_1+2r_2}^2)$$

Note that $f(\sigma(x)) = N_{K/\mathbb{Q}}(x)$ since f takes x to the product of all its embeddings into $\overline{\mathbb{Q}} \subseteq \mathbb{C}$.

Let S be a closed bounded convex subset with positive volume and which is symmetric about the origin, and set $M = \max_{x \in S} f(x)$ which is well-defined since S is compact and therefore has compact image, where we apply the extreme value theorem. Let $c = \operatorname{vol}(\mathbb{R}^n/\sigma(I^{-1})) = 2^{-r_2}\sqrt{|D_K|}N_{\mathcal{O}_K/\mathbb{Z}}(I)^{-1}$, $v = \operatorname{vol}(S)$, $\lambda = 2\left(\frac{c}{v}\right)^{\frac{1}{n}}$, with

$$\operatorname{vol}(\lambda S) = \lambda^n \operatorname{vol}(S) = 2^n \frac{c}{v} v = 2^n \operatorname{vol}(\mathbb{R}^n/\sigma(I^{-1}))$$

By Minkowski's Theorem, there exists $b \neq 0 \in \sigma(I^{-1}) \cap \lambda S$, and let $a \in I^{-1}$ be the element with $\sigma(a) = b$. We want to calculate the volume of $\mathbb{R}^n/\sigma(aI)$ with $aI \subseteq \mathcal{O}_K$:

$$N_{\mathcal{O}_K/\mathbb{Z}}(aI) = N_{K/\mathbb{Q}}(a)N_{\mathcal{O}_K/\mathbb{Z}}(I) \leq \lambda^n M N_{\mathcal{O}_K/\mathbb{Z}}(I) = \frac{1}{v}M2^{n-r_2}\sqrt{|D_K|}$$

The rightmost term above is clearly equal to $2^{r_1+r_2}\sqrt{|D_K|}Mv^{-1}$, so it remains to find S such that this bound agrees with $\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$. This S is given by

$$S = \left\{ (x_1, \cdots, x_n) : \sum_{i=1}^{r} |x_i| + 2\sum_{j=1}^{r_2}\sqrt{x_{r_1+j}^2 + x_{r_1+r_2+j}^2} \leq n \right\}$$

which one can verify satisfies the properties to be satisfied. ■

The last part of this proof is a sketch which leaves a lot to be verified; a good resource is Marcus' Number Fields, around page 98.

Exercise 15.2.10

Calculate the class groups of $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\zeta_5)$.

In the first case, the Minkowski bound is $\sqrt{20}\frac{4}{\pi}\frac{2}{4} \approx 2.85$ so we only need to check above 2. One can show that $(2) = (2, 1+\sqrt{-5})^2$, from which it follows that $\operatorname{Cl}(\mathbb{Q}(\sqrt{-5})) = \mathbb{Z}/(2)$. For the latter case, if we accept that the discriminant of $\mathbb{Q}(\zeta_p)$ is p^{p-2} up to sign, it is clear that r_1 for $\mathbb{Q}(\zeta_5)$ is 0 (in fact $\mathbb{Q}(\zeta_5)$ is dense in $\mathbb{C}$, as is $\mathbb{Z}[\zeta_5]$), so the Minkowski bound is around 1.7 so the class group is immediately trivial.

Example 15.2.11

Let $f(x) = x^5 + ax + b$ with $a, b \in \mathbb{Z}$, α a root of f, $K = \mathbb{Q}(\alpha)/\mathbb{Q}$. First, we calculate the discriminant of $\mathbb{Z}[\alpha]$, which we know (up to sign) is equal to $N_{K/\mathbb{Q}}(f'(\alpha))$ where $f'(\alpha) = 5\alpha^4 + a$, so that

$$\alpha f'(\alpha) = 5\alpha^5 + a\alpha = 5(-a\alpha - b) + a\alpha \iff f'(\alpha) = -\frac{4a\alpha + 5b}{\alpha}$$

Then writing $f(x) = (x-\alpha_1)\cdots(x-\alpha_5)$ with $\alpha = \alpha_1$, we have that

$$N_{K/\mathbb{Q}}(4a\alpha+5b) = \prod_{i=1}^{5} 4a\alpha_i + 5b = -(4a)^5 b + 5b(4a)^4 + (5b)^5 = 4^4a^5b + 5^5b^5$$

where our calculation essentially follows by the Viète relations on f. It follows that $|N(f'(\alpha))| = \left|4^4a^5 + 5^5b^4\right|$ since $N(\alpha) = b$ again by Viète's relations.

Note that the class group $\operatorname{Cl}(K)$ and class number $|\operatorname{Cl}(K)|$ measure, in a sense, the failure of unique factorization in $\mathcal{O}_K$; in particular, if $|\operatorname{Cl}(K)| = 1$, then all fractional ideals are principal, so $\mathcal{O}_K$ is a PID and therefore a UFD. The intuition one should have, apparently, is that the larger the class number, the larger the obstruction to unique factorization.

Exercise 15.2.12: Lang, Artin

Let $f(x) = x^5 - x + 1$. Show that f is irreducible by reducing modulo 3. The discriminant as calculated above is $2869 = 19 \cdot 151$ which is square free so $\mathcal{O}_K = \mathbb{Z}[\alpha]$. One can show that f has one real root, so $r_1 = 1$, $r_2 = 2$, which gives

$$M_K = \frac{5!}{5^5} \left(\frac{4}{\pi} \right)^2 \sqrt{2869} \approx 3.3$$

Therefore, to calculate $\mathrm{Cl}(K)$, check for the ideals above 2 and 3.

That the discriminant being square-free implies that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ sounds familiar, but I don't know if we've ever stated it explicitly.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lectures 21 and 22: 16-18 November

Professor Martin Olsson Abhishek Shivkumar

Dirichlet's Unit Theorem

Let $K/\mathbb{Q}$ be a finite extension, with r_1 real embeddings and r_2 complex embeddings up to conjugation, with an embedding $\sigma : K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as we have discussed previously.

Theorem 16.1.1: Dirichlet's Unit Theorem

$\mathcal{O}_K^\times$ is isomorphic to $\mathbb{Z}^{r_1+r_2-1}$ up to torsion, where the torsion group is cyclic, given by the roots of unity in K.

Example 16.1.2

Let $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$, square-free, $D \equiv 3 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, $r_1 = 2$, and $r_2 = 0$. $a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ is a unit iff $N(a + b\sqrt{D}) = a^2 - Db^2 = \pm 1$ (since the norm of an invertible element must be invertible in $\mathbb{Z}$).

Moreover, $a^2 - Db^2 = -1$ has no solutions in the integers because this would imply that $\left(\frac{-1}{D}\right) = 1$ (where this is the Jacobi symbol for D not necessarily prime) which is not true since $D \equiv 3 \pmod 4$. It follows that

$$\mathcal{O}_K^\times = \{a + b\sqrt{D} : a^2 - Db^2 = 1\} \cong \mathbb{Z} \times \mathbb{Z}/(2)$$

where the latter isomorphism is from the theorem.

The equation $x^2 - Dy^2 = 1$ is called a *Pell equation*, and by the above, when $D \equiv 3 \pmod 4$, has infinitely many solutions. Moreover, since $\mathbb{Z}$ is free, all the solutions (up to torsion, e.g, flipping sign) are generated by a single solution.

Proof: Consider $(K \otimes_{\mathbb{Q}} \mathbb{R})^\times \xrightarrow{\sim} (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \xrightarrow{l} \mathbb{R}^{r_1+r_2}$ where the first map is just the restriction of our isomorphism to the group of units, and the second map is

$$l(x_1, \cdots, x_{r_1}, z_1, \cdots, z_{r_2}) = (\log|x_1|, \cdots \log|x_{r_1}|, 2\log|z_1|, \cdots, 2\log|z_{r_2}|)$$

This map fits into the following commutative diagram:

$$\begin{tikzcd}
(K \otimes_{\mathbb{Q}} \mathbb{R})^\times \arrow[rr, "\sim"] & & (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \arrow[r, "l"] \arrow[d, "N"] & \mathbb{R}^{r_1+r_2} \arrow[d, "\mathrm{Tr}"] \\
K^\times \arrow[u, hook, "x \mapsto x \otimes 1"] \arrow[r, "N_{K/\mathbb{Q}}"] & \mathbb{Q}^\times \arrow[r, hook] & \mathbb{R}^\times \arrow[r, "\log|\cdot|"] & \mathbb{R}
\end{tikzcd}$$

where N is given by

$$N(x_1, \cdots, x_{r_1}, z_1, \cdots, z_{r_2}) = x_1 \cdots x_{r_1} z_1 \overline{z_1} \cdots z_{r_2} \overline{z_{r_2}}$$

Note that $N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) \subseteq \{\pm 1\}$ since the norm of an invertible element must be invertible, so $\log \left| N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) \right| = 0$ so by commutativity of the right square, we must have that $l(\mathcal{O}_K^\times) \subseteq H := \ker \mathrm{Tr} \subseteq \mathbb{R}^{r_1+r_2}$ (with $H \cong \mathbb{R}^{r_1+r_2-1}$ since the subspace with trace 0 is one-dimensional). Then, we claim that $\lambda : \mathcal{O}_K^\times \to H$ (defined as the restriction of l) satisfies the following properties: $\ker \lambda$ is equal to the set of roots of unity in K, and $\Gamma := \lambda(\mathcal{O}_K^\times)$ is a full rank lattice (meaning a discrete subgroup whose basis spans the entire space).

That the norm of an invertible element is invertible uses the believable fact that $N_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}_K$ which I don't know if we have shown or stated previously.

For the first point, note that if $x^n = 1$, then for any embedding $\tau : K \hookrightarrow \mathbb{C}$, $\log|\tau(x^n)| = 0 = n \log|\tau(x)|$ so we must have that $\log|\tau(x)| = 0$, so $x \in \ker \lambda$ (since x is clearly a unit with inverse x^{n-1}). Conversely, if $x \in \ker \lambda$, then $\log|\tau(x)| = 0 \iff |\tau(x)| = 1$ for all embeddings τ as above, so $|\tau(x)^n| = 1$ for all n. It remains to show that $\tau(x)$ has finite order; however, since τ was arbitrary, we may look at the image of x under $\sigma : \mathcal{O}_K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R}$ which lies in $[-1,1]^{r_1+r_2}$. Then since $\mathcal{O}_K$ is a lattice, and since x was arbitrary, $\ker \lambda$ lies in the intersection of a lattice with a bounded region, and is therefore finite, so, in particular, $\tau(x)$ has finite order and is therefore a root of unity.

For the second point, we first want to show that $\Gamma \subseteq H$ is a lattice, e.g, it is discrete. To see this, note that for any $c > 0$, the set $S_c = \Gamma \cap \{(x_i) \in H : |x_i| \leq c\}$ is finite since we can write

$$S_c = \{x \in \mathcal{O}_K^\times : |\log|\sigma_i(x)|| \leq c \text{ for all } i\}$$

Therefore, for all $x \in S_c$, we have $e^{-c} \leq |\sigma_i(x)| \leq e^c$ for all σ_i, so S_c embeds into the intersection of $\mathcal{O}_K^\times$ with a bounded domain, and is therefore finite, since the intersection of a lattice with a bounded region is finite.

Now, we want to show that Γ is a full lattice, e.g, it spans $\mathbb{R}^{r_1+r_2}$; it suffices to show that there exists a bounded subset $M \subseteq H$ such that $H = \bigcup_{\gamma \in \Gamma}(\gamma + M)$, e.g, H is the union of the translates by Γ of some bounded fundamental domain M.

Supposing that such an M exists, let $W \subset H$ be the span of Γ (note that we are assuming strict inclusion), with $H = W \times V$ for some V nonzero and orthogonal to W, with $\pi : H \to V$. Note that $\pi(\gamma + M) = \pi(M)$ for M since $\gamma \in V$ so $\pi\left(\bigcup_{\gamma \in \Gamma}(\gamma + M)\right) = \pi(M) \subseteq V$ which is bounded since

M is bounded, and therefore is not all of V (which is unbounded). This is a contradiction since $\pi\left(\bigcup_{\gamma\in\Gamma}(\gamma+M)\right) = \pi(H) = V$ since π is surjective, from which it follows that $V = 0$ and Γ spans H.

This is a very strange proof, I'm not sure if I've transcribed it correctly.

To see that such an M exists, define $S = \{y \in (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} : N(y) = \pm 1\}$ which is the kernel of the following chain:

$$(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \xrightarrow{l} \mathbb{R}^{r_1+r_2} \xrightarrow{\mathrm{Tr}} \mathbb{R}$$

and therefore clearly surjects onto $H = \ker \mathrm{Tr}$.

Now, given the real and complex embeddings (σ_i and η_i as above), pick constants $c_1, \cdots, c_{r_1}, c_{r_1+1}, \cdots, c_{r_1+r_2} > 0$ such that their (adjusted) product C satisfies

$$C = \prod_{i=1}^{r_1} c_i \prod_{i=1}^{r_2} c_{r_1+i}^2 > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|D_K|}$$

and set $X = \{(x_j) \in (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} : |x_j| < c_j\}$ which has volume $\pi^{r_2} 2^{r_1} C$ since each complex term gives a circle and each real term gives an interval. By the assumption on C, we now have that $\mathrm{vol}(X) > 2^{r_1+r_2}\sqrt{|D_K|}$. Now, recall that $\mathrm{vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|D_K|}$ from the proof of Theorem 15.2.3, which gives us that

$$\mathrm{vol}(X) > 2^{r_1+2r_2}\,\mathrm{vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K)) = 2^n\,\mathrm{vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K))$$

from which we may apply Minkowski's Theorem (15.2.9), which tells us that there exists $a \neq 0$ in $\sigma(\mathcal{O}_K) \cap X$. Given $y = (y_i) \in S$, notice that the volume of $X \cdot y$ is equal to the volume of X, so in fact, $Xy \cap \sigma(\mathcal{O}_K)$ also contains a nonzero element by the same argument.

By the lemma below (Lemma 16.1.4), given $a \in \mathbb{Z}$, up to units, there exist finitely many $\alpha \in \mathcal{O}_K$ with $N(\alpha) = a$. Therefore, picking some fixed integer larger than C, we have finitely many elements $\alpha_1, \cdots, \alpha_N \in \mathcal{O}_K$ such that for all $a \in \mathcal{O}_K$ with $0 < \left|N_{K/\mathbb{Q}}(a)\right| \leq C$, $a = \epsilon\alpha_i$ for some i with $\epsilon \in \mathcal{O}_K^\times$. Let $T = S \cap \bigcup_{i=1}^N X\alpha_i^{-1}$. We claim that $M = l(T)$ is the region we want.

First, note that T is bounded since it is the the intersection of S with the union of a finite number of bounded regions. Moreover, $S = \bigcup_{\epsilon\in\mathcal{O}_K^\times} T\epsilon$; to see this, fix $y \in S$, with $a \neq 0 \in \mathcal{O}_K^\times$ such that $a \in Xy^{-1}$ (by previous discussions), so that

$$|N(a)| = \left|N(x)N(y^{-1})\right| = |N(x)| < C$$

Very convoluted proof. Unsure if I have all the details right.

so $\alpha_i = \epsilon a$ for some i, $\epsilon \in \mathcal{O}_K^\times$. Therefore, $y = xa^{-1} = x\epsilon\alpha_i^{-1}$; moreover, $x\alpha_i^{-1} \in S \cap X\alpha_i^{-1} \subseteq \Gamma$ so $y \in T\epsilon$, from which the claim follows since y was arbitrary in S. ■

Exercise 16.1.3

Let $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$, square-free, $D \not\equiv 1 \pmod 4$. Show that there is an action of $\mathcal{O}_K^\times$ on the set of solutions to the equation$x^2 - Dy^2 = n$ for any n. Further, show that the quotient of the solution set by this action is finite.

The first part is easy, since solutions to $x^2 - Dy^2 = n$ are just elements of $\mathbb{Z}[\sqrt{D}] = \mathcal{O}_K$ with norm n. Clearly, multiplication of $x + y\sqrt{D}$ (which is of norm n) by elements of norm 1 ($\mathcal{O}_K^\times$) will produce another norm n element, since the norm is multiplicative. For the second part, we need a lemma:

Lemma 16.1.4

Given $n \in \mathbb{Z}$, there exist finitely many $\alpha_1, \cdots, \alpha_N \in \mathcal{O}_K$ such that if $\alpha \in \mathcal{O}_K$ has norm n, then $\alpha = \epsilon\alpha_i$ for some $\epsilon \in \mathcal{O}_K^\times$. In fact, if $\alpha, \beta \in \mathcal{O}_K$ with $N(\alpha) = N(\beta) = n$, and $\alpha \cong \beta \pmod{n\mathcal{O}_K}$, then α and β differ by a unit.

Proof: Suppose $\alpha = \beta + n\gamma$ with $\gamma \in \mathcal{O}_K$. Then $\frac{\alpha}{\beta} = 1 + \frac{N(\beta)}{\beta}\gamma$ with $\frac{N(\beta)}{\beta} \in \mathcal{O}_K$ since $N(\beta)$ is just β multiplied by all of its conjugates (in the Galois case, and a similar statement is true generally via looking at embeddings into $\overline{\mathbb{Q}}$. Similarly, $\frac{\beta}{\alpha} = 1 - \frac{N(\alpha)}{\alpha}\gamma \in \mathcal{O}_K$ with $\frac{N(\alpha)}{\alpha} \in \mathcal{O}_K$ as above. It follows that, since both fractions of α and β are in $\mathcal{O}_K$, $\frac{\alpha}{\beta} \in \mathcal{O}_K^\times$, so the latter claim is proven, which implies the former claim via the unit theorem. ■

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lecture 23: 23 November

Professor Martin Olsson Abhishek Shivkumar

Pell's Equation

Let $D \in \mathbb{Z}$ be square-free and positive, with $D \not\equiv 1 \pmod 4$. In this case, $K = \mathbb{Q}(\sqrt{D})$ has $r_1 = 2$, $r_2 = 0$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, with $\mathcal{O}_K^\times \cong \mathbb{Z}/(2) \times \mathbb{Z}$ via the unit theorem, together with the observation that a field extension with only real embeddings always has precisely 2 roots of unity (± 1). Finding the units is equivalent to solving the equation

$$N(a + b\sqrt{D}) = a^2 - Db^2 = \pm 1$$

where the equation $x^2 - Dy^2 = 1$ is the classical *Pell equation*, with $x^2 - Dy^2 = n$ its natural generalization. By Lemma 16.1.4, it is useful to understand solutions to $x^2 - Dy^2 = 1$ in order to understand solutions to $x^2 - Dy^2 = n$.

Definition 17.1.1: Fundamental Unit

When $\mathcal{O}_K^\times$ has free part $\mathbb{Z}$, a *fundamental unit* is an element $\alpha \in \mathcal{O}_K^\times$ which multiplicatively generates the free part.

Set U_n to be the subset of $\mathcal{O}_K^\times$ with norm n, with U_1 in fact a subgroup. U_1 is index 1 or 2 in $\mathcal{O}_K^\times$ depending on whether the fundamental unit has norm 1 or -1, and U_1 acts multiplicatively on U_n for any n.

In the case that $D \equiv 1 \pmod 4$, which we have excluded from discussion thus far, we still have that $\mathcal{O}_K^\times \cong \mathbb{Z}/(2) \times \mathbb{Z}$ even though $\mathcal{O}_K^\times \cong \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, with the sequence $\mathbb{Z}[\sqrt{D}]^\times \hookrightarrow \mathcal{O}_K^\times \to (\mathcal{O}_K/(2))^\times$ exact.

I didn't fully follow the meaning of this discussion.

Theorem 17.1.2

Let $u = a + b\sqrt{D}$ be a unit in $\mathcal{O}_K^\times$, where $a, b \in \mathbb{Z}$, $u > 1$, and b minimal. Then u is a fundamental unit with norm one.

We proved this result in homework, so a proof is omitted here.

Theorem 17.1.3

Let $D \not\equiv 1 \pmod 4$ and squarefree, $u \in \mathcal{O}_K^\times = \mathbb{Z}[\sqrt{D}]^\times$ with norm 1. Then every solution of $x^2 - Dy^2 = n$ is of the form $u^r(a + b\sqrt{D})$ with $|a| \leq \frac{\sqrt{|n|(1+\sqrt{u})}}{2}$ and $|b| \leq \frac{\sqrt{|n|(1+\sqrt{u})}}{2\sqrt{D}}$.

Proof omitted here as well.

Example 17.1.4: due to Brian Conrad

Consider the equation $x^2 - 82y^2 = 31$; we want to find all integer solutions. We know that there exists a finite number of elements $\alpha_1, \cdots, \alpha_r \in \mathcal{O}_K$ (where $K = \mathbb{Q}(\sqrt{82})$) such that $N(\alpha) = 31$ implies that $\alpha = u^r\alpha_i$ where $u \in \mathcal{O}_K^\times$ is a fundamental unit. One can show that $u = 9 + \sqrt{82}$ which has norm -1, so $(9+\sqrt{82})^2 = 163 + 18\sqrt{82}$ has norm 1.

Theorem 17.1.3 gives us that $|a| \leq 53$ and $|b| \leq 5$, and manual search can show that $31 + 82b^2$ is not a perfect square within these bounds, so this equation has no integer solutions. $s_1 = \left(\frac{101}{3}, \frac{11}{3}\right)$ is a $\mathbb{Q}$-solution, which we will see generates infinitely many $\mathbb{Q}$-solutions. $s_2 = \left(\frac{149}{11}, \frac{15}{11}\right)$ is another $\mathbb{Q}$-solution, and since s_1 is well-defined mod p for every prime but 3, and s_2 is well-defined mod p for every prime but 11, we may conclude that our equation has solutions mod p for all primes p.

This is an important example because it shows that it is impossible to determine whether $x^2 - 82y^2 = 31$ has integer solutions via congruences alone, since the equation is solvable mod p for all primes p, but is not solvable in the integers.

We may interpret the equation $x^2 - Dy^2 = n$ geometrically by homogenizing the equation to $x^2 - Dy^2 = nz^2$ and viewing it as a projective curve over $\mathbb{C}$ (e.g a variety C in $\mathbb{P}^2_{\mathbb{C}}$). For solutions $[a, b, c]$ with $c \neq 0$, we may set $c = 1$ and we obtain the usual solutions $a^2 - Db^2 = n$ with $a, b \in \mathbb{C}$. If $c = 0$, then $[a, b, c]$ is "at ∞," and $a^2 - Db^2 = 0$, so neither coordinate can be 0, so we may set $b = 1$, so $a = \pm\sqrt{D}$. Therefore, viewing this curve projectively gives us two extraneous solutions.

However, via some algebraic geometry, we know that C is a genus 0 curve, and is therefore birational to $\mathbb{P}^1$ (in fact isomorphic to $\mathbb{P}^1$ as we will see). To see this, first recall the standard description of the isomorphism $\mathbb{P}^1_{\mathbb{C}} \cong S^2$: think of the complex plane as bisecting a sphere along a great circle, and take the stereographic projection from the "north pole" of the sphere to $\mathbb{C}$.

Then, fixing $c \in C_{\mathbb{Q}}$ (where $C_{\mathbb{Q}}$ restricts C to the rational solutions, and assuming $C_{\mathbb{Q}}$ is nonempty) the idea is that we may define a map $C_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{C}}$ via the stereographic projection taking c to ∞ (e.g the sphere is embedded with the north pole "above" c).

More explicitly, consider $H = \{[a, b, 0]\} \subset \mathbb{P}^2_{\mathbb{Q}}$ which is a line in projective space, equal to $\mathbb{Q} \cup \{\infty\}$. Using the general fact that any two distinct lines in projective space meet at precisely one point (parallel lines in projective space meet at infinity), given any $y \in C_{\mathbb{Q}}$, set L_{cy} to be the unique line between c and y, whose intersection $L_{cy} \cap H$ with H is a single point. This defines a map $C \to H$ given by $y \mapsto L_{cy} \cap H$.

Exercise 17.1.5

Write down a formula for $L_{cy} \cap H$.

Exercise 17.1.6

Find a norm one fundamental unit for $D = 79$.

A quick Python script finds $u = 80 + 9\sqrt{79}$.

Math 254A: Introduction to Algebraic Number Theory **Fall 2020**

Lectures 24 and 25: 30 November - 2 December

Professor Martin Olsson Abhishek Shivkumar

Zeta Functions

Let $K/\mathbb{Q}$ be a number field, $N = [K : \mathbb{Q}]$, with r_1 real embeddings, r_2 complex embeddings up to conjugation (σ_i and η_i, respectively), D_K the discriminant, w the number of roots of unity in K, e.g, the size of the torsion part of $\mathcal{O}_K^\times$. Recall that H is the kernel of $\mathbb{R}^{r_1+r_2} \xrightarrow{\text{Tr}} \mathbb{R}$, so $\bigwedge^{r_1+r_2-1} H \cong \mathbb{R}$, and we have a short exact sequence

$$0 \to H \to \mathbb{R}^{r_1+r_2} \to \mathbb{R} \to 0$$

Recall that the free part of $\mathcal{O}_K^\times$ embeds in H via the logarithmic embedding.

Definition 18.1.1: Regulator

The *regulator* of K as above is a number R given by the image of $1 \in \bigwedge^{r_1+r_2-1}(\mathcal{O}_K^\times)_{\text{free}} \cong \mathbb{Z}$ in $\mathbb{R}$. Alternatively, one may define the regulator as the determinant of the logarithmic map l written as a matrix.

Definition 18.1.2: Zeta Function

The *zeta function* of K is

$$\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s}$$

When $K = \mathbb{Q}$, the ideals are indexed by the natural numbers, so $\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, which is the ordinary Riemann zeta function.

Theorem 18.1.3

$\zeta_K(s)$ is an analytic function for $\text{Re}(s) > 1 - \frac{1}{N}$ except for a simple pole at $s = 1$, with residue

$$\frac{2^{r_1}(2\pi)^{r_2} R h_K}{w\sqrt{|D_K|}}$$

where h_K is the class number.

Lemma 18.1.4: Summation by Parts (Abel's Transform)

Let a_n, b_n be sequences, and set $A_n = a_1 + \cdots + a_n$, $B_n = b_1 + \cdots + b_n$. Then

$$\sum_{n=1}^{N} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_N (b_n - b_{n+1})$$

The proof is left as an exercise.

Proposition 18.1.5

Consider a series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ with $a_n \in \mathbb{C}$. If this series converges for some $s = s_0$, then it converges for all s with $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, and this convergence is uniform in any compact subset of this region.

Proof: Let $n^s = n^{s_0} n^{s-s_0}$, $P_n(s_0) = \sum_{m=1}^{n} \frac{a_m}{m^{s_0}}$. For $n > m$, we have

$$\sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} = \frac{P_n(s_0)}{n^{s-s_0}} + \sum_{k=m+1}^{n-1} P_k(s_0) \left[\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right] - \frac{P_m(s_0)}{(m+1)^{s-s_0}}$$

by the above lemma, and similarly,

$$\sum_{k=1}^{n} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} = \frac{P_n(s_0)}{n^{s-s_0}} + \sum_{k=1}^{n-1} P_k(s_0) \left[\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right]$$

whose difference is

$$\sum_{k=1}^{m} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} = \frac{P_m(s_0)}{m^{s-s_0}} + \sum_{k=1}^{m-1} P_k(s_0) \left[\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right]$$

Note that

$$\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} = (s - s_0) \int_k^{k+1} \frac{1}{x^{s-s_0+1}} dx$$

If $\mathrm{Re}(s) \geq \mathrm{Re}(s_0) + \delta$ for $\delta > 0$, then $\left| \frac{1}{x^{s-s_0+1}} \right| \leq \left| \frac{1}{x^{1+\delta}} \right|$. Since $P_k(s_0)$ converges as $k \to \infty$, we may therefore bound the right hand side above as follos:

$$\left| \sum_{k=m+1}^{n-1} P_k(s_0) \left[\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right] \right| \leq C|s - s_0| \int_{m+1}^{n} \frac{1}{x^{1+\delta}} dx \leq C|s - s_0| \left(\frac{1}{n^{\delta}} - \frac{1}{(m+1)^{\delta}} \right)$$

so if $|s - s_0|$ is bounded, then the error is bounded. ■

This is pretty much just a transcript of what was said in lecture, I have no real understanding of what this means but I assume it's just inequality bashing.

Exercise 18.1.6

Show that

$$\zeta_K(s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

This follows basically from unique prime factorization as a formal identity, a little more work is required for an analytic identity. A reference is Ahlfors, Complex Analysis.

Definition 18.1.7: Abscissa of Convergence

The *abscissa of convergence* for a given series is defined to be the smallest real number σ_0 such that $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $\mathrm{Re}(s) >$

σ_0.

Proposition 18.1.8

Assume that there exists C and $\sigma_1 \geq 0$ s.t

$$|A_n| = |a_1 + \cdots + a_n| \leq Cn^{\sigma_1}$$

for all n. Then the abscissa of convergence is $\leq \sigma_1$.

Example 18.1.9

For $\zeta(s)$ the ordinary Riemann ζ function, $a_n = 1$ for all n, so we may take $C = \sigma_1 = 1$, so the proposition implies that $\zeta(s)$ is convergent for $\mathrm{Re}(s) > 1$.

Proof:

$$P_n(s) - P_m(s) = \frac{A_n}{n^s} + \sum_{k=m+1}^{n-1} A_k \left[\frac{1}{k^s} - \frac{1}{(k+1)^s}\right] = \frac{A_n}{n^s} + \sum_{k=m+1}^{n-1} A_k s \int_k^{k+1} \frac{1}{x^{s+1}} dx$$

Let $\delta > 0$, $\mathrm{Re}(s) \geq \sigma_1 + \delta$. By assumption, we have

$$\left| A_k \int_k^{k+1} \frac{1}{x^{s+1}} dx \right| \leq C \int_k^{k+1} \frac{1}{x^{\mathrm{Re}(s) - \sigma_1 + 1}}$$

Therefore, $P_n(s) - P_m(s) \leq \frac{C}{n^s} + C\frac{|s|}{\delta}\frac{1}{(m+1)^\delta}$ from which the result follows. ■

Another inequality bash that I have no real understanding of.

Theorem 18.1.10

$\zeta(s)$ is analytic for $\mathrm{Re}(s) > 0$ except for a simple pole at $s = 1$ with residue 1.

Proof: Consider

$$\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \cdots$$

By the proposition, ζ_2 is analytic for $\mathrm{Re}(s) > 0$, since A_n is either 1 or 0. Note that $\frac{2}{2^s}\zeta(s) + \zeta_2(s) = \zeta(s)$ which implies that

$$\zeta(s) = \left(1 - \frac{1}{2^{s-1}}\right)^{-1} \zeta_2(s)$$

The above equality shows that $\zeta(s)$ is analytic for $\mathrm{Re}(s) > 0$, except at poles which can only be at the values $s = \frac{2\pi i n}{\log 2} + 1$. To whittle this down, we repeat the above argument with

$$\zeta_3(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \cdots$$

which gives a factorization

$$\zeta(s) = \left(1 - \frac{1}{3^{s-1}}\right)^{-1} \zeta_3(s)$$

which in turn implies that the poles are among $s = \frac{2\pi i n}{\log 3} + 1$, which implies that the only pole of $\zeta(s)$ is at $s = 1$.

It remains to calculate the residue of $\zeta(s)$ at $s = 1$. Suppose $s > 1$, and note that, by the left and right sums approximating $\zeta(s)$ as a series, we have

$$\frac{1}{s-1} \leq \int_1^\infty \frac{1}{x^s} dx \leq \zeta(s) \leq 1 + \frac{1}{s-1}$$

which implies that

$$1 \leq \lim_{s\to 1}(s-1)\zeta(s) \leq \lim_{s\to 1}(s-1) + 1 = 1$$

so $\lim_{s\to 1}(s-1)\zeta(s) = 1$ from which it follows that the residue of $\zeta(s)$ at $s = 1$ is 1, as claimed. ■

Theorem 18.1.11

Let a_n be a sequence of complex numbers,

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Assume there exists $C > 0$, φ, and $0 \leq \sigma_1 < 1$ such that $|A_n - n\varphi| \leq Cn^{\sigma_1}$ where $A_n = a_1 + \cdots + a_n$. Then $f(s)$ has analytic continuation to $\mathrm{Re}(s) > \sigma_1$, except for a simple pole with residue φ at $s = 1$.

Proof: Consider

$$g(s) = f(s) - \varphi\zeta(s) = \sum_{n=1}^{\infty} \frac{a_n - \varphi}{n^s}$$

By Proposition 18.1.8, $g(s)$ has abscissa of convergence $\leq \sigma_1$, and since $\varphi\zeta(s)$ has pole φ at $s = 1$, it follows that g does as well. ■

That φ is uniquely determined here hinges upon $\sigma_1 < 1$.

Define now

$$\zeta_K(s, \eta) = \sum_{I \subseteq \mathcal{O}_K, [I]=\eta} \frac{1}{N(I)^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where the first sum is over the ideals in the class determined by η, and the latter (equal) sum is where a_n is equal to the number of ideals I with norm n and class η, with corresponding A_n given by the number of ideals I with norm at most n in the class of η.

Note that ideals of the same class need not have the same norm, since principal ideals are obviously not always norm 1.

Proposition 18.1.12

$$A_n = \varphi n + O\left(n^{1-\frac{1}{N}}\right)$$

where

$$\varphi = \frac{2^{r_1}(2\pi)^{r_2} R h_K}{w\sqrt{|D_K|}}$$

We will not show this, although this result is within the scope of the tools we've developed. This shows that $|A_n - \varphi n| \leq Cn^{1-\frac{1}{N}}$ for all sufficiently large n. Note that φ above does not depend on the choice of η, which can be understood by noting that choosing a different class of ideals essentially shifts the lattice we are summing over, which does not affect asymptotic growth; this in turn implies that the statement of Theorem 18.1.3 is true if we replace $\zeta_K(s)$ with $\zeta_K(s,\eta)$ (by various of the above results), and in fact, $\zeta_K(s) = \sum_{\eta \in \mathrm{Cl}(K)} \zeta_K(s,\eta)$, from which Theorem 18.1.3 itself follows.

Exercise 18.1.13

Define $\zeta_K(s)$ for $K = \mathbb{Q}(\sqrt{D})$ with D square-free.

Recall the product expansion

$$\zeta_K(s) \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{p \text{ prime}} \prod_{\mathfrak{p} | p} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

which splits as a product into the products over the ramified primes, over the inert primes, and over the split primes. The inert primes contribute terms $(1-p^{-2s})^{-1}$, and the split primes contribute terms $(1-p^{-s})^{-2}$; we omit discussion of the ramified primes for the moment.

Consider Λ, a field of characteristic 0, and $V = \Lambda^{\{K \hookrightarrow \overline{\mathbb{Q}}\}}$ which has an action by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In our case, $V = \Lambda^2$ with $\sigma_{\pm}(\sqrt{D}) = \pm\sqrt{D}$.

Λ is generally $\mathbb{Q}_l$ when talking about Galois representations, which we are apparently talking about.

Consider $\left(\frac{D}{-}\right) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathbb{Z}/(2) = \{\pm 1\}$ given by taking Frob_p to $\left(\frac{D}{p}\right)$. Frob_p acts on V by the identity when $\left(\frac{D}{p}\right) = 1$, and by permutation when $\left(\frac{D}{p}\right) = -1$ (e.g, by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$). It follows that

I don't know what Frob_p means here. I know that $x \mapsto x^p$ is an automorphism of $\overline{\mathbb{F}_p}$, so maybe this somehow lifts to an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$? I don't really even know how our map $\left(\frac{D}{-}\right)$ is well-defined here.

$$\det\bigl(1 - t\,\mathrm{Frob}_p^{-1}|_V\bigr) = \begin{cases} (1-t)^2 & \left(\frac{D}{p}\right) = 1 \\ 1 - t^2 & \left(\frac{D}{p}\right) = -1 \end{cases}$$

Therefore, $\zeta_K(s)$ can be written as

$$\zeta_K(s) = R \prod_{p \text{ prime}} L_p(V, p^{-s})$$

where $L_p(V,t) = \det\bigl(1 - t\,\mathrm{Frob}_p^{-1}|_V\bigr)^{-1}$ and where R is the contribution from the ramified primes. The moral point of this discussion is that $\zeta_K(s)$ is controlled by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on V, e.g, a Galois representation.

Note that ζ_K only depends on $\mathcal{O}_K$, so we may generalize the situation of $\mathcal{O}_K$ over $\mathbb{Z}$ by replacing $\mathcal{O}_K$ with any finitely generated $\mathbb{Z}$-algebra A, e.g, $A = \mathbb{Z}[x_1, \cdots, x_n]/(f_1, \cdots, f_m)$, and write $\zeta(A,s) = \prod_{p \text{ prime}} \zeta_p(A,s)$, where $\zeta_p(A,s)$ is the number of maximal ideals in $A \otimes_{\mathbb{Z}} \mathbb{F}_p$ counted with weight, e.g, the number of solutions in the f_i in $\overline{\mathbb{F}}_p$.

Example 18.1.14

Let $A = \mathbb{Z}[t]$, with

$$\zeta(A, s) = \prod_{p \text{ prime}} (1 - p^{1-s})$$

This zeta function corresponds to the Galois representation $\chi_p : \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathbb{Z}_p^\times$ where χ_p is a cyclotomic character. To understand this action, choose a system of elements $x_n \in \overline{\mathbb{Q}_p}$ with $x_0 = 1$, $x_n^p = x_{n-1}$, and set $g(x_n) = x_n^{\alpha_n}$ where $\alpha_n \in (\mathbb{Z}/(p^n))^\times$, $\alpha_0 = 1$, $\alpha \in \varprojlim(\mathbb{Z}/(p^n))^\times = \mathbb{Z}_p^\times$.

No idea what this last bit meant. Fun class, though.

Part II: Math 254B

Math 254A: Introduction to Algebraic Number Theory **Spring 2021**

Lectures 1-3: 20-25 January

Professor Paul Vojta Abhishek Shivkumar

Administrative Stuff

No official textbook, mostly Professor Vojta's notes. Auxiliary references include Lang's Fundamentals of Diophantine Geometry, Neukirch's Algebraic Number Theory, Hartshorne's Algebraic Geometry, Vakil's The Rising Sea, and Lang's Introduction to Arakelov Theory. Homework will be given every week or other week. Knowledge of 254A and 256A are assumed as prerequisite.

The course will begin with a survey of the classical theory of diophantine geometry (heights and Weil functions), then Arakelov theory (application of algebraic geometry to diophantine geometry), towards the ultimate goal of proving Mordell's conjecture (Faltings' Theorem) or Roth's theorem. Lectures will probably continue into RRR week.

The table Vojta is writing on has beautiful grain, looks like curly white oak.

Conventions for the course: $\mathbb{N}$ starts at 0, all rings are commutative and have 1, and ring homomorphisms are assumed to map unity to unity.

Four Main Theorems of Diophantine Geometry

Theorem 19.2.1: Mordell-Weil

Let A be an elliptic curve or abelian variety over a number field k. Then the set of k-rational points $A(k)$ is a finitely generated abelian group.

We won't prove this result in this course, but we might use it to prove Faltings' Theorem.

The second result is Northcutt's finiteness theorem (which we do not state here), which is an end result of the development of the classical theory of heights.

The third result is Schmidt's subspace theorem, a special case of which is Roth's Theorem:

Theorem 19.2.2: Roth

Given $\alpha \in \overline{\mathbb{Q}}$, $\epsilon > 0$, $c \in \mathbb{R}_{\geq 0}$, there are finitely many rational numbers $x = \frac{p}{q} \in \mathbb{Q}$ such that $|x - \alpha| \leq \frac{c}{|q|^{2+\epsilon}}$.

The final result is Mordell's conjecture/Faltings' Theorem:

Theorem 19.2.3

Let C be a curve of genus $g > 1$ over a number field k. Then the set $C(k)$ of k-rational points on C is finite.

Roth's theorem has the following Diophantine corollary:

Corollary 19.2.4

For all $N \in \mathbb{Z}$, the equation $x^3 - 2y^3 = N$ has finitely many solutions $(x, y) \in \mathbb{Z}^2$.

Proof: There is at most one solution with $y = 0$ (N can have at most one integer cube root). If $y \neq 0$, then

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2) = N$$

Then, we may write

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| = \frac{N}{y(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2)} \leq c\frac{N}{|y|^3}$$

after which we may apply Roth's theorem, from which the result follows. ■

The idea of this proof is to look at the graph of $y = \sqrt[3]{\frac{x^3 - N}{2}}$ which has a strong asymptote given by $y = \frac{x}{\sqrt[3]{2}}$; this is the geometry of our diophantine approximation.

Definitions and Foundations

Definition 19.3.1: Varieties

Let k be an arbitrary field, then (for this course), a *variety* over k (or a k-variety) is an integral scheme, separated and of finite type over k. A morphism of k-varieties is a morphism of schemes over k.

This definition gives us a category of varieties over a given field k; the primary case of interest for us will be when k is a number field. Note that we require varieties to be integral (equivalently, reduced and irreducible), but not necessarily *geometrically* integral. There is no universal standard for this, and other authors may use other conventions.

A scheme X over a field k is geometrically integral if for every field extension $k \subseteq k'$ and every $x' \in X_{k'}$ over $x \in X$, the local ring $\mathcal{O}_{X_{k'},x'}$ is integral.

Question 19.3.2

Let P be the point $\sqrt{2}$ on $\mathbb{A}^1_{\mathbb{Q}}$. Does this make sense?

Tautologically, this is not defined, but there is well-defined point corresponding to the Galois orbit $\{\pm\sqrt{2}\}$ of $\sqrt{2}$ over $\mathbb{Q}$.

Question 19.3.3

Consider the closed subscheme $\sqrt{2}$ in $\mathbb{A}^1_{\mathbb{Q}}$. Does this make sense?

This subscheme is the above point, now with reduced induced subscheme structure, e.g, $\operatorname{Spec}\mathbb{Q}[x]/(x^2-2) = \operatorname{Spec}\mathbb{Q}(\sqrt{2}) \hookrightarrow \operatorname{Spec}\mathbb{Q}[x] = \mathbb{A}^1_{\mathbb{Q}}$.

Many commonly used terms in algebraic geometry often have multiple definitions in wide use, which can lead to confusion. For example, an elliptic curve over a field k either means a nonsingular cubic $y^2z = x^3 + axz^2 + bz^3$ in $\mathbb{P}^2_k$ (with $a, b \in k$), or the corresponding curve in $\mathbb{P}^2_{\overline{k}}$ where $\overline{k}$ is a fixed algebraic closure of k. Similarly, a projective variety over k means either a geometrically integral closed subscheme of $\mathbb{P}^n_k$, or an integral closed subscheme X of $\mathbb{P}^n_{\overline{k}}$ that can be defined by homogeneous polynomials with coefficients in k (equivalently, there exists a subscheme X_0 of $\mathbb{P}^n_k$ such that X corresponds to $X_0 \times_k \overline{k}$ under the isomorphism $\mathbb{P}^n_{\overline{k}} = \mathbb{P}^n_k \times_k \overline{k}$).

This is where lecture 2 begins, we're backtracking a bit and defining some terms we've already been using.

Definition 19.3.4: Geometric adjectives

A scheme X over a field k is *geometrically integral* if $X \times_k \overline{k}$ is integral. Likewise for *geometrically irreducible* and *geometrically reduced.*

Example 19.3.5

Let $X = V(y^2 - 2x^2) \subseteq \mathbb{A}^2_{\mathbb{Q}} = \operatorname{Spec}\mathbb{Q}[x,y]$, e.g, $X = \operatorname{Spec}\mathbb{Q}[x,y]/(y^2 - 2x^2)$ which looks like the intersection of two lines. This is an integral scheme, since $\sqrt{2} \notin \mathbb{Q}$, so $(y^2 - 2x^2)$ is a prime ideal as $y^2 - 2x^2$ is irreducible. X is not geometrically integral or geometrically irreducible as $y^2 - 2x^2$ factors as $(y - \sqrt{2}x)(y + \sqrt{2}x)$ in $k[x,y]$ for any field k containing $\sqrt{2}$.

This example partially justifies the prefix "geometric" in use here, as this alternative notion of integrality rules out pathologies introduced by the lack of algebraic closure.

Recall that a scheme is reducible if it can be written as the union of two proper closed subsets (equivalently, it contains two disjoint nonempty open subsets), and that a (nonempty) scheme is irreducible if it cannot be written in this way.

Exercise 19.3.6: Hartshorne II.3.15a

Let X be a scheme of finite type over a field k. Then, the following are equivalent:

1. $X \times_k \overline{k}$ is irreducible
2. $X \times_k k^{\text{sep}}$ is irreducible (where k^{sep} is the separable closure of k)
3. $X \times_k K$ is irreducible for all extensions K of k

We've written $X \times_k K$ where K is a field in several places above; this is nonsense if read literally, and is shorthand for $X \times_k \operatorname{Spec} K$; this holds true more generally if K is replaced with a ring.

Towards this exercise, we have the following general results:

Lemma 19.3.7

Let E/F be a field extension and let Y be a scheme over F. Then $Y_E = Y \times_F E$, and let $\pi : Y_E \to Y$ be the canonical projection. If Y is nonempty, then so is Y_E.

Proof: If Y is nonempty, then $Y \supseteq U = \operatorname{Spec} A$, and $A \neq 0$, so $A_E := A \otimes_F E$ is also nontrivial as a vector space over F (since it is the tensor product of two nonzero vector spaces), so $\pi^{-1}(U) = \operatorname{Spec} A_E$ is nonempty, from which the result follows. ■

Lemma 19.3.8

If Y is reducible, then so is Y_E.

Proof: By assumption, let U_1, U_2 be disjoint nonempty open subsets in Y, so $\pi^{-1}(U_i)$ are disjoint nonempty open subsets of Y_E, from which the result follows. ■

Lemma 19.3.9

If Y is of finite type over F and E/F is purely inseparable, then $\pi : Y_E \to Y$ induces a homeomorphism of the underlying topological spaces.

The proof of this is omitted to avoid doing too much algebraic geometry.

Lemma 19.3.10

If Y is noetherian and irreducible, then every irreducible component of Y_E dominates Y via π, e.g, the image of each component is dense in Y (or, equivalently, the generic point of Y is in the image of each irreducible component).

Proof: Let Z be an irreducible component of Y_E, ζ its generic point, $U = \operatorname{Spec} A$ an affine open neighborhood of $\pi(\zeta)$ in Y. Let

$$U_E = \pi^{-1}(U) = U \times_F E = \operatorname{Spec}(A \otimes_F E) = \operatorname{Spec} A_E$$

Since E is flat as an F-module, $A \times_F E$ is flat over A, so the Going-Down theorem of commutative algebra applies. Let $P' \subseteq A$ be the prime corresponding to the generic point η of Y, $P \subseteq A$ the prime corresponding to $\pi(\zeta)$, $Q \subseteq A_E$ the prime corresponding to ζ. Then $Q \cap A = P$ and $P' \subseteq P$, so, by Going-Down, there exists a prime Q' of A_E such that $Q' \subseteq Q$ and $Q' \cap A = P'$. Let ζ' be the point in Spec A_E corresponding to Q', then ζ' specializes to ζ and $\pi(\zeta') = \eta$. ■

There was some more discussion after this but I didn't follow it or the rest of this proof. This proof is probably incomplete. We also discussed how to apply these results to solve the Hartshorne exercise, but it was a sketch that I don't feel like going back and filling in at the moment.

The moral of this result (together with our above example demonstrating the inadequacy of the non-geometric adjectives) is that when you go to a larger field, irreducible components may become reducible, but they don't disappear, they don't change dimension (this is not explicitly shown above, but follows by looking at transcendence degrees), and different irreducible components don't coalesce. Moreover. if X is an integral scheme over a field k, E/k a normal algebraic field extension, then all irreducible components of X_E are conjugates under $\mathrm{Gal}(E/k)$. One can show that, in characteristic 0, all irreducible components of X_E are geometrically integral iff E contains the algebraic closure of k in $K(X)$.

Professor Vojta notes that he does not remember exactly why this is true.

Heights of Algebraic Numbers

The height of a number, to be defined, is essentially a measure of its complexity.

Definition 19.4.1: Rational Heights

Let $x \in \mathbb{Q}$, $x = \frac{p}{q}$ in lowest terms. Then the *multiplicative height* of x is

$$H_{\mathbb{Q}}(x) = \max(|p|, |q|)$$

and the *logarithmic height* of x is

$$h_{\mathbb{Q}}(x) = \log H_{\mathbb{Q}}(x) = \log \max(|p|, |q|)$$

Proposition 19.4.2

For all $c \in \mathbb{R}$, the set $\{x \in \mathbb{Q} : H_{\mathbb{Q}}(x) \leq c\}$ is finite (and similarly for $h_{\mathbb{Q}}(x)$).

Proof: $H_{\mathbb{Q}}(x) \leq c$ iff $-c \leq p \leq c$ and $-c \leq q \leq c$, from which the result is immediate. ■

We can now restate Roth's Theorem in a way which will suggest generalization when heights over number fields are defined:

Theorem 19.4.3: Roth

Given $\alpha \in \overline{\mathbb{Q}}$, $\epsilon > 0$, $c \in \mathbb{R}_{\geq 0}$, the set $\{x \in \mathbb{Q} : |x - \alpha| \leq \frac{c}{H_{\mathbb{Q}}(x)^{2+\epsilon}}\}$ is finite.

In Theorem 19.2.2, we had $|q|$ in place of $H_{\mathbb{Q}}(x)$; trivially, $|q| \leq H_{\mathbb{Q}}(x)$, so $\frac{c}{H_{\mathbb{Q}}(x)^{2+\epsilon}} \leq \frac{c}{|q|^{2+\epsilon}}$, so our original formulation implies this revised version. In fact, one can show the converse as well, i.e, the two formulations are equivalent.

$H_{\mathbb{Q}}$ and $h_{\mathbb{Q}}$ roughly measure the complexity of a rational number (for example, $h_{\mathbb{Q}}(x)$ is, up to linear functions, the number of decimal digits of p and q); we'd like to generalize this definition to $x \in \overline{\mathbb{Q}}$, to $\mathbb{P}^n(\overline{\mathbb{Q}})$, and more generally to $X(\overline{\mathbb{Q}})$ where X is a variety over a number field. We'd also like to generalize to the case where $\mathbb{Q}$ is replaced with $F(t)$ for F a field (and consequently $\overline{\mathbb{Q}}$ is replaced with $\overline{F(t)}$).

Definition 19.4.4

Let $M_{\mathbb{Q}} = \{\infty, 2, 3, 5, 7, 11, \cdots\}$ be the set of *places* of $\mathbb{Q}$ (equivalence classes of absolute values on $\mathbb{Q}$). For all $\nu \in M_{\mathbb{Q}}$, let

$$\|x\|_\nu = \begin{cases} |x| & \nu = \infty \\ |x|_p & \nu = p \end{cases}$$

Proposition 19.4.5: Product Formula for $\mathbb{Q}$

$$\prod_{\nu \in M_{\mathbb{Q}}} \|x\|_\nu = 1$$

for all $x \neq 0$.

Proof: Write

$$x = (-1)^l \frac{p_1^{n_1} \cdots p_r^{n_r}}{q_1^{m_1} \cdots q_s^{m_s}}$$

where the p_i and q_j are distinct primes, and l represents the sign of x. Note the obvious fact that $|x|_p = 1$ for primes not among the p_i or q_j (since $\nu_p(x) = 0$ for such primes). Furthermore, $|x|_{p_i} = p_i^{-n_i}$ and $|x|_{q_j} = q_j^{m_j}$. Then

$$\prod_{\nu \in M_{\mathbb{Q}}} \|x\|_\nu = \frac{q_1^{m_1} \cdots q_s^{m_s}}{p_1^{n_1} \cdots p_r^{n_r}} |x|_\infty = 1$$

where the last equality follows by noting that

$$|x|_\infty = \frac{p_1^{n_1} \cdots p_r^{n_r}}{q_1^{m_1} \cdots q_s^{m_s}}$$

As we noted above, this infinite product makes sense since it can have only finitely many terms which are not 1. ■

Proof taken from 254A homework.

Proposition 19.4.6

For all $x \in \mathbb{Q}$,

$$H_{\mathbb{Q}}(x) = \prod_{\nu \in M_{\mathbb{Q}}} \max(1, \|x\|_\nu)$$

Proof omitted here, not too hard to check though. No real content besides a few substitutions.

Let k be a number field, M_k the set of places of k (a place of k being an equivalence class of nontrivial absolute values on k), and recall that if $|\cdot|_1$ and $|\cdot|_2$ are equivalent, then there exists $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in k^\times$.

Math 254B: Arakelov Theory **Spring 2021**

Lectures 4 and 5: 27-29 January

Professor Paul Vojta Abhishek Shivkumar

Heights

Let k be a number field. Recalling Definition 9.1.6, let M_k^0 and M_k^∞ denote the sets of non-archimedean (or finite) and archimedean (or infinite) places of k, and let $\rho_1, \cdots, \rho_r$ be the real and $\sigma_1, \overline{\sigma_1}, \cdots, \sigma_s, \overline{\sigma_s}$ the complex embeddings $k \hookrightarrow \mathbb{C}$. M_k^∞ is in canonical bijection with the set

$$\{\rho_1, \cdots, \rho_r, \{\sigma_1, \overline{\sigma_1}\}, \cdots, \{\sigma_s, \overline{\sigma_s}\}\}$$

in such a way that if $\nu \in M_k^\infty$ corresponds to ρ or $\{\sigma, \overline{\sigma}\}$, then ν is represented by the absolute value $x \mapsto |\rho(x)|$ or $x \mapsto |\sigma(x)| = \left|\overline{\sigma(x)}\right|$.

Definition 20.1.1

A place $\nu \in M_k$ is *real* or *complex* if it is archimedean and corresponds to one of the embeddings $k \hookrightarrow \mathbb{C}$, in which case we may define $\|x\|_\nu$ as $|\rho(x)|$ or $|\sigma(x)|^2$ as above (which gives us an "absolute value" as opposed to an equivalence class). Note that $|x|_\nu$ is not technically a norm when ν is complex, as the triangle inequality fails.

The non-archimedean places of k are in canonical bijection with the set of nonzero prime ideals of $\mathcal{O}_k$ in such a way that $\nu \in M_k^0$ corresponding to $\mathfrak{p} \neq 0 \in \operatorname{Spec} \mathcal{O}_k$ is represented by the absolute value $\|\cdot\|_\nu$ on k defined by

$$\|x\|_\nu = \begin{cases} (\mathcal{O}_k : \mathfrak{p})^{-\nu_\mathfrak{p}(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

These norms have the property that, for all $x \in k$, multiplication by x multiplies the Haar measure on the additive group k_ν by $\|x\|_\nu$.

Do not know anything about Haar measures, nor what k_ν means.

Proposition 20.1.2

Let L/k be number fields, $\nu \in M_k$. Then

$$\prod_{\substack{\omega \in M_L \\ \omega | \nu}} \|x\|_\omega = \left\|N_k^L x\right\|_\nu$$

for all $x \in L$. In particular, for $x \in k$,

$$\prod_{\substack{\omega \in M_L \\ \omega | \nu}} \|x\|_\omega = \|x\|_\nu^{[L:k]}$$

Corollary 20.1.3: Product Formula

Let k be a number field, then

$$\prod_{\nu \in M_k} \|x\|_\nu = 1$$

for all $x \in k^*$.

Proof: Let $x \in k^*$, then $N_{\mathbb{Q}}^k x \in \mathbb{Q}^*$, so

$$\prod_{\nu \in M_k} \|x\|_\nu = \prod_{p \in M_{\mathbb{Q}}} \prod_{\substack{\nu \in M_k \\ \nu | p}} \|x\|_\nu = \prod_{p \in M_{\mathbb{Q}}} \left\|N_{\mathbb{Q}}^k x\right\|_p = 1$$

where the first equality is just grouping, the second equality follows by the above proposition, and the third equality follows by the product formula for $\mathbb{Q}$. ■

In particular, $N_{\mathbb{Q}}^k x$ is just a nonzero element of $\mathbb{Q}$, so the product over norms result applies. Note that $p \in M_{\mathbb{Q}}$ allows for $p = \infty$.

Definition 20.1.4: Heights on Number Fields

Let k be a number field. Then

$$H_k(x) := \prod_{\nu \in M_k} \max(1, \|x\|_\nu)$$

and

$$h_k(x) = \log H_k(x) = \sum_{\nu \in M_k} \log \max(1, \|x\|_\nu)$$

are the *multiplicative* and *logarithmic* heights of $x \in k$.

Not *a priori* clear to me that the sum in h_k converges. Probably something to do with all but finitely many terms being 0.

Proposition 20.1.5

Let L/k be number fields, $x \in k$. Then $H_L(x) = H_k(x)^{[L:k]}$, and $h_L(x) = [L:k]h_k(x)$.

This follows immediately by the product formula.

Corollary 20.1.6

Let k be a number field, $x \in \overline{k}$. Then $\frac{1}{[L:k]} h_L(x)$ is independent of a choice of $L/k(x)$.

Definition 20.1.7

Let k be a number field, $x \in \overline{k}$. Then $h_k(x) := \frac{1}{[L:k]} h_L(x)$ and $H_k(x) := H_L(x)^{1/[L:k]}$ for any number field $L/k(x)$.

It does not make sense, *a priori*, to evaluate h_k or H_k on an element of $\overline{k}$, but these definitions allow us to and are consistent by the above corollary.

Function Fields in One Variable

Let F be an arbitrary field, t an indeterminate over F, $k = F(t)$. Then k is the function field of the nonsingular projective curve $\mathbb{P}^1_F$ over F. Note that $\mathbb{P}^1_F \supseteq \mathbb{A}^1_F = \operatorname{Spec} F[t]$; this allows us to consider an analogy to number fields where k plays the role of $\mathbb{Q}$, $F[t]$ the role of $\mathbb{Z}$, and the set of closed points on $\mathbb{P}^1_F$ identify with $M_{\mathbb{Q}}$. Note that the set of closed points on $\mathbb{P}^1_F$ (denoted M_k) is equal to the set of closed points of $\mathbb{A}^1_F$ together with $\infty = \mathbb{P}^1_F \setminus \mathbb{A}^1_F$, where the closed points of $\mathbb{A}^1_F$ correspond bijectively to maximal ideals of $F[t]$.

By our analogy, we want to define $\|\cdot\|_\nu$ for $\nu \in M_k$; however, $(F[t] : \mathfrak{p})$ will be infinite if F is infinite. To remedy this, we have the following definition:

Definition 20.2.1

Let $\nu \in M_k$. Then for all $\alpha \in k$, define $\|\alpha\|_\nu$ by

$$\|\alpha\|_\nu = \begin{cases} e^{-(\deg f)\nu_{\mathfrak{p}}(\alpha)} & \text{if } \nu \text{ corresponds to } \mathfrak{p} = (f) \in \operatorname{Spec} F[t] \\ e^{-\nu_\infty(\alpha)} & \text{if } \nu \text{ corresponds to } \infty \\ 0 & \alpha = 0 \end{cases}$$

where $\nu_\infty(\alpha) = \deg b - \deg a$ where $\alpha = \frac{a}{b}$, $a, b \in F[t]$ and where $\nu_{\mathfrak{p}}(\alpha)$ is the ordinary $\mathfrak{p}$-adic valuation on k.

Proposition 20.2.2: Product Formula for $F(t)$

$$\prod_{\nu \in M_k} \|\alpha\|_\nu = 1$$

for all $\alpha \in k^\times$.

Proof: Taking logs, this is equivalent to

$$\sum_{\nu \in M_k} -\log \|\alpha\|_\nu = 0$$

for all $\alpha \in k^\times$, which we can rearrange as

$$\nu_\infty(\alpha) + \sum_{\mathfrak{p}} (\deg f)\nu_{\mathfrak{p}}(\alpha) = 0$$

This is true for all $\alpha \in F^\times$ since all terms in the sum vanish, and is true for all monic irreducible α since all terms vanish except for $v_\infty(\alpha) = -\deg f$ and $(\deg f)v_{\mathfrak{p}}(\alpha) = \deg f$ which cancel (where $\mathfrak{p} = (f)$ as above). Therefore the formula holds for all of $k^\times$ since monic irreducible α generate $k^\times$ as a group, and $\alpha \mapsto \sum_{\mathfrak{p}} -\log \|\alpha\|_{\mathfrak{p}}$ is a group homomorphism from $k^\times$ to $\mathbb{Z}$. ■

Note that for all closed points P of $\operatorname{Spec} F[t]$ (maximal ideals of $F[t]$), the residue field at P is $\kappa(P) = F[t]/\mathfrak{p} = F[t]/(f)$ where P corresponds to

$\mathfrak{p} = (f)$, so $[\kappa(P) : F] = \deg f$. Since $\kappa(\infty) = F$, the logged product formula for $F(t)$ reads

$$\sum_{P \in M_k} [\kappa(P) : F] \nu_p(\alpha) = 0$$

for all $\alpha \in k^\times$, i.e, the degree of the principle divisor (α) on $\mathbb{P}^1_F$ is 0.

Note also that we may use any real number $c > 1$ in place of e in the definition of $\|\cdot\|_\nu$; in particular, if F is a finite field $\mathbb{F}_q$, then we may use $c = q$.

Definition 20.2.3: Heights on $F(t)$

Let $k = F(t)$. For all $\alpha \in k$, let

$$H_k(\alpha) := \prod_{\nu \in M_k} \max(1, \|\alpha\|_\nu)$$

and

$$h_k(\alpha) := \log H_k(\alpha) = \sum_{\nu \in M_k} \log \max(1, \|\alpha\|_\nu)$$

If you wind through this definition together with the norms above, it turns out that $h_k\left(\frac{f(t)}{g(t)}\right) = \max(\deg f(t), \deg g(t))$ where f and g are coprime.

Proposition 20.2.4

Let $\alpha \in F(t)^\times$, with $\alpha = a/b$, and with $a, b \in F[t]$ relatively prime. Then $h_k(\alpha) = \max(\deg a, \deg b)$.

The proof is omitted.

Example 20.2.5

Let $k = F(t)$, then $h_k(t - a) = 1$ for all $a \in F$. This shows that, for $c \in \mathbb{R}$, if F is infinite, then the set $\{\alpha \in F(t) : h_k(\alpha) \leq c\}$ may be infinite (and *will* be infinite for large enough c). In general, such points can be parameterized by sets of F-points of schemes of finite type over F.

Theorem 20.2.6

Every finitely generated field extension k/F is the function field of a variety over F. The dimension of this variety equals the transcendence degree of k over F.

Proof: Let $\alpha_1, \cdots, \alpha_r$ generate k over F, e.g, $k = F(\alpha_1, \cdots, \alpha_r)$. Let $A = F[\alpha_1, \cdots, \alpha_r]$. Then $\operatorname{Spec} A$ is a variety over F which satisfies our claim (see Hartshorne I Theorem 1.8A). ■

Note that $\operatorname{Spec} A$ is an affine variety in $\mathbb{A}^r_F$, so we can also use the projective closure of $\operatorname{Spec} A$ in $\mathbb{P}^r_F$ for our variety in this result, i.e, our variety can be taken to be projective. This variety is only unique up to birational equivalence over F.

Theorem 20.2.7

If k has transcendence degree 1 over F, then the variety is a curve, and we may assume that it is a nonsingular projective curve over F. In this case, it is unique (up to isomorphism over F).

Proof is in a handout.

Definition 20.2.8: Function Fields

A *function field* over F in d variables is a finitely generated field extension of F of transcendence degree d.

Let k be a function field in one variable over F, and choose a transcendence base for k over F. It will have exactly one element, which we denote as t. Then k is an algebraic extension of $F(t)$, and k is finitely generated over $F(t)$, hence is *finite* over F.

Let C be a nonsingular projective curve over F such that $k = K(C)$ over F. Then the rational $t \in k$ gives a rational function $t : C \to \mathbb{A}^1_F$ which extends uniquely to $t : C \to \mathbb{P}^1_F$ because C is normal of dimension 1 and $\mathbb{P}^1_F$ is proper over F (using the valuative criterion of properness).

Don't understand the significance of any of this algebraic geometry. $t : C \to \mathbb{A}^1_F$ makes sense, unique extension makes sense, how are we using it?

Math 254B: Arakelov Theory **Spring 2021**

Lectures 6 and 7: 1-3 February

PROFESSOR PAUL VOJTA ABHISHEK SHIVKUMAR

Northcott's Theorem

Let F be an arbitrary field, k a function field in one variable over F, C a nonsingular projective curve over F such that $K(C) \cong k$. We have shown that we may choose $t \in k$ transcendental over F which provides a singleton transcendence base for k/F, which gives a morphism $t : \mathbb{C} \to \mathbb{P}^1_F$ over F.

Proposition 21.1.1

If L is a finite extension of k, C' a nonsingular projective curve over F s.t $K(C') \cong L$, then there exists a unique finite morphism $\varphi : C' \to C$ that induces the inclusion $k \hookrightarrow L$.

Proof: Let C' be the normalization of C in L, e.g, for all open affines $U = \operatorname{Spec} A$ in C, let B be the integral closure of A in L. This construction commutes with localization, so as U varies, the schemes $\operatorname{Spec} B$ over U glue to give a well-defined scheme C' over C. C' is normal by construction, and finite over C by finiteness of the integral closure (Theorem 6.1.2). Therefore, C' is proper over C, and hence projective over F (see Hartshorne I.6).

A scheme is normal if the local ring at each point is integrally closed in its field of fractions. Also this proof is the first time I've understood normalization.

Since $K(C') \cong L$, by uniqueness of the curve giving the field, we are done, with φ given by the normalization morphism. ■

Now let $P \in C$ be a closed point, and let $A = \mathcal{O}_{C,P}$ the corresponding local ring, B the integral closure of A in L; this is a *semilocal* ring (whose maximal ideals correspond to points of $\varphi^{-1}(P)$) and since A and B are both Dedekind domains, Theorem 6.1.6 applies:

$$\sum_{\substack{Q \in \operatorname{Spec} B \\ Q \neq 0}} e_{Q/P} f_{Q/P} = [L : k]$$

Theorem 6.1.6 assumes that L/k is separable, but according to Professor Vojta, this identity holds more generally as well.

In algebraic geometry (see Vakil 17.4.5-6 and 17.4.D-E) if $t \in A$ is a uniformizer, then

$$\deg \varphi = \sum_{Q \neq 0} \nu_Q(\varphi^* t)[\kappa(Q) : \kappa(P)] = \sum_{Q \neq 0} e_{Q/P} f_{Q/P}$$

Vakil defines $\deg \varphi$ to be the rank of $\varphi_* \mathcal{O}_{C'}$ which he proves to be locally free, and which can therefore be found by looking at the stalks at the generic points γ, γ' of C and C' respectively:

$$\deg\varphi = \dim_{\kappa(\gamma)}\kappa(\gamma') = \dim_k L = [L:k]$$

Note that for a divisor $D = \sum_i n_i P_i$ on a nonsingular projective curve C over an arbitrary field F (not necessarily algebraically closed), $\deg D$ is defined to be $\sum_i [\kappa(P_i):F]n_i$ so the product formula for $F(t)$ follows from the fact that the degree of the principal divisor (α) on $\mathbb{P}^1_F$ is zero for all $\alpha \in F(t)^\times$, since $[\kappa(P):F]$ is 1 if $P=\infty$, and $\deg f$ if P corresponds to $(f)\subseteq F[t]$. Taking logs, the product formula says that

I don't think I've seen this definition of degree before, need to see what happens if we assume that $F=\mathbb{C}$ or something.

$$0 = \sum_{P\in M_{F(t)}} -\log\|\alpha\|_P = \sum_P [\kappa(P):F]\nu_P(\alpha) = \deg(\alpha) = 0$$

Let k be a function field over F in one variable, X a nonsingular projective curve over F such that $K(X)=k$. Then M_k (relative to F) is in canonical bijection with the set of closed points of X, as follows: for each closed $P\in X$, the local ring $\mathcal{O}_{X,P}$ is a DVR, let ν_P denote its valuation (normalized so that $\nu_P(k^\times)=\mathbb{Z}$), and let $\kappa(P)$ denote the residue field. Replacing an earlier definition (when $k=F(t)$), let $M_k = \{\nu_P : P \text{ a closed point of } X\}$. Note that $P\mapsto\nu_P$ is a bijection from the closed points of X to M_k.

We then define $\|\alpha\|_\nu$ similarly, in a way that agrees with the earlier definition where $k=F(t)$:

$$\|\alpha\|_\nu = \begin{cases} e^{-[\kappa(P):F]\nu_P(\alpha)} & \alpha\in k^\times \\ 0 & \alpha = 0\end{cases}$$

This definition is more general in that it does not require choosing a transcendence base in t. As before, note that $M_k^\infty=\emptyset$ and $M_k^0 = M_k$, as there are no archimedean places.

Not immediately clear to me why there are no archimedean places.

Proposition 21.1.2

Let L/k be finite extensions of $F(t)$, and let $\varphi: X'\to X$ be the corresponding morphism of nonsingular projective curves over F. Then for all $\nu\in M_k$, all $\alpha\in L$,

$$\prod_{\substack{\omega\in M_L\\ \omega|\nu}} \|\alpha\|_\omega = \left\|N_k^L\alpha\right\|_\nu$$

where $\omega|\nu$ means the closed points $Q\in X'$ and $P\in X$ corresponding to ω and ν respectively are related by $\varphi(Q)=P$.

Proof:

$$\left\|N_k^L\alpha\right\|_\nu = \prod_{\substack{\omega\in M_L\\ \omega|\nu}} \left\|N_{k_\nu}^{L_\omega}\alpha\right\|_\nu = \prod_{\substack{\omega\in M_L\\ \omega|\nu}} \left\|N_{k_\nu}^{L_\omega}\alpha\right\|_\omega^{1/[L_\omega:k_\nu]} = \prod_{\omega|\nu}\|\alpha\|_\omega$$

where the various intermediate equalities are results from Bourbaki, Neukirch, and Neukirch II. ■

This gives the product formula for function fields in one variable over F:

Corollary 21.1.3

Let k be as above, then $\prod_{\nu \in M_k} \|\alpha\|_\nu = 1$ for all $\alpha \in k^\times$.

The proof is essentially the same as the previous product formula proofs.

Definition 21.1.4: Heights on Function Fields

Let k be a function field in one variable over a field. Then

$$H_k(\alpha) := \prod_{\nu \in M_k} \max(1, \|\alpha\|_\nu)$$

and

$$h_k = \log H_k(\alpha) := \sum_{\nu \in M_k} \log \max(1, \|\alpha\|_\nu)$$

As before, if L/k is a finite extension (with compatible M_L and M_k), then $h_L(\alpha) = [L : k] h_k(\alpha)$, so we may define $h_k(\alpha) = \frac{1}{[L:k]} h_L(\alpha)$ for all $\alpha \in \overline{k}$, where L is any finite extension of k containing α.

Note that most authors use the convention that $h_k(\alpha)$ and $H_k(\alpha)$ are only defined for $\alpha \in k$ and call them *relative heights*, with *absolute heights* being given by $h : \overline{\mathbb{Q}} \to \mathbb{R}$ and $H : \overline{\mathbb{Q}} \to \mathbb{R}$ (in the number field case) to be what we refer to as $h_{\mathbb{Q}}$ and $H_{\mathbb{Q}}$ respectively. We always use absolute heights, where the subscript indicates normalizations. In the function field case, there's no canonical "bottom field," since $k \supseteq F(t) \supseteq F(t^2) \supseteq \cdots$.

Theorem 21.1.5: Northcott

Let k be a number field, $C \in \mathbb{R}$. Then the set $\{\alpha \in k : H_k(\alpha) \leq C\}$ is finite, and, more generally, for all $d > 0$, the set

$$\{\alpha \in \overline{k} : [k(\alpha) : k] \leq d \text{ and } H_k(\alpha) \leq C\}$$

is finite.

I think the first half of this is obvious over $\mathbb{Q}$, interesting that it holds more generally.

Remark 21.1.6

In diophantine geometry, you often want to prove finiteness of k-rational points, and this is often done by bounding the height.

Definition 21.1.7

Let k be a field, and $\|\cdot\|$ a norm on k. Let $f(t) = a_n t^n + \cdots + a_0$ be a polynomial in $k[t]$ with $n \geq 0$; then, we define $\|f\| = \max(\|a_0\|, \cdots, \|a_n\|)$.

Definition 21.1.8

Let k be a number field and let $f \in k[t]$ with $\deg f > 0$. Then $H_k(f) = \prod_{\nu \in M_k} \|f\|_\nu$.

Note that by the product formula, $H_k(cf) = H_k(f)$ for all $c \in k^\times$. Moreover, $H_k(\alpha) = H_k(t-\alpha)$ where the left height is that of a number, the right height that of a polynomial.

Definition 21.1.9

Let k be a number field, $\alpha \in \overline{k}$, then we define $H_{\text{ancient},k}(\alpha) = H_k(f)$ where f is the monic irreducible polynomial of α over k.

Lemma 21.1.10

Let L/k be number fields. Then $H_L(f) = H_k(f)^{[L:k]}$ for all nonconstant $f \in k[t]$. Moreover, let $\sigma : L \to L$ be a k-automorphism of L. Then $H_L(\sigma(\alpha)) = H_L(\alpha)$ for all $\alpha \in L$.

The proof is left as an exercise. The second statement is easier in the Galois case, but the Galois hypothesis is unnecessary.

Definition 21.1.11

Let k be a number field or function field, and let $\nu \in M_k$. Then N_ν is defined to be 0 if ν is non-archimedean, 1 if ν is real, and 2 if ν is complex.

Note that $\sum_{\nu \in M_k} N_\nu$ is $[k : \mathbb{Q}]$ when k is a number field (via the $n = r_1 + 2r_2$ identity) and 0 when k is a function field (since the places are all non-archimedean). Further note that for all $\alpha_1, \cdots, \alpha_n \in k$,

$$\|\alpha_1 + \cdots + \alpha_n\|_\nu \leq n^{N_\nu} \max(\|\alpha_1\|_\nu, \cdots, \|\alpha_n\|_\nu)$$

This inequality follows by the non-archimedean property (in the non-archimedean case) together with the triangle inequality (in the archimedean case). This inequality is not sharp in the archimedean case, in fact, we have

$$\|\alpha_1 + \cdots + \alpha_n\|_\nu \leq n \max(\|\alpha_1\|_\nu, \cdots, \|\alpha_n\|_\nu)$$

by the triangle inequality.

Lemma 21.1.12

Let k be a number field, $\alpha_1, \cdots, \alpha_n \in k$, and let $f(t) = \prod_{i=1}^n (t - \alpha_i) \in k[t]$. Then, given $\nu \in M_k$,

$$2^{-nN_\nu} \prod_{i=1}^n \max(1, \|\alpha_i\|_\nu) \leq \|f\|_\nu \leq 2^{nN_\nu} \prod_{i=1}^n \max(1, \|\alpha_i\|_\nu)$$

The constants $2^{\pm nN_\nu}$ come from the archimedean property of $|\cdot|$ on $\mathbb{C}$, and they go away at non-archimedean places.

Proof: If ν is non-archimedean, then the given inequalities follow from the fact that

$$\|f\|_\nu = \prod_{i=1}^n \max(1, \|\alpha_i\|_\nu) = \prod_{i=1}^n \|t - \alpha_i\|_\nu$$

which in turn follows from Gauss' lemma from commutative algebra. If ν is archimedean, it will suffice to prove the given inequalities with k replaced by $\mathbb{C}$ (since all such places are essentially the ordinary complex norm) and $\|\cdot\|_\nu$ replaced by $|\cdot|$. We will only prove the second inequality (the first

Recall that Gauss' lemma states that $\operatorname{cont}(fg) \subseteq \operatorname{cont}(f)\operatorname{cont}(g) \subseteq \sqrt{\operatorname{cont}(fg)}$, where $\operatorname{cont}(f)$ is the ideal generated by the coefficients of f.

inequality is a lot harder, and we won't be using it as much), but this is easy since for all $d = 0, 1, \cdots, n$ the coefficient of t^{n-d} in f is (up to sign) the elementary symmetric polynomial of degree d in the α_i, which has $\binom{n}{d} \leq 2^n$ terms and all coefficients 1, from which the results follow. ■

Proposition 21.1.13

Let k be a number field, $\alpha \in \overline{k}$. Then

$$2^{-[k(\alpha):\mathbb{Q}]} H_{k(\alpha)}(\alpha) \leq H_{\text{ancient},k}(\alpha) \leq 2^{[k(\alpha):\mathbb{Q}]} H_{k(\alpha)}(\alpha)$$

Proof: Let L be a finite normal extension field of k that contains α, $\alpha_1, \cdots, \alpha_n$ the conjugates of α over k in L, and $f(t) = \prod_{i=1}^n (t - \alpha_i)$. Then f is the irreducible polynomial for α over k, $n = [k(\alpha) : k]$. Applying the previous lemma by taking the product of the inequalities over all $\omega \in M_L$, we obtain

$$\left(\prod_{\omega \in M_L} 2^{N_\omega} \right)^{-n} \prod_{i=1}^n H_L(\alpha_i) \leq H_L(f) \leq \left(\prod_{\omega \in M_L} 2^{N_\omega} \right)^{n} \prod_{i=1}^n H_L(\alpha_i)$$

Note that

$$H_L(f) = H_k(f)^{[L:k]} = H_{\text{ancient},k}(\alpha)^{[L:k]}$$

and $\prod_{i=1}^n H_L(\alpha_i) = H_L(\alpha)^n$, and that $\prod_{\omega \in M_L} 2^{N_\omega} = 2^{[L:\mathbb{Q}]}$. Substituting these into the above inequalities and taking the $[L : k]^{\text{th}}$ root of all parts gives

$$2^{-[k:\mathbb{Q}]n} H_{k(\alpha)}(\alpha) \leq H_{\text{ancient},k}(\alpha) \leq 2^{[k:\mathbb{Q}]n} H_{k(\alpha)}(\alpha)$$

from which the result is immediate, since $[k(\alpha) : k] = n$. ■

Math 254B: Arakelov Theory **Spring 2021**

Lectures 8-10: 5-10 February

Professor Paul Vojta Abhishek Shivkumar

Proof of Northcott's Theorem

Recall Proposition 21.1.13; this result has an analogue over function fields in one variable (as usual), although in that case, the proposition says that $H_{\text{ancient},k}(\alpha) = H_{k(\alpha)}(\alpha)$ and can be fully proved (we only proved one of the two inequalities in Lemma 21.1.12) without much difficulty. With these preliminaries, we are ready to prove Theorem 21.1.5:

I don't fully understand the reduction to $k = \mathbb{Q}$. It seems that $\overline{k}$ can only ever be $\overline{\mathbb{Q}}$, in which case this all makes sense, but then I don't understand why we write $\overline{k}$ at all.

Proof: It clearly suffices to show that

$$\{\alpha \in \overline{k} : [k(\alpha) : k] \leq d \text{ and } H_k(\alpha) \leq C\}$$

is finite for all $d > 0$, since finiteness of $\{\alpha \in k : H_k(\alpha) \leq C\}$ is clearly a special case of this. We may assume that $C \geq 1$, since otherwise, our set will be empty. Replacing k with $\mathbb{Q}$, d with $[k : \mathbb{Q}]d$, and C with $C^{[k:\mathbb{Q}]}$, we may assume that $k = \mathbb{Q}$. By Proposition 21.1.13, it will suffice to show that the set

$$\Sigma_n := \{\alpha \in \overline{\mathbb{Q}} : [\mathbb{Q}(\alpha) : \mathbb{Q}] = n \text{ and } H_{\text{ancient},\mathbb{Q}}(\alpha) \leq 2^n C\}$$

is finite for all $n = 1, \cdots, d$. These sets are finite since, for all $\alpha \in \Sigma_n$, clearing denominators in the irreducible polynomial for α over $\mathbb{Q}$ gives a polynomial of degree n in $\mathbb{Z}[t]$ whose coefficients (assumed collectively relatively prime) are bounded in absolute value by $2^n C$. Only finitely many polynomials satisfy these constraints, and each polynomial can contribute at most finitely many elements of Σ_n. ■

Heights on $\mathbb{P}^n$

For the rest of this chapter, function fields are assumed to be function fields in one variable over a field F.

Definition 22.2.1: Heights on Projective Spaces

Let k be a number field or function field, $n \in \mathbb{N}$, and let $P \in \mathbb{P}^n(k)$.

Let $[x_0 : \cdots : x_n]$ be homogeneous coordinates for P, then

$$H_k(P) := \prod_{\nu \in M_k} \max(\|x_0\|_\nu, \cdots, \|x_n\|_\nu)$$

and

$$h_k(P) := \log H_k(P) = \sum_{\nu \in M_k} \log \max(\|x_0\|_\nu, \cdots, \|x_n\|_\nu)$$

This is well-defined since

$$\prod_{\nu \in M_k} \max(\|\alpha x_0\|_\nu, \cdots, \|\alpha x_n\|_\nu) = \prod_{\nu \in M_k} \max(\|x_0\|_\nu, \cdots, \|x_n\|_\nu)$$

for all $\alpha \in k^\times$ by the product formula (since $\|\alpha\beta\|_\nu = \|\alpha\|_\nu \|\beta\|_\nu$). As before, if L is a finite extension of k, then $H_L(P) = H_k(P)^{[L:k]}$ and $h_L(P) = [L:k]h_k(P)$, so we may again define $H_k(P) = H_L(P)^{1/[L:k]}$ for all $P \in \mathbb{P}^n(\overline{k})$ and any field L finite over k for which $P \in \mathbb{P}^n(L)$.

If you identify $\alpha \in k$ or $\alpha \in \overline{k}$ with $\mathbb{A}^1(k)$ or $\mathbb{A}^1(\overline{k})$, with $\mathbb{A}^1$ itself identified with an open subset of $\mathbb{P}^1$ as usual, then $\alpha \mapsto [1 : \alpha]$ gives bijections $i : k \to \mathbb{P}^1(k) \setminus \{\infty\}$ and $\overline{i} : \overline{k} \to \mathbb{P}^1(\overline{k}) \setminus \{\infty\}$ for which $h_k(\alpha) = h_k(i(\alpha))$ and similarly for $\overline{k}$.

Lemma 22.2.2

Let $P \in \mathbb{P}^n(\overline{k})$ with homogeneous coordinates $[x_0 : \cdots : x_n]$. If $x_0 \neq 0$, then $H_k\left(\frac{x_i}{x_0}\right) \leq H_k(P)$ for all $i = 1, \cdots, n$.

Proof: Choose a field L finite over k, such that $x_i \in L$ for all i. Then, by the above,

$$H_L\left(\frac{x_i}{x_0}\right) = \prod_{\omega \in M_L} \max(\|x_0\|_\omega, \|x_i\|_\omega) \leq \prod_{\omega \in M_L} \max(\|x_0\|_\omega, \cdots, \|x_n\|_\omega) = H_L(P)$$

■

Theorem 22.2.3: Northcott for $\mathbb{P}^n(k)$

Let k be a number field, $n \in \mathbb{N}$, $d \in \mathbb{Z}_{>0}$, and $C \in \mathbb{R}$. Then $\{P \in \mathbb{P}^n(\overline{k}) : [k(P) : k] \leq d \text{ and } H_k(P) \leq C\}$ is a finite set, where $k(P)$ is the residue field at $P \in \mathbb{P}^n(\overline{k})$.

Proof: By permuting coordinates, it suffices to show that

$$\{P \in \mathbb{P}^n(\overline{k}) \cap D_+(x_0) : [k(P) : k] \leq d \text{ and } H_k(P) \leq C\}$$

is a finite set, where $D_+(x_0) = \{\mathfrak{p} \in \mathbb{P}^n(\overline{k}) : x_0 \notin \mathfrak{p}\}$. This follows from the above lemma together with the original Northcott theorem. ■

Confused about the interspersed usage of $\mathbb{P}^n_k$ and $\mathbb{P}^n(k)$, unsure if that's actually a meaningful difference or not. Maybe one is a scheme?

Note that for all k, $n \in \mathbb{Z}_{>0}$, the height function $h_k : \mathbb{P}^n(\overline{k}) \to \mathbb{R}$ is *not* invariant under $\operatorname{Aut}(\mathbb{P}^n_k)$, since h_k is not constant but $\operatorname{Aut}(\mathbb{P}^n_k)$ acts transitively on $\mathbb{P}^n(k)$. We shall see, however, that for all $\varphi \in \operatorname{Aut}(\mathbb{P}^n_k)$, $h_k(\varphi(P)) = h_k(P) + O(1)$ as P varies over $\mathbb{P}^n(\overline{k})$, where the constant in $O(1)$ depends on φ and k but not P.

Definition 22.2.4: M_k-constants

Fix a number field or function field k. Then an M_k-constant γ is a function $\nu \mapsto \gamma_\nu$ from M_k to $\mathbb{R}$ such that $\gamma_\nu = 0$ for all but finitely many $\nu \in M_k$.

These form a group under addition, and in fact an $\mathbb{R}$-vector space. We say that $\gamma \geq 0$ if $\gamma_\nu \geq 0$ for all ν, and $\gamma \geq \gamma'$ if $\gamma - \gamma' \geq 0$. Also let $|\gamma|$ denote $\sum_{\nu \in M_k} \gamma_\nu$. Finally, for all finite extensions L of k, all $\omega \in M_L$, and all M_k-constants γ, we write $\gamma_\omega = [L_\omega : k_\nu]\gamma_\nu$ where $\omega \in M_L$ lies over $\nu \in M_k$, and L_ω and k_ν are the completions. Then, as with heights, $|\gamma| = \frac{1}{[L:k]} \sum_{\omega \in M_L} \gamma_\omega$ and $\log \|\alpha\|_\omega \leq \gamma_\omega \iff \log \|\alpha_\nu\| \leq \gamma_\nu$ for all ω, ν as above, all $\alpha \in k_\nu$.

We have already defined one M_k-constant: N_ν which is 0 for non-archimedean ν, 1 for ν real, and 2 for ν complex is an M_k-constant, with $|N| = \sum_{\nu \in M_k} N_\nu = [k : \mathbb{Q}]$ in the case of number fields, and 0 in the case of function fields. As above, $N_\omega = [L_\omega : k_\nu] N_\nu$ with ω over ν.

Example 22.2.5

Let $a_0, \cdots, a_n \in k$, not all zero. Then

$$\gamma_\nu = \log \max(\|a_0\|_\nu, \cdots, \|a_n\|_\nu)$$

defines an M_k-constant γ.

Not sure I really understand the significance of M_k-constants.

Note that if L/k is a finite extension, and $\omega \in M_L$ lies over $\nu \in M_k$, then $\gamma_\omega = \log \max(\|a_0\|_\omega, \cdots, \|a_n\|_\omega)$ (via $\|a\|_\omega = \|a\|_\nu^{[L_\omega : k_\nu]}$).

Lemma 22.2.6

Let $n \in \mathbb{N}$, $\varphi \in \operatorname{Aut}(\mathbb{P}^n_k)$. Then

$$h_k(\varphi(P)) = h_k(P) + O(1)$$

for all $P \in \mathbb{P}^n(\overline{k})$, where the implied constant in $O(1)$ depends only on k and φ, but not P.

Proof: By Hartshorne II 7.1.1, the map $\mathrm{GL}_{n+1}(k) \to \operatorname{Aut}(\mathbb{P}^n_k)$ given by

$$M \mapsto \left(\begin{pmatrix} x_0 \\ \ddots \\ x_n \end{pmatrix} \mapsto M \begin{pmatrix} x_0 \\ \ddots \\ x_n \end{pmatrix} \right)$$

induces an isomorphism $\mathrm{PGL}_{n+1}(k) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{P}^n_k)$. Let $M \in \mathrm{GL}_{n+1}(k)$ be a matrix corresponding to φ, and write $M = (a_{ij})$. Then $\varphi([x_0 : \cdots : x_n]) = [y_0 : \cdots : y_n]$, where $y_i = \sum_j a_{ij} x_j$. For all L finite over k, $\omega \in M_L$, we have

$$\max(\|y_0\|_\omega, \cdots, \|y_n\|_\omega) \leq (n+1)^{N_\omega} \max(\|a_{ij}\|_\omega) \max(\|x_0\|_\omega, \cdots, \|x_n\|_\omega)$$

for all $[x_0 : \cdots : x_n] \in \mathbb{P}^n(L)$.

This covers all points in $\mathbb{P}^n(\overline{k})$.

Let γ be the M_k-constant $\gamma_\nu = \log \max \|a_{ij}\|_\nu$ for $0 \leq i, j \leq n$. Then for all L, ω, and all $[x_0 : \cdots : x_n]$ as above, we have

$$\log \max(\|y_0\|_\omega, \cdots, \|y_n\|_\omega) \leq \log \max(\|x_0\|_\omega, \cdots, \|x_n\|_\omega) + \gamma_\omega + N_\omega \log(n+1)$$

Therefore, summing over all $\omega \in M_L$, and dividing by $[L : k]$, we have

$$h_k(\varphi(P)) \leq h_k(P) + |\gamma| + |N| \log(n+1)$$

Let γ' be the M_k-constant defined similarly to γ, but with M^{-1} in place of M. Then, we similarly obtain

$$h_k(P) \leq h_k(\varphi(P)) + |\gamma'| + |N| \log(n+1)$$

from which the result follows. ■

The inequality with the term $N_\omega \log(n+1)$ is obtained by the following chain:

$$\|y_i\|_\omega = \left\| \sum_j a_{ij} x_j \right\|_\omega \leq (n+1)^{N_\omega} \max(\|a_{ij} x_j\|_\omega)$$

The right hand side of the above is in turn bounded above by

$$(n+1)^{N_\omega} \max(\|a_{ij}\|_\omega) \max(\|x_i\|_\omega)$$

and $\max(\|a_{ij}\|_\omega) \leq e^{\gamma_\omega}$ from which the result follows.

Lemma 22.2.7

Let $n \in \mathbb{Z}_{>0}$, V and W linear subspaces of $\mathbb{P}^n_k$ with $V \cap W = \emptyset$, and $\dim V + \dim W = n - 1$. Let $\varphi : \mathbb{P}^n_k \setminus V \to W$ be the linear projection

$$P \mapsto \mathrm{Span}(P, V) \cap V$$

Let X be a closed subscheme of $\mathbb{P}^n_k$ with $X \cap V = \emptyset$. Then

$$h_k(\varphi(P)) = h_k(P) + O(1)$$

for all $P \in X(\overline{k})$, with the implied constant depending only on k, X, and φ.

Proof: By the previous lemma, we may take an automorphism of $\mathbb{P}^n_k$ and thereby assume that V is given by $x_0 = \cdots = x_m = 0$, and W by $x_{m+1} = \cdots = x_n = 0$ where $0 \leq m < n$. In this basis, φ is given by

$$[x_0 : \cdots : x_n] \mapsto [x_0 : \cdots : x_m : 0 : \cdots : 0] \in W$$

Therefore, the $\leq$ inequality is easy since

$$\max(\|x_0\|_\omega, \cdots, \|x_m\|_\omega) \leq \max(\|x_0\|_\omega, \cdots, \|x_n\|_\omega)$$

as $m < n$.

To prove the other inequality, we will start with the special case $m = n-1$, so φ is the projection from the point $Q = [0 : \cdots : 0 : 1]$. We claim there is an M_k-constant γ with the following property: for all finite extensions L/k, all $P = [x_0 : \cdots : x_n] \in X(L)$, all $\omega \in M_L$,

$$\|x_n\|_\omega \leq e^{\gamma_\omega} \max(\|x_0\|_\omega, \cdots, \|x_{n-1}\|_\omega)$$

To see this, let $\nu \in M_k^\infty$ (in the case of number fields), and choose $\sigma : k \hookrightarrow \mathbb{C}$ corresponding to ν. Let L be a finite extension of k, $\omega \in M_L$ lying over ν. Then $\omega \in M_L^\infty$, and σ extends to $\tau : L \hookrightarrow \mathbb{C}$ corresponding to ω. We get maps $\operatorname{Spec}\mathbb{C} \to \operatorname{Spec} L \to \operatorname{Spec} k$ corresponding to the chain of embeddings, and may define $X_\mathbb{C} = X \times_k \mathbb{C}$; then $X_\mathbb{C}$ is a closed subscheme of $\mathbb{P}^n_\mathbb{C}$ not containing $Q_\mathbb{C} := [0 : \cdots : 0 : 1] \in \mathbb{P}^n(\mathbb{C})$. Since $X(\mathbb{C})$ is a closed subset of $\mathbb{P}^n(\mathbb{C})$ in the classical topology, it is compact, so the continuous function

$$[x_0 : \cdots : x_n] \mapsto \frac{|x_n|}{\max(|x_0|, \cdots, |x_{n-1}|)}$$

on $X_\mathbb{C}(\mathbb{C})$ has a maximum M (by the extreme value theorem). Then the desired inequality holds with $\gamma_\nu = N_\nu \log M$, and $\gamma_\omega = N_\omega \log M$ for all L and $\omega \in M_L^\infty$, ω lying over ν.

In the other case, $\nu \in M_k^0$, $\mathbb{P}^n(k_\nu)$ is compact if k is a global field, but is not compact if k is a function field over an infinite field, and in any case, $\mathbb{P}^n(\overline{k_\nu})$ is never compact. However, since $Q \notin X$, there exists a homogeneous polynomial $f \in k[t_0, \cdots, t_n]$ which vanishes at all points of X but not at Q. Write

$$f(t) = \sum_{|\underline{i}=d|} a_{\underline{i}} t^{\underline{i}}$$

in multi-index notation, where $d = \deg f$. Since $f(Q) \neq 0$, i.e, $Q \notin D_+((f))$, $a_{(0,\cdots,o,d)} \neq 0$ since this is the coefficient of t_n^d and must be nonzero for $f(Q)$ to be nonzero. We may assume $a_{(0,\cdots,o,d)} = 1$. Let L/k, $P \in X(L)$, $\omega \in M_L$ above ν be as in the claim, and let $\omega \in M_L$. If $P = [x_0 : \cdots : x_n]$, and $x_n = 0$, then

$$\|x_n\|_\omega \leq e^{\gamma_\omega} \max(\|x_0\|_\omega, \cdots, \|x_{n-1}\|_\omega)$$

holds trivially, so we may assume $x_n \neq 0$, and therefore that $x_n = 1$. Since $f(P) = 0$,

$$\sum_{\substack{|\underline{i}=d| \\ \underline{i} \neq (0,\cdots,d)}} a_{\underline{i}} x^{\underline{i}} = -a_{(0,\cdots,o,d)} x_n^d = -1$$

Therefore, since ω is non-archimedean, some term in the sum has $\|\cdot\|_\omega \geq 1$. Therefore, there exists a multi-index $\underline{i}$ such that $|\underline{i}| = d$, $\underline{i} \neq (0, \cdots, 0, d)$, and $\|a_{\underline{i}} x^{\underline{i}}\|_\omega \geq 1$. This gives

$$\|a_{\underline{i}}\|_\omega \max(\|x_0\|_\omega, \cdots, \|x_{n-1}\|_\omega)^{i_0 + \cdots + i_{n-1}} \geq \|a_{\underline{i}} x^{\underline{i}}\|_\omega \geq 1$$

This section of the proof is completely meaningless to me, just some weird inequality bash. This proof is overly long as written here, and poorly structured; the claim we use in the middle should probably be proved separately earlier as a proposition.

so

$$\log \max(\|x_0\|_\omega, \cdots, \|x_{n-1}\|_\omega) + \max_{\substack{|\underline{i}|=d, a_{\underline{i}} \neq 0 \\ \underline{i} \neq (0,\cdots,0,d)}} \frac{\log \|a_{\underline{i}}\|_\omega}{i_0 + \cdots + i_{n-1}} \geq 0$$

Therefore, letting

$$\gamma_\nu = \max_{\substack{|\underline{i}|=d, a_{\underline{i}}\neq 0 \\ \underline{i}\neq(0,\cdots,0,d)}} \frac{\log \|a_{\underline{i}}\|_\nu}{i_0+\cdots+i_{n-1}}$$

the desired inequality holds for all $\omega|\nu$, and $\nu \mapsto \gamma_\nu$ is clearly an M_k-constant, since the assignment is 0 for almost all $\nu \in M_k$, from which the claim follows.

With the claim in hand, let $\gamma' = \max(\gamma, 0)$ taken coordinate wise at each $\nu \in M_k$, then the claim holds with the key inequality above replaced by

$$\max(\|x_0\|_\omega, \cdots, \|x_n\|_\omega) \leq e^{\gamma'_\omega} \max(\|x_0\|_\omega, \cdots, \|x_{n-1}\|_\omega)$$

Taking logs, summing over $\omega \in M_L$, and dividing by $[L:k]$, we obtain

$$h_k(P) \leq h_k(\varphi(P)) + |\gamma'|$$

for all L finite over k, all $P \in X(L)$.

This settles the special case $m = n-1$. For the general case, we may induct on $n-m$; assume $n-m > 1$, and by induction, assume the case of $n-m-1$. We have the following diagram:

$$\begin{tikzcd}
& \mathbb{P}^n \setminus \{Q\} \arrow[r, "\varphi_0"] & W_0 & \\
X \arrow[ur, hook] \arrow[r, hook] \arrow[rrr, bend right, "\varphi"'] & \mathbb{P}^n \setminus V \arrow[u] \arrow[r, "\varphi_0|_{\mathbb{P}^n \setminus V}"] & W_0 \setminus V' \arrow[u, hook] \arrow[r, "\varphi'"] & W
\end{tikzcd}$$

The maps φ_0 and φ' respectively act by

$$[x_0 : \cdots : x_n] \mapsto [x_0 : \cdots : x_{n-1} : 0] \mapsto [x_0 : \cdots : x_m : 0 : \cdots : 0]$$

Here, W_0 is the set given by $x_n = 0$, $V' = V \cap W_0 = \varphi(V \setminus \{Q\})$, so $\varphi_0^{-1}(V') = \{x_0 = \cdots = x_m = 0\} \setminus \{Q\} = V \setminus \{Q\}$. And, $X \cap V = \emptyset$ so $\varphi_0(X) \cap \varphi_0(V \setminus \{Q\}) = \emptyset$ which in turn implies that $\varphi_0(X) \cap V' = \emptyset$. Also $X' := \varphi_0(X)$ is a closed subscheme of W_0 with reduced induced subscheme structure by Hartshorne II 4.4. Then

$$h_k(\varphi(P)) = h_k(\varphi'(\varphi_0(P))) = h_k(\varphi_0(P)) + O(1) = h_k(P) + O(1)$$

by the above and by induction, for all $P \in X(\overline{k})$. ■

Math 254B: Arakelov Theory **Spring 2021**

Lectures 11 and 12: 12-17 February

Professor Paul Vojta Abhishek Shivkumar

Heights on Varieties

We've seen that, under certain transformations, heights are invariant up to adding $O(1)$. We will see that in more general transformations, heights are scaled by a positive integer, again up to $O(1)$.

In this context, coherent means finite rank.

Definition 23.1.1: Vector Sheaves

A *line sheaf* on a scheme X is a locally free sheaf of $\mathcal{O}_X$-modules of rank 1, also called an *invertible sheaf*. More generally, a *vector sheaf* on X is a coherent locally free sheaf on X, assumed to have constant rank.

Vector sheaves are the same data as vector bundles.

Note that, given $f : X \to Y$ a morphism of schemes, $\mathcal{L}$ a line sheaf on X, $f_*\mathcal{L}$ is not necessarily a line sheaf, or even a vector sheaf, on Y. For example, take $X = \mathbb{A}^1_k$, k a field, $f : X \to \operatorname{Spec} k$, $\mathcal{L} = \mathcal{O}_X$. Then $f_*\mathcal{O}_X = k[x]$ (since $\operatorname{Spec} k$ is a point) which is locally free of infinite rank. More pathologically, if $X = Y = \mathbb{A}^1_k$, $f : X \to Y$ the constant function 0, then $f_*\mathcal{O}_X$ is the skyscraper sheaf $k[x]$ at 0, which is not locally free.

Pullbacks are better behaved than pushforwards:

This is mostly a sketch.

Proposition 23.1.2

Let $f : X \to Y$ be a morphism of schemes, $\mathcal{E}$ a vector sheaf on Y, then $f^*\mathcal{E}$ is a vector sheaf on X of the same rank.

Proof: $f^*\mathcal{O}_Y \cong \mathcal{O}_X$ by Hartshorne II 5.2e, or by applying the definition of f^*. Therefore, $f^*\mathcal{O}_Y^r \cong \mathcal{O}_X^r$ for all r, so pulling back vector sheaves looks just like pulling back vector bundles: you can trivialize locally, write out transition maps on intersections, and pull them back to combine $\mathcal{O}^r_{f^{-1}(U)}$ and $\mathcal{O}^r_{f^{-1}(V)}$ on $f^{-1}(U) \cap f^{-1}(V) = f^{-1}(U \cap V)$. ■

One can also define tensor products of vector sheaves, and, again, pullbacks of these behave well.

Definition 23.1.3: Picard Group

Let X be a scheme, then $\mathrm{Pic}(X)$ is the group of isomorphism classes of line sheaves on X, with group operation $\otimes$, inverse $\mathcal{L} \mapsto \mathcal{L}^*$, and identity element $\mathcal{O}_X$.

Example 23.1.4

Let k be a field, $n \in \mathbb{Z}_{>0}$. On $\mathbb{P}^n_k = \mathrm{Proj}\, k[x_0, \cdots, x_n]$, $\mathcal{O}(1) = \widetilde{S(1)}$ where $S = k[x_0, \cdots, x_n]$ and $S(n)$ shifts degrees by n. The line sheaf $\mathcal{O}(m)$ can be described by giving the standard open cover $U_i = \{x_i \neq 0\} = D_+(x_i)$, local trivializations $\varphi : \mathcal{O}(m)|_{U_i} \xrightarrow{\sim} \mathcal{O}_{U_i}$ by $s \mapsto s/x_i^m$, and transition functions $f_{ij} = (x_j/x_i)^m$.

Based on the linear flow of time, I kind of thought that this example would maybe talk about $\mathrm{Pic}(\mathbb{P}^n_k) = \mathbb{Z}$, but I guess that that point was left to subtext.

Theorem 23.1.5: Height Machine

Let k be a number field or function field (in one variable). Then there is a way to assign to each pair $(X, \mathcal{L})$ of a complete variety X over k and a line sheaf $\mathcal{L}$ on X, a *height function* $h_{X,\mathcal{L}} : X(\bar{k}) \to \mathbb{R}$ unique up to $O(1)$ satisfying *additivity*:

$$h_{X,\mathcal{L}\otimes\mathcal{L}'} = h_{X,\mathcal{L}} + h_{X,\mathcal{L}'} + O(1)$$

as well as *functoriality*, as in, for all morphisms $f : X \to Y$ of varieties over k, and for all line sheaves $\mathcal{L}$ on Y,

$$h_{X,f^*\mathcal{L}} = h_{Y,\mathcal{L}} \circ f + O(1)$$

(where f on the right hand side means $f(\bar{k}) : X(\bar{k}) \to Y(\bar{k})$). Finally, these heights satisfy the criterion of *normalization*: if $X = \mathbb{P}^n_k$ for some n, then

$$h_{\mathbb{P}^n_k,\mathcal{O}(1)} = h_k + O(1)$$

for all $n \in \mathbb{N}$. In each case, the implied constants do not depend on the points in $X(\bar{k})$ or $\mathbb{P}^n_k(\bar{k})$.

Our goal is to build up to this result. The point of the normalization requirement is that our height functions are actually meaningful, otherwise we could just set the 0 function for each height.

Definition 23.1.6

Let $\mathcal{L}$ be a line sheaf on a scheme X. We say that $\mathcal{L}$ is *globally generated*, or *generated by global sections* (gbgs) if there exists a surjective sheaf map $\mathcal{O}_X^{\oplus I} \to \mathcal{L}$. Equivalently, for all $P \in X$, there exists $s \in \Gamma(X, \mathcal{L})$ such that $s_P \notin \mathfrak{m}_P \mathfrak{L}_P$.

Moreover, given U an open subset of X, we say that $\mathcal{L}$ is *globally generated over* U if there exists a sheaf morphism $\mathcal{O}_X^{\oplus I} \to \mathcal{L}$ whose restriction to U is surjective.

If $\mathcal{L}$ is generated by a single section, I think it should be trivial.

Theorem 23.1.7: Hartshorne II 7.1b

Let X be a scheme over a ring A, $\mathcal{L}$ a line sheaf on X, $s_0, \cdots, s_n \in \Gamma(X, \mathcal{L})$ global sections that generate $\mathcal{L}$. Then there exists a unique A-morphism $\varphi : X \to \mathbb{P}^n_A$ such that $\mathcal{L} \cong \varphi^* \mathcal{O}(1)$, with $s_i = \varphi^* x_i$.

Proof: The idea of the proof is to set φ in homogeneous coordinates by $[s_0 : \cdots : s_n]$. In detail, set $V_i = X_{s_i}$ which are open subsets of X that cover X (where s_i generates $\mathcal{L}$ over V_i). Then, there exist $f_{ij} \in \mathcal{O}(V_i)$ such that $s_j|_{V_i} = f_{ij} s_i|_{V_i}$. Set $U_i = D_+(x_i) \subseteq \mathbb{P}^n_A$, e.g, $U_i = \operatorname{Spec} A[x_0/x_i, \cdots, x_n/x_i]$ (where x_i/x_i is omitted), and $\varphi_i : V_i \to U_i$ the morphism over $\operatorname{Spec} A$ corresponding to the homomorphism $A[x_0/x_i, \cdots, x_n/x_i] \to \Gamma(V_i, \mathcal{O}_{V_i})$ of A-algebras given by $x_j/x_i \mapsto f_{ij}$ for $j \neq i$. This implies that $P \mapsto (f_{i0}(P), \cdots, f_{in}(P)) \in \mathbb{A}^n_A$ by Hartshorne II Exercise 2.4, where again $f_{ii}(P)$ is omitted, so φ_i has homogeneous coordinates $[f_{i0} : \cdots : f_{in}]$ with $f_{ii} = 1$ not omitted. By the cocycle condition on the f_{ij}, $\varphi_i|_{V_i \cap V_j} = \varphi_j|_{V_i \cap V_j}$ so the φ_i glue to give a well-defined morphism $\varphi : X \to \mathbb{P}^n_A$. ■

The remainder of the theorem is left as an exercise.

Definition 23.1.8

Let X, $\mathcal{L}$, $s_0, \cdots, s_n$, and φ be as above, with $\underline{s} = (s_0, \cdots, s_n)$. Then we define

$$h_{\underline{s},k}(P) = h_k(\varphi(P))$$

for all $P \in X(\overline{k})$.

Example 23.1.9

Let $X = \mathbb{P}^n_k$, $\mathcal{L} = \mathcal{O}(1)$, $s_i = x_i$. Then $\varphi : \mathbb{P}^n_k \to \mathbb{P}^n_k$ is the identity map, $h_{\underline{s},k} = h_k$.

Example 23.1.10

Let X be proper over k, $\mathcal{L} = \mathcal{O}_X$, $\underline{s} = (1)$. Then φ is the constant map $X \to \mathbb{P}^0_k = \operatorname{Spec} k$ and $h_{\underline{s},k}(P) = 0$.

Example 23.1.11

Let $X = \mathbb{P}^1_k$, $\mathcal{L} = \mathcal{O}(2)$, $\underline{s} = (x_0^2, x_1^2)$. Then $h_{\underline{s},k}(P) = 2h_k(P)$ for all $P \in X(\overline{k})$.

Example 23.1.12

Let $X = \mathbb{P}^1_{\mathbb{Q}}$, $\mathcal{L} = \mathcal{O}(2)$, $\underline{s} = (ax_0^2, x_0 x_1, x_1^2)$ for some $a \in \mathbb{Q}^\times$. Then $h_{\underline{s},\mathbb{Q}} = h_{\mathbb{Q}} \circ \varphi_a$. This differs from $2h_{\mathbb{Q}}$ by a bounded function, which is nonconstant unless $a = \pm 1$.

We want to define a height function $h_{\mathcal{L},k} : X(\overline{k}) \to \mathbb{R}$. This will be a well defined map up to adding a bounded function (i.e, the specific values of the function do not themselves matter as much as understanding the general distribution of points of bounded height). Here X is any proper scheme over k, $\mathcal{L}$ any line sheaf, although we will begin with globally generated line sheaves.

Lemma 23.1.13

Let $\mathcal{L}$ be a line sheaf on X. Assume that $\mathcal{L}$ is generated by global sections $\underline{s} = (s_0, \cdots, s_n)$ and also generated by global sections $\underline{t} = (t_0, \cdots, t_m)$. Then

$$h_{\underline{s},k} = h_{\underline{t},k} + \mathcal{O}(1)$$

Proof: By comparing $h_{\underline{s},k}$ and $h_{\underline{t},k}$ with $h_{\underline{n},k}$ where $\underline{n} = (s_0, \cdots, s_n, t_0, \cdots, t_m)$, we may reduce to the case where $\underline{t} = (s_0, \cdots, s_n, s_{n+1}, \cdots, s_m)$ (reusing m as a different index). Let $\varphi : X \to \mathbb{P}^n_k$ and $\psi : X \to \mathbb{P}^m_k$ be the morphisms $[s_0 : \cdots : s_n]$ and $[s_0 : \cdots : s_m]$ respectively. Identify $\mathbb{P}^n_k$ with the linear subspace $x_{n+1} = \cdots = x_m = 0$ in $\mathbb{P}^m_k$; then, we have a linear projection $\Theta : \mathbb{P}^m_k \setminus \{x_0 = \cdots = x_n = 0\} \to \mathbb{P}^n_k$ as in Lemma 22.2.7, such that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[d, "\psi"] \arrow[dr, "\varphi"] & \\
\mathbb{P}^m_k \arrow[r, "\Theta"] & \mathbb{P}^n_k
\end{tikzcd}$$

Since $\psi(X)$ is a closed subset of $\mathbb{P}^m_k$ (as X is proper) disjoint from $\{x_0 = \cdots = x_n = 0\}$, Lemma 22.2.7 applies, and we have

$$h_{\underline{s},k}(P) = h_k(\varphi(P)) = h_k(\Theta(\psi(P))) = h_k(\psi(P)) + O(1) = h_{\underline{t},k}(P) + O(1)$$

■

Lemma 23.1.14

Let $\mathcal{L}$ and $\mathcal{M}$ be line sheaves on X generated by global systems $\underline{s}$ and $\underline{t}$ respectively. Then

$$\underline{s} \otimes \underline{t} := (s_i \otimes t_j)_{i,j}$$

is a generating system of global sections of $\mathcal{L} \otimes \mathcal{M}$, and

$$h_{\underline{s}\otimes\underline{t}} = h_{\underline{s},k} + h_{\underline{t},k}$$

Proof: The first assertion is obvious. For the second assertion, let $\varphi_{\underline{s}} : X \to \mathbb{P}^n_k$, $\varphi_{\underline{t}} : X \to \mathbb{P}^m_k$, and $\varphi_{\underline{s}\otimes\underline{t}} X \to \mathbb{P}^{mn+m+n}_k$ (via the Segre embedding) be the maps determined by our global generating systems. Let $P \in X(\overline{k})$, L a finite extension of k such that $P \in X(L)$, and let $[x_0 : \cdots : x_n]$ and $[y_0 : \cdots : y_m]$ be homogeneous coordinates for $\varphi_{\underline{s}}(P)$ and $\varphi_{\underline{t}}(P)$ in L, respectively. Then

$$H_L(\varphi_{\underline{s}\otimes\underline{t}}(P)) = \prod_{\omega\in M_L} \max_{i,j} \|x_i y_j\|_\omega =$$
$$\prod_{\omega\in M_L} \max_i \|x_i\|_\omega \max_j \|y_j\|_\omega = H_L(\varphi_{\underline{s}}(P)) H_L(\varphi_{\underline{t}}(P))$$

Taking logs, we obtain the desired equality. ■

Corollary 23.1.15

Let $\mathcal{L}$ be a line sheaf on X, with $\mathcal{L} \cong \mathcal{M}_1 \otimes \mathcal{N}_1^\vee$ and $\mathcal{L} \cong \mathcal{M}_2 \otimes \mathcal{N}_2^\vee$ where $\mathcal{M}_1$, $\mathcal{N}_1$, $\mathcal{M}_2$, and $\mathcal{N}_2$ are generated by systems of global sections $\underline{s}$, $\underline{t}$, $\underline{u}$, and $\underline{v}$ respectively. Then

$$h_{\underline{s},k} - h_{\underline{t},k} = h_{\underline{u},k} - h_{\underline{v},k} + O(1)$$

This follows easily from the above two lemmas.

Math 254B: Arakelov Theory **Spring 2021**

Lectures 13-16: 19-26 February

Professor Paul Vojta Abhishek Shivkumar

Height Machine

As before, k is a number field or function field in one variable, X is a projective scheme over k.

Lemma 24.1.1

Let $\mathcal{L}$ be a line sheaf on X. Then there exist globally generated line sheaves $\mathcal{M}$ and $\mathcal{N}$ on X such that $\mathcal{L} \cong \mathcal{M} \otimes \mathcal{N}^\vee$.

Proof: Let $\mathcal{A}$ be an ample line sheaf on X. By definition of ampleness, $\mathcal{L} \otimes \mathcal{A}^{\otimes n}$ and $\mathcal{O}_X \otimes \mathcal{A}^{\otimes n}$ are globally generated for all sufficiently large n. Pick such an n, then take $\mathcal{M} = \mathcal{L} \otimes \mathcal{A}^{\otimes n}$ and $\mathcal{N} = \mathcal{A}^{\otimes n}$. ■

Recall that $\mathcal{A}$ is ample if, for any $\mathcal{F}$ coherent, and sufficiently large n, $\mathcal{F} \otimes \mathcal{A}^{\otimes n}$ is globally generated.

Definition 24.1.2

Two real-valued functions on the same domain are said to be *equivalent* if their difference is a bounded function.

E.g, if $f = g + O(1)$, then $f \sim g$.

Definition 24.1.3: Height Associated to a Line Sheaf

Let $\mathcal{L}$ be a line sheaf on X, $\mathcal{M}$ and $\mathcal{N}$ such that $\mathcal{L} \cong \mathcal{M} \otimes \mathcal{N}^\vee$ as above. Let $\underline{s}$ and $\underline{t}$ be systems of global sections that generate $\mathcal{M}$ and $\mathcal{N}$ respectively (which can be taken to be finite since X is quasi-compact), then $h_{\mathcal{L},k}$ is the equivalence class of $h_{\underline{s},k} - h_{\underline{t},k}$ which is well-defined by Corollary 23.1.15. A height function for $\mathcal{L}$ is any such representative of the equivalence class.

If $\mathcal{L}$ itself is globally generated, then we may take $\mathcal{M} = \mathcal{L}$, $\mathcal{N} = \mathcal{O}_X$.

Theorem 24.1.4: Height Machine for Projective Schemes

There is a unique way to assign to each pair $(X, \mathcal{L})$ of a projective scheme over k and a line sheaf on it, a height function $h_{\mathcal{L},k}$ (up to equivalence) such that the properties in the statement of Theorem 23.1.5 (with "variety" replaced by "projective scheme") hold.

Note that we did not have uniqueness in the original statement of the height machine.

Proof: Write $\mathcal{L} \cong \mathcal{A} \otimes \mathcal{B}^\vee$, $\mathcal{M} \cong \mathcal{C} \otimes \mathcal{D}^\vee$, where $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are globally generated line sheaves on X with generating systems $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ respectively. Then, $\mathcal{L} \otimes \mathcal{M}$ is clearly also globally generated, and by Corollary 23.1.15 and its preceding lemma,

$$h_{\mathcal{L}\otimes\mathcal{M},k} = h_{\underline{a}\otimes\underline{c},k} - h_{\underline{b}\otimes\underline{d},k} = h_{\underline{a},k} + h_{\underline{c},k} - h_{\underline{b},k} - h_{\underline{d},k} = h_{\mathcal{L},k} + h_{\mathcal{M},k}$$

where the final equality follows by pairing terms. Thus, additivity holds for our height machine.

For functoriality, with $f : X \to Y$ a morphism of projective schemes, let $\mathcal{M} \cong \mathcal{A} \otimes \mathcal{B}^\vee$ over Y, with $\mathcal{A}$ and $\mathcal{B}$ globally generated as above. If $\underline{a} = (a_0, \cdots, a_n)$, then $f^*\mathcal{A}$ is globally generated by $f^*\underline{a} = (f^*a_0, \cdots, f^*a_n)$, and if $\underline{a}$ determines a morphism $\varphi = [a_0 : \cdots : a_n]$ from Y to $\mathbb{P}^n_{\overline{k}}$ over $\overline{k}$, then $f^*\underline{a}$ determines a morphism $\psi = [f^*a_0 : \cdots : f^*a_n]$ from X to $\mathbb{P}^n_{\overline{k}}$. Moreover, $\psi = \varphi \circ f$, so

$$h_{f^*\underline{a},k}(\varphi) = h_k(\psi(P)) = h_k(\varphi(P)) = h_{\underline{a},k}(f(P))$$

and similarly $h_{f^*\underline{b},k}(P) = h_{\underline{b},k}(f(P))$. Subtracting gives

$$h_{f^*\mathcal{M},k}(P) = h_{\mathcal{M},k}(f(P)) + O(1)$$

for all P as desired.

Finally, for normalization, $h_{\mathcal{O}(1),k} = h_{\underline{s},k} + O(1) = h_k + O(1)$ by Example 23.1.9.

It remains to show that this assignment is essentially unique: given $\mathcal{L}$, write $\mathcal{L} \cong \mathcal{M} \otimes \mathcal{N}^\vee$ as before. If $\mathcal{M}$ is globally generated by $\underline{s} = (s_0, \cdots, s_n)$ and $\varphi : X \to \mathbb{P}^n_{\overline{k}}$ is the map $[s_0 : \cdots : s_n]$, then $\mathcal{M} \cong \varphi^*\mathcal{O}(1)$; therefore

$$h_{\mathcal{M},k}(P) = h_{\mathcal{O}(1),k}(\varphi(P)) = h_k(\varphi(P)) = h_{\underline{s},k}(P)$$

all up to $O(1)$, where we have applied functoriality and normalization. Similarly, if $\mathcal{N}$ is globally generated by $\underline{t}$, then $h_{\mathcal{N},k} = h_{\underline{t},k} + O(1)$, so

$$h_{\mathcal{L},k} = h_{\mathcal{M},k} - h_{\mathcal{N},k} = h_{\underline{s},k} - h_{\underline{t},k}$$

up to $O(1)$ from which the result follows. ■

If X is only quasi-projective (i.e in the case of varieties), you lose uniqueness, since Lemma 22.2.7 fails when X is not complete, hence $h_{\underline{s},k} = h_{\underline{t},k} + O(1)$ no longer holds when $\underline{s}$ and $\underline{t}$ both globally generate $\mathcal{L}$.

Additional Properties of Heights

Theorem 24.2.1: Northcott for Projective Schemes

Let X be a projective scheme over k a number field, $\mathcal{L}$ an ample line sheaf on X, and $h_{\mathcal{L},k}$ a height function for $\mathcal{L}$. Then for all $d \in \mathbb{Z}_{>0}$, $C \in \mathbb{R}$, the set

$$\{P \in X(\overline{k}) : [k(P) : k] \le d \text{ and } h_{\mathcal{L},k}(P) \le C\}$$

is finite.

Northcott's theorem as stated *fails* when k is a function field.

Proof: Pick $n \in \mathbb{Z}_{>0}$ such that $\mathcal{L}^{\otimes n}$ is very ample over k, and let $\varphi : X \to \mathbb{P}^N_k$ be a closed embedding such that $\mathcal{L}^{\otimes n} \cong \varphi^*\mathcal{O}(1)$. Then, adjusting C if necessary, we may assume $h_{\mathcal{L},k} = \frac{1}{n} h_k \circ \varphi$, and we have an injection (induced by φ) from the set in the theorem statement into

$$\{Q \in \mathbb{P}^N(\overline{k} : [k(\mathbb{Q}) : k] \le d \text{ and } h_k(Q) \le nc\}$$

which is finite by Northcott's theorem on $\mathbb{P}^N_k$, from which the result follows. ■

Proposition 24.2.2: Positivity

Let $\mathcal{L}$ be a line sheaf on X a projective scheme, and let $h_{\mathcal{L},k}$ be an associated height function. If $\mathcal{L}$ is gbgs, then $h_{\mathcal{L},k}$ is bounded from below; moreover if $\mathcal{L}$ is generated by global sections over an open subset $U \subseteq X$, then $h_{\mathcal{L},k}$ is bounded from below on all $P \in U(\overline{k})$.

Proof: For the first part, since X is quasicompact, there exists a finite system of generating global sections $s_0, \cdots, s_n$. Let $\varphi : X \to \mathbb{P}^n_k$ be the map $[s_0 : \cdots : s_n]$, then $h_{\mathcal{L},k} = h_{\underline{s},k} + O(1) \ge O(1)$ where the inequality follows from the fact that $h_{\underline{s},k}(P) = h_k(\varphi(P)) \ge 0$ for all $P \in X(\overline{k})$.

For the second part, which is strictly stronger than the first part, note that since X is noetherian, U is quasicompact, so $\mathcal{L}$ is generated over U by finitely many sections $u_0, \cdots, u_l \in \Gamma(X, \mathcal{L})$. Write $\mathcal{L} = (\mathcal{L} \otimes \mathcal{M}) \otimes \mathcal{M}^\vee$ with $\mathcal{M}$ and $\mathcal{L} \otimes \mathcal{M}$ globally generated line sheaves. Let $\underline{s} = (s_0, \cdots, s_n)$ be a generating system for $\mathcal{M}$, $\underline{t} = (t_0, \cdots, t_m)$ a generating system for $\mathcal{L} \otimes \mathcal{M}$. We may assume that $\underline{u} \otimes \underline{s}$ is a subset of $\underline{t}$ by choice of $\underline{t}$. We want to show that $h_{\underline{t},k}(P) \le h_{\underline{u}\otimes\underline{s},k}(P) = h_{\underline{u},k}(P) + h_{\underline{s},k}(P)$ for all $P \in U(\overline{k})$, but $h_{\underline{u}\otimes\underline{s},k}$ is not really defined on X, and likewise for $h_{\underline{u},k}$. However, we do have $h_{\mathcal{L},k} = h_{\underline{t},k} - h_{\underline{s},k} + O(1)$ so it suffices to show that $h_{\underline{t},k} \ge h_{\underline{s},k}$ on $U(\overline{k})$. To that end, let $\varphi : X \to \mathbb{P}^n$, $\psi : X \to \mathbb{P}^m$, $\theta : U \to \mathbb{P}^l$ be the maps given by the global sections $\underline{s}$, $\underline{t}$, and $\underline{u}$ respectively. Let L be a finite extension of k, $P \in U(L)$, and let $[x_0 : \cdots : x_n]$, $[y_0 : \cdots : y_m]$, and $[w_0 : \cdots : w_l]$ be homogeneous coordinates for $\varphi(P)$, $\psi(P)$, and $\theta(P)$ respectively. By permuting indices, we may assume that x_0 and w_0 are nonzero. Then s_0 and u_0 generate $\mathcal{M}$ and $\mathcal{L}$ respectively at P, and $s_0 \otimes u_0$ generates $\mathcal{L} \otimes \mathcal{M}$ at P. Again, by permuting indices, we may assume that $t_0 = u_0 \otimes s_0$, so $y_0 \ne 0$ as well, and we may therefore assume that $x_0 = y_0 = w_0 = 1$. Then, since we have assumed that $\{w_h x_i : 0 \le h \le l \text{ and } 0 \le i \le n\}$ is a subset

We need the fact that $P \in U$ when assuming that $w_0 \ne 0$ below.

of $\{y_j : 0 \leq j \leq m\}$, it follows that

$$H_L(\psi(P)) = \prod_{\nu \in M_L} \max(\|y_0\|_\nu, \cdots, \|y_m\|_\nu) \geq$$
$$\prod_{\nu \in M_L} \max\{w_h x_i : 0 \leq h \leq l \text{ and } 0 \leq i \leq n\} =$$
$$\prod_{\nu \in M_L} \max(\|w_h\|_\nu)_h \prod_{\nu \in M_L} \max(\|x_i\|_\nu)_i \geq H_L(\varphi(P))$$

where in the final inequality, we have used the fact that $H_L \geq 1$. Taking logs, this gives that $h_{\underline{t},k}(P) \geq h_{\underline{s},k}(P)$, from which the result follows. ■

Next, we want to show that heights relative to ample divisors dominate all other heights, up to constant multiples and $O(1)$.

Proposition 24.2.3

Let $\mathcal{L}$, $\mathcal{M}$, be line sheaves on X, with $\mathcal{L}$ ample. Then there is a constant C, depending only on $\mathcal{L}$ and $\mathcal{M}$, such that

$$h_{\mathcal{M},k}(P) \leq C h_{\mathcal{L},k}(P) + O(1)$$

for all $P \in X(\overline{k})$.

Proof: Since $\mathcal{L}$ is ample, there exists an integer n such that $\mathcal{M}^\vee \otimes \mathcal{L}^{\otimes n}$ is globally generated. Then, by positivity, $h_{\mathcal{M}^\vee \otimes \mathcal{L}^{\otimes n},k} \geq O(1)$, so $n h_{\mathcal{L},k} - h_{\mathcal{M},k} \geq O(1)$, from which the result follows. ■

Recall (for convenience) that a line sheaf is ample if some tensor power of it is very ample, and a line sheaf is very ample if it is globally generated by global sections and the associated morphism to $\mathbb{P}^n$ (given by global sections) is a closed immersion. Many equivalent forms of these definitions exist (especially when assuming various adjectives about the base scheme), and we may be using a different one for the basis of our discussion.

Heights on Proper Schemes

Definition 24.3.1

Let X be a proper scheme over k, and $\mathcal{L}$ a line sheaf on X. Then a *height function* for $\mathcal{L}$ and k is a function $h_{\mathcal{L},k} : X(\overline{k}) \to \mathbb{R}$ such that there exists a proper birational k-morphism $g : X' \to X$, with X' projective over k, and $g^* h_{\mathcal{L},k} := h_{\mathcal{L},k} \circ g$ is a height function for $g^*\mathcal{L}$ and k on X'.

By Chow's lemma, Hartshorne II Ex. 4.10, morphisms g and schemes X' as above do exist for all X. Note that the wording "g is a birational morphism" means that g is a morphism of schemes (i.e, regular everywhere on X') and is birational (i.e, invertible as a rational map). This is stronger than simply a birational map.

Proposition 24.3.2

If $h_{\mathcal{L},k}$ as above satisfies the given criterion for some $g : X' \to X$ (again, as above), then it satisfies the given criterion for all such g. Thus, the earlier definition is compatible with this one, as we may take g to be the identity map if X is projective.

Towards proving this key result, we need to develop some basic notions from algebraic geometry.

Definition 24.3.3: Graphs

Let S be a scheme, $f : X \to Y$ a morphism of S-schemes. Then $\Gamma_f = (\mathrm{id}_X, f)_S : X \to X \times_S Y$ is called the *graph* of f.

Proposition 24.3.4

If Y is separated over S, then Γ_f as above is a closed immersion.

Without separatedness of Y/S, the image of Γ_f is only locally closed.

Proof: The following diagram is Cartesian:

$$\begin{tikzcd}
X \arrow[r, "\Gamma_f"] \arrow[d, "f"] & X \times_S Y \arrow[d, "f \times \mathrm{id}_Y"] \\
Y \arrow[r, "\Delta"] & Y \times_S Y
\end{tikzcd}$$

This follows from Vakil Ex. 1.3.S. Since Δ is a closed immersion (as Y/S is separated), so is Γ_f. ■

Definition 24.3.5: Graph Closure

Let X be a scheme, $U \subseteq X$ an open dense subset, $f : U \to Y$ a morphism, with Y separated. Let $Z \subseteq X \times_S Y$ be the closure of the image of Γ_f. This is the *closure of the graph* of f.

Proposition 24.3.6

$Z \cap (U \times Y)$ is the graph of f.

Proposition 24.3.7

Let Z' be the image of Γ_f in $U \times Y$. Then Z' is closed in $U \times Y$, so $Z \cap (U \times Y) = Z'$, since $U \times Y$ is open in $X \times Y$.

Proposition 24.3.8

If Y is proper over S, then $Z \to X$ is surjective.

Proposition 24.3.9

$Z \to X \times_S Y \to X$ is a composition of proper maps (the first a closed immersion, the second the base change of a proper map), and is therefore itself proper, so its image is closed. Also, this image contains U, so it must contain $\overline{U} = X$. The image contains U since $U \to U \times_S Y \to U$ is the identity map.

As before, with the convention that k is a number field or function field, we are now ready to prove Proposition 24.3.2:

Proof: Let $g_i : X_i \to X$ be birational morphisms from projective k-schemes for $i = 1, 2$, and let $h : X(\bar{k}) \to \mathbb{R}$ be a function. Let X_3 be a projective k-scheme and $f : X_3 \to X_1$ a birational k-morphism. Then $P \mapsto h(g_1(P))$ is a height function for $g_1^*\mathcal{L}$ and k on X_1 iff $Q \mapsto h(g_1(f(Q)))$ is a height function for $(g_1 \circ f)^*\mathcal{L}$ and k on X_3. The forward direction is clear via the functoriality of heights, and the reverse direction is left as an exercise.

Since g_1 and g_2 are birational maps, we have a birational map $g := g_2^{-1} \circ g_1$ from X_1 to X_2 over X. Let $Z \subseteq X_1 \times_k X_2$ be the closure of Γ_g; then Z is projective over k, and the projections $p_i : Z \to X_i$ are birational morphisms, and the following diagram commutes identically:

$$\begin{tikzcd}
Z \arrow[r, "p_1"] \arrow[d, "p_2"] & X_1 \arrow[d, "g_1"] \\
X_2 \arrow[r, "g_2"] & X
\end{tikzcd}$$

To see the latter claim, note that there exists an open dense subset $U \subseteq X$ such that $g_i^{-1} : U \to U$ is an isomorphism for all i, so $g : X_1 \dashrightarrow X_2$ is defined on $g_1^{-1}(U)$, $p_1^{-1}(g_1^{-1}(U)) \to g_1^{-1}(U)$ is an isomorphism, so

$$p_2 = g \circ p_1 = g_2^{-1} \circ g_1 \circ p_1$$

so $g_2 \circ p_2 = g_1 \circ p_1$ over U. Since $p_1^{-1}(g_1^{-1}(U))$ is dense in Z, $g_2 \circ p_2 = g_1 \circ p_1$ on Z by Hartshorne II Ex 4.2 (e.g, given some adjectives, morphisms agreeing on open dense subsets agree are equal) assuming that X_1, X_2, and X are reduced.

Now, using the two above claims, $P \mapsto h(g_1(P))$ is a height function for $g_1^*\mathcal{L}$ on X_1 iff $Q \mapsto h(g_1(p_1(Q)))$ is a height function for $p_1^*g_1^*\mathcal{L}$ on Z iff $Q \mapsto h(g_1(p_1(Q)))$ is a height function for $p_2^*g_1^*\mathcal{L}$ on Z iff $P \mapsto h(g_2(P))$ is a height function for $g_2^*\mathcal{L}$ on X_2, from which the result follows. ■

Corollary 24.3.10

If X is projective, then this definition of a height function on X coincides with the earlier definition.

Proof: Let $X' = X$ and $g = \mathrm{id}_X$. ■

Theorem 24.3.11: Height Machine for Proper Schemes

There is a unique way to assign to each pair $(X, \mathcal{L})$ of a proper scheme over k and a line sheaf on it, a height function $h_{\mathcal{L},k}$ (up to equivalence) such that the properties in the statement of Theorem 23.1.5 (with "variety" replaced by "proper scheme") hold.

There was a partial proof of functoriality here before, but Vojta seems to have switched tracks and abandoned finishing it. I think that the existence of σ as described below may require the axiom of choice.

Proof: Additivity follows from additivity on the projective case, and normalization holds by the above corollary. Uniqueness up to $O(1)$ follows from the projective case by the below reformulation (with surjective maps replacing birational maps). Functoriality is left as an exercise, which is again made easier by the below reformulation in terms of surjective maps. It remains to show existence: let X be a proper scheme over k, $\mathcal{L}$ a line sheaf on X, and $g : X' \to X$ a surjective morphism over k, with X' projective over k; such a g exists by Chow's lemma. Then $g(\overline{k}) : X'(\overline{k}) \to X(\overline{k})$ is surjective, so there exists a function $\sigma : X(\overline{k}) \to X'(\overline{k})$ such that $g(\overline{k}) \circ \sigma$ is the identity on $X(\overline{k})$. Let $h_{g^*\mathcal{L},k}$ be a height function for $g^*\mathcal{L}$ and k on X', then $h : X(\overline{k}) \to \mathbb{R}$ defined by $P \mapsto h_{g^*\mathcal{L},k}(\sigma(P))$ is a height function for $\mathcal{L}$ and k on X (i.e, $P' \mapsto h_{g^*\mathcal{L},k}(\sigma(g(P')))$ is a height function for $g^*\mathcal{L}$ and k on X', the proof of which we leave as an exercise). ■

It seems we're redoing this whole discussion with birational replaced with surjective to prove the above result (more easily?). It seems to sidestep the discussion about graphs and graph closures.

Recalling Definition 24.3.1, we may in fact alter the birational assumption on $g : X' \to X$ to assuming that g is surjective, satisfying the properties in that definition. Then, the analogous result holds:

Proposition 24.3.12

If $h_{\mathcal{L},k} : X(\overline{k}) \to \mathbb{R}$ satisfies the above condition for one morphism $g : X' \to X$, with X' projective over k, then it satisfies the condition for all surjective $g : X' \to X$ over k with X' projective over k.

Proof: For $i = 1, 2$ let $g_i : X_i \to X$ be surjective morphisms over k with X_i projective over k, and let $h : X(\overline{k}) \to \mathbb{R}$ be a function. Assume that $P' \mapsto h(g_1(P'))$ is a height function for $g_1^*\mathcal{L}$ and k on X_1. We want to show that $P' \mapsto h(g_2(P'))$ is a height function for $g_2^*\mathcal{L}$ and k on X_2. Let $X_3 = X_1 \times_X X_2$; this is projective over k, and the projections $p_i : X_3 \to X_i$ are both surjective. Then since $P' \mapsto h(g_1(P'))$ is a height function for $g_1^*\mathcal{L}$, $Q \mapsto h(g_1(p_1(Q)))$ is a height function for $p_1^*g_1^*\mathcal{L}$ on X_3 (by functoriality of heights on projective schemes), which in turn implies that $Q \mapsto h(g_2(p_2(Q)))$ is a height function for $p_2^*g_2^*\mathcal{L}$ on X_3 (since base change is projective, and $g_1 \circ p_1 = g_2 \circ p_2$), which finally implies that $P' \mapsto h(g_2(P'))$ is a height function, since p_2 is surjective. ■

On projective schemes, the Northcott property and the property that heights corresponding to ample line sheaves "dominate" all other heights in a precise sense both require the existence of ample line sheaves on X. and a proper scheme with an ample line bundle is projective, so there is no extending these properties. The positivity property (that heights associated to gbgs line sheaves are bounded below) follows immediately for proper schemes by pulling back to a projective scheme.

Cartier Divisors

For this section, X is an integral scheme, not necessarily proper over k. $K(X)$ denotes the function field of an integral scheme X, and $\mathcal{K}_X^\times$ is the constant sheaf $K(X)^\times$ on X, with $\mathcal{K}^\times(U)$ equal to 1 for $U = \emptyset$, and $K(X)^\times$ otherwise (since X is integral and therefore irreducible). $\mathcal{O}_X^\times$ is the sheaf given by $\mathcal{O}_X^\times(U) = \mathcal{O}_X(U)^\times$, where $\mathcal{O}_X^\times \subseteq \mathcal{K}^\times$ are sheaves of abelian groups under multiplication.

Definition 24.4.1: Cartier Divisors

A *Cartier divisor* on X is a global section of $\mathcal{K}^\times/\mathcal{O}_X^\times$.

Evidently, Cartier divisors form a group $\Gamma(X, \mathcal{K}^\times/\mathcal{O}_X^\times)$ under multiplication, which is usually denoted $\mathrm{CDiv}(X)$ and written additively. Concretely, the data of a Cartier divisor on X can be represented by a collection (U_i, f_i) of pairs in which the U_i are an open cover of X, $f_i \in K(X)^\times$, and $f_i/f_j \in \mathcal{O}_X(U_i \cap U_j)^\times$ for all i, j. Two such collections (U_i, f_i) and (V_j, g_j) describe the same Cartier divisor iff $f_i/g_j \in \mathcal{O}_X(U_i \cap V_j)^\times$ for all i and j. If so, the union of these collections also describes the same Cartier divisor.

I don't understand what happens when U_i and V_j have empty intersection - something to do with the fact that nonempty opens are dense? Also, Cartier divisors have the same data as invertible ideal sheaves - will this relate to the ideal class group?

Definition 24.4.2: Effectivity

A Cartier divisor is *effective* if it is described by a collection (U_i, f_i) with $f_i \in \mathcal{O}_X(U_i)$ for all i. If so, then the condition holds for all collections representing the given divisor.

Definition 24.4.3

Let D be a Cartier divisor on X, (U_i, f_i) a collection representing it. Then the *support* of D is the set $\mathrm{Supp}(D) = \{x \in X : \exists i \text{ s.t } f_i \notin \mathcal{O}_{X,x}^\times\}$.

Note that if $x \in U_i \cap U_j$, then $f_i \notin \mathcal{O}_{X,x}^\times \iff f_j \notin \mathcal{O}_{X,x}^\times$ since f_i and f_j must have the same poles and zeros on $U_i \cap U_j$, so the support of D does not depend on the choice of collection representing D. Intuitively, $x \in \mathrm{Supp}(D)$ iff some f_i with $U_i \ni x$ has a zero or pole at x (or both, for different i). As an example, consider the Cartier divisor D on $X = \mathbb{A}_k^2 = \operatorname{Spec} k[t, u]$ represented by the collection with one element $(X, t/u)$. Here, $\mathrm{Supp}(D)$ is the union of coordinate axes. This description gets messy when X has singularities.

Math 254B: Arakelov Theory **Spring 2021**

Lectures 17-19: 1-5 March

Professor Paul Vojta Abhishek Shivkumar

Cartier Divisors

Let X be an integral scheme, D a Cartier divisor on X.

Proposition 25.1.1

Supp(D) is a proper closed subset of X.

Proof: Equivalently, $X \setminus \mathrm{Supp}(D)$ is nonempty and open. Nonemptiness follows from the fact that the generic point ξ of X has local ring $\mathcal{O}_{X,\xi} = K(X)$, so $\mathcal{O}_{X,\xi}^\times = K(X)^\times$ which always contains f_i, so $\xi \notin \mathrm{Supp}(D)$. For openness, if $f_i \in \mathcal{O}_{X,x}^\times$, then $f_i \in \mathcal{O}_{X,y}^\times$ for all y in some open neighborhood of x (by sheaf theory). ■

The support of a Weil divisor $\sum_Y n_Y Y$ on X is the union $\cup_{n_Y \neq 0} Y$.

Definition 25.1.2

Let $f \in K(X)^\times$. Then the principal Cartier divisor (f) of f is the Cartier divisor represented by the single pair (X, f).

The group of Cartier divisor classes on X is the cokernel of the map $K(X)^\times \to \mathrm{CDiv}(X)$ given by $f \mapsto (f)$, denoted CaCl(X).

Morphisms of schemes satisfying certain properties induce pullbacks on Cartier divisors: let $\varphi : X \to Y$ be a morphism of integral schemes, D a Cartier divisor on Y, and assume that $\varphi(X) \nsubseteq \mathrm{Supp}(D)$. Let ζ be the generic point of X, $y = \varphi(\zeta) \in Y$ (which need not be the generic point of Y if φ is not dominant). Let (V_i, f_i) be a collection that represents D. To define $\varphi^* D$, for all i, let $U_i = \varphi^{-1}(V_i)$, which contains ζ if it is nonempty. Conversely, for such i, since $y = \varphi(\zeta) \notin \mathrm{Supp}(D)$, the stalk $(f_i)_y$ is in $\mathcal{O}_{Y,y}^\times$ so $\varphi^* f_i \in \mathcal{O}_{X,\zeta}^\times = K(X)^\times$. Also, if U_i and U_j are nonempty, $\zeta \in U_i \cap U_j$, and $f_i/f_J \in \mathcal{O}_Y(V_i \cap V_j)^\times$, so $\varphi^* f_i / \varphi^* f_j \in \mathcal{O}_X(U_i \cap U_j)^\times$. If $U_i = \emptyset$, take $f_i = 1$; these don't matter. Then, for all j, $U_i \cap U_j = \emptyset$, so $f_i/f_j \in \mathcal{O}(U_i \cap U_j)^\times$ because $\mathcal{O}(U_i \cap U_j)$ is the zero ring. This definition does not depend on the collection (V_i, f_i).

This definition is useful for actual calculations, but I'd rather think of pullbacks of Cartier divisors as pullbacks of fractional ideal sheaves.

If φ is dominant, then the condition $\varphi(X) \nsubseteq \mathrm{Supp}(D)$ holds for all D, so we get a pullback map $\varphi^* : \mathrm{CDiv}(Y) \to \mathrm{CDiv}(X)$ which is a group homomorphism.

Compare this to Weil divisors, which are equipped with a natural pushforward map as opposed to a pullback map $\varphi_* : \mathrm{Div}(X) \to \mathrm{Div}(Y)$ given by taking a prime divisor $Z \subseteq X$ to $[K(Z) : K(\varphi(Z))]\varphi(Z)$ if $\varphi(Z)$ has codimension one in Y, and 0 otherwise. Here φ is required to be a finite or generically finite proper surjective morphism.

Comparing Weil and Cartier Divisors

Let X be a noetherian, integral, separated scheme that is regular in codimension one. We can define a canonical group homomorphism $\mathrm{CDiv}(X) \to \mathrm{Div}(X)$ as follows: let D be a Cartier divisor on X represented by a collection (U_i, f_i). For each prime divisor Y on X, pick i such that $U_i \cap Y \neq \emptyset$, and let $n_Y = v_Y(f_i) \in \mathbb{Z}$ where v_Y is the valuation on the local ring $\mathcal{O}_{X,\eta}$, where η is the generic point of Y (as $\mathcal{O}_{X,\eta}$ is a DVR since it is regular and noetherian of dimension one). This is well-defined; if $U_j \cap Y \neq \emptyset$ with $i \neq j$, then $v_Y(f_i) = v_Y(f_j) \iff v_Y(f_i/f_j) = 0$ since $f_i/f_j \in \mathcal{O}_{X,\eta}^\times$ and units have valuation 0. n_Y is therefore independent of i, and also independent of the choice of collection (U_i, f_i) representing D by the same reasoning.

The claimed homomorphism results from extending the above map linearly, and is easily seen to be a group homomorphism that sits within the following commutative diagram:

$$\begin{tikzcd}
\mathrm{CDiv}(X) \arrow[r] & \mathrm{Div}(X) \\
K(X) \arrow[u] \arrow[ur] &
\end{tikzcd}$$

where the maps out of $K(X)$ are $f \mapsto (f)$. If X is a regular scheme (e.g a nonsingular variety), then $\mathrm{CDiv}(X) \to \mathrm{Div}(X)$ is an isomorphism. For information on the zoo of adjectives that control when this map is injective or surjective, see Hartshorne.

When $\mathrm{CDiv}(X) \to \mathrm{Div}(X)$ is an isomorphism, one can think of collections (U_i, f_i) representing D as having the property that $f_i|_{U_i} = D|_{U_i}$ for all i, e.g, D is locally given by the principal divisors (f_i) on U_i, so $\mathrm{Supp}(D - (f_i))$ is disjoint from U_i.

I don't really follow this intuition.

Weil Divisors

Returning to heights on k and $\mathbb{P}^1(k)$, with k a number field or function field, we have $k = \mathbb{A}^1(k) \hookrightarrow \mathbb{P}^1(k)$ given by $x \mapsto x \mapsto [1 : x]$. The schemes we will be discussing are (at least) integral, noetherian, separated, and regular in codimension 1 (note that normal schemes are regular in codimension 1). We may replace the assumptions of integrality and regularity in codimension 1 with the stronger condition of normality.

This result amounts to showing that every reasonable expectation on the homomorphism $\mathrm{CDiv}(X) \to \mathrm{Div}(X)$ holds.

Proposition 25.3.1

Let X be a normal scheme, separated and of finite tpye over a field or $\mathbb{Z}$. Let D be a Cartier divisor on X, then D is effective iff its image in $\mathrm{Div}(X)$ is effective as a Weil divisor. Moreover, the support of D equals the support of its image in $\mathrm{Div}(X)$, and the map $\mathrm{CDiv}(X) \to \mathrm{Div}(X)$ is injective.

Proof: For the first claim, let D be represented by a collection (U_i, f_i). If $f_i \in \mathcal{O}(U_i)$ for all i (e.g D is effective as a Cartier divisor), then for any prime divisor Y, i s.t U_i meets Y, $f_i \in \mathcal{O}_{U_i, Y\cap U_i}$, so $v_Y(f_i) \geq 0$. For the other direction, if $v_Y(f_i) \geq 0$ for all prime divisors Y, then we may first reduce to the case where U_i is affine for all i by taking a refinement of our open cover. Then, for all prime divisors Y meeting U_i, $v_Y(f_i) \geq 0$, so $f_i \in \mathcal{O}_{U_i, Y\cap U_i}$ for all $Y \cap U_i$ of codimension one. By Hartshorne II Proposition 6.3A or Vakil's "algebraic Hartog's lemma," $f_i \in \mathcal{O}(U_i)$, so D is effective.

Recall that, for $Y \subseteq X$ a subvariety, $\mathcal{O}_{Y,X}$ is the local ring of equivalence classes (U, f) where $U \subseteq X$ is open, $U \cap Y \neq \emptyset$, and $f \in \Gamma(U, \mathcal{O}_U)$, where the equivalence relation is given by agreement on the intersection.

The second claim is left as an exercise. For the final claim, let D' be the image of D in $\mathrm{Div}(X)$. Then $D' = 0$ iff both D' and $-D'$ are effective, which holds iff both D and $-D$ are effective (by the first claim), which in turn holds iff $f_i \in \mathcal{O}(U_i)^\times$ for all i, which by definition is true iff $D = 0$. ■

Here we have shown that the kernel of the map $\mathrm{CDiv}(X) \to \mathrm{Div}(X)$ is zero; gaining control on the image of this map is more difficult, and we will not discuss this here. See Hartshorne II, 6.11 and 6.11.2.

Divisor-Line Sheaf correspondence

For this section, X is an integral scheme.

Definition 25.4.1

Rational Sections of Line Sheaves Let $\mathcal{L}$ be a line sheaf on X. A *rational section* of $\mathcal{L}$ is an equivalence class of pairs (U, s) where U is a nonempty open subset of X and $s \in \Gamma(U, \mathcal{L})$, under the equivalence relation $(U, s) \sim (V, t)$ if $s|_{U\cap V} = t|_{U\cap V}$.

Equivalently, one may think of a rational section s as an element of the stalk $\mathcal{L}_\xi$ where ξ is the (unique, since X is integral) generic point of X. More compactly, we may write $s \in \Gamma(X, \mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{K}(X))$, where $\mathcal{K}(X)$ is the constant sheaf of rational functions on X.

With $\mathcal{L}$ as above, s a nonzero rational section of $\mathcal{L}$, let U_i be an open cover such that $\mathcal{L}|_{U_i} \cong \mathcal{O}_{U_i}$ for all i. Pick isomorphism $\varphi_i : \mathcal{L}|_{U_i} \to \mathcal{O}_{U_i}$; we have the following commutative diagram:

$$\begin{tikzcd}
& \mathcal{O}(U_i \cap U_j) \arrow[d, "\psi_{ij}"] \\
\mathcal{L}_{U_i \cap U_j} \arrow[ur, "\varphi_i|_{U_i \cap U_j}"] \arrow[r, "\varphi_j|_{U_i \cap U_j}"'] & \mathcal{O}(U_i \cap U_j)
\end{tikzcd}$$

Here ψ_{ij} is an isomorphism $\mathcal{O}(U_i \cap U_j) \to \mathcal{O}(U_i \cap U_j)$ which must be multiplication by some $f_{ij} \in \mathcal{O}(U_i \cap U_j)^\times$. For all i, let $f_i = \varphi_i(s|_{U_i})$. Then $f_i \in K(U_i)^\times = K(X)^\times$, and $f_j = f_{ij} f_i$, so $f_i/f_j = f_{ij}^{-1} \in \mathcal{O}(U_i \cap U_j)^\times$ for all i, j, so the collection of (U_i, f_i) represents a Cartier divisor on X which is independent of the choice of open cover and isomorphisms φ_i (this is an exercise). We denote this divisor by (s), or $\mathrm{div}(s)$, or $\mathrm{div}_{\mathcal{L}}(s)$.

If $\mathcal{L}$ and $\mathcal{M}$ are line sheaves, $\mathcal{L}$ a subsheaf of $\mathcal{M}$, then $\mathrm{div}_{\mathcal{L}}(s) \neq \mathrm{div}_{\mathcal{M}}(s)$ in general.

Example 25.4.2

If $\mathcal{L} = \mathcal{O}_X$, then the rational sections of $\mathcal{L}$ are the elements of $K(X)$, and for all $f \in K(X)^\times$, $\mathrm{div}(f)$ is equal to the principal Cartier divisor (f).

Some remarks - if X, $\mathcal{L}$, s, and (U_i, f_i) are as in the above construction, then $(s)|_{U_i} = (f_i)|_{U_i} = \mathrm{div}_{\mathcal{O}_X}(s/s_0)$ for any generator s_0 of $\mathcal{L}|_{U_i}$ (e.g $\varphi_i^{-1}(1)$). Moreover, if $x \in X$ disjoint from the support of (s) iff s is a regular nonzero section of $\mathcal{L}$ in an open neighborhood of X iff s_x generates the stalk $\mathcal{L}_x$. (s) is effective as a Cartier divisor iff $s \in \Gamma(X, \mathcal{L})$. The Weil divisor $\sum_Y n_Y Y$ obtained from (s) is characterized by $n_Y = v_Y(s/s_0)$ for any local generator s_0 of $\mathcal{L}$ in an open neighborhood of the generic point of Y. If s and t are nonzero rational sections of line sheaves $\mathcal{L}$ and $\mathcal{M}$, then $s \otimes t$ is a nonzero rational section of $\mathcal{L} \otimes \mathcal{M}$, and $(s \otimes t) = (s) + (t)$. Finally, if s is a nonzero rational section of $\mathcal{L}$, then s^{-1} is a nonzero rational section of $\mathcal{L}^\times$, and $(s^{-1}) = -(s)$.

Definition 25.4.3: Pullbacks

Let $\varphi : X \to Y$ be a morphism of integral schemes, $\mathcal{L}$ a line sheaf on Y, s a nonzero rational section of $\mathcal{L}$. If there exists a nonempty open subset V of Y such that s is represented by a regular section $s_V \in \mathcal{L}(V)$, and $\varphi^*(s_V) \in \varphi^*\mathcal{L}(\varphi^{-1}(V))$ is nonzero, then $\varphi^{-1}(V) \neq \emptyset$, and we define $\varphi^* s$ to be the nonzero rational section of $\varphi^*\mathcal{L}$ on X represented by $\varphi^* s_V \in \varphi^*\mathcal{L}(\varphi^{-1}(V))$.

Definition 25.4.4

Let D be a Cartier divisor on an integral scheme X, represented by a collection (U_i, f_i). Then $\mathcal{O}_X(D)$ (sometimes written $\mathcal{L}(D)$) is the $\mathcal{O}_X$-submodule of $\mathcal{K}_X$ (the constant sheaf $K(X)$ on X) such that $\mathcal{O}_X(D)|_{U_i}$ is the $\mathcal{O}_{U_i}$-submodule of $\mathcal{K}|_{U_i}$ generated by f_i^{-1} for all i.

It is called the *line sheaf associated to D*.

How I'm used to thinking of this: the subsheaf of $\mathcal{K}_X$ whose sections f have poles contained in the locus of zeros of D (as a Weil divisor); as a mnemonic (possibly a correct definition, I can't remember), f such that $(f)+D \geq 0$, i.e $(f)+D$ is effective.

This is a well-defined construction, since $f_i^{-1}/f_j^{-1} \in \mathcal{O}(U_i \cap U_j)^\times$ for all i, j, and is independent of the choice of collection.

Proposition 25.4.5

Let X be an integral scheme. Then the sequence

$$K(X)^\times \xrightarrow{f \mapsto (f)} \mathrm{CDiv}(X) \xrightarrow{D \mapsto \mathcal{O}(D)} \mathrm{Pic}(X) \to 0$$

is exact, e.g $\mathrm{CaCl}(X) \to \mathrm{Pic}(X)$ is an isomorphism.

For the proof, see Hartshorne II, Prop 6.13.

Definition 25.4.6

Let X be an integral scheme, D a Cartier divisor on X. Then $1 \in \mathcal{K}_X$ determines a nonzero rational section 1_D of $\mathcal{O}(D)$, called the *canonical rational section* of $\mathcal{O}(D)$.

Note that $(1_D) = D$, since if D is represented by (U_i, f_i), then $\mathcal{O}(D)|_{U_i} \xrightarrow{\sim} \mathcal{O}_{U_i}$ via $s \mapsto s \times f_i$, so $1_D \mapsto f_i$ for all i, so (1_D) is represented by the collection (U_i, f_i). Also note that D is effective iff 1_D is a global section of $\mathcal{O}(D)$; this follows from the requirement that $(1_D) + D \geq 0$ globally.

Proposition 25.4.7

Let X be an integral scheme, $\mathcal{L}$ a line sheaf on Y, s a nonzero rational section of $\mathcal{L}$, $D = (s)$. Then $\mathcal{O}(D) \cong \mathcal{L}$.

The proof is left as an exercise.

The punch line of this discussion is that we can redo our height machine discussion entirely in terms of divisors: let X be a proper (equivalently, for a variety, complete) variety over a number field or function field k, D a Cartier divisor on X. Then, a height function for D and k is a height function for $\mathcal{O}(D)$ and k. The results of the height machine (Theorem 23.1.5), now given in terms of Cartier divisors, hold with the additional condition that $h_{D_1,k} = h_{D_2,k} + O(1)$ if $D_1 \sim D_2$.

Background for Weil Functions

Let k be a number field, and recall that $h_k(x) = \sum_{\nu \in M_k} \log\max(1, \|x\|_\nu)$ for $x \in k$, which extends to $P \in \mathbb{P}^1(k)$ as

$$h_k(P) = \sum_{\nu \in M_k} \log\max(\|x_0\|_\nu, \|x_1\|_\nu) = \sum_{\nu \in M_k} -\log \frac{\|x_0\|_\nu}{\max(\|x_0\|_\nu, \|x_1\|_\nu)}$$

where the latter equation is valid on $\mathbb{P}^1(k) \setminus \{[0:1]\}$. In the first and third equations for h_k, we have well-defined components (i.e terms in the sum) for each $\nu \in M_k$; in the second equation, we don't (because of the scaling property of $\mathbb{P}^n$). In going from the second to the third equation, we needed to eliminate the point $\infty = [0 : 1]$; this corresponds to working relative to the divisor $D = (\infty)$. We'll see that the summands in the final form of h_k are *Weil functions* for D, and that they sum to give the height $h_{D,k}(P)$ (note that $\mathcal{O}(D) \cong \mathcal{O}(1)$, so $h_{D,k} = h_{\mathcal{O}(1),k} + O(1) = h_k + O(1)$ by normalization).

Definition 25.5.1

Let k be a number field or function field. For all $\nu \in M_k$, $\mathbb{C}_\nu$ is defined to be the completion of $\overline{k}_\nu$ which is the algebraic closure of k_ν (itself the completion of k with respect to ν).

Example 25.5.2

If ν is archimedean, then k_ν is $\mathbb{R}$ or $\mathbb{C}$, $\overline{k}_\nu = \mathbb{C}$, so $\mathbb{C}_\nu = \mathbb{C}$.

Example 25.5.3

If $k = \mathbb{Q}$, $\nu = p$, then $k_\nu = \mathbb{Q}_p$, $\overline{k}_\nu = \overline{\mathbb{Q}}_p$, which is not complete, but its completion $\mathbb{C}_\nu$ is algebraically closed.

The fact that $\overline{\mathbb{Q}}_p$ is not complete shows that completion and algebraic closure do not generally commute. The completion of an algebraically closed field remains algebraically closed.

Math 254B: Arakelov Theory **Spring 2021**

Lectures 20-22: 8-12 March

Professor Paul Vojta Abhishek Shivkumar

Weil Functions

As before, k is a number field or a function field, and X is a variety over k. Recall that $\mathbb{C}_\nu$ is the completion of $\overline{k}_\nu$ at $\nu \in M_k$. Let X be a variety over k. Then $X(M) := \coprod_{\nu \in M_k} X(\mathbb{C}_\nu)$, where M is used to refer to M_k, and a Weil function for a Cartier divisor D on X (relative to k) is a function $\lambda_D : (X \setminus \operatorname{Supp}(D))(M) \to \mathbb{R}$ (satisfying certain conditions, which we will specify below). The restriction $\lambda_D|_{(X\setminus\operatorname{Supp}(D))(\mathbb{C}_\nu)}$ will be denoted $\lambda_{D,\nu}$.

We want to show that $h_{\lambda_D,k} : (X \setminus \operatorname{Supp}(D))(k) \to \mathbb{R}$ given by $P \mapsto \sum_{\nu\in M_k} \lambda_{D,\nu}(P_\nu)$ is equal to $h_{D,k}|_{(X\setminus\operatorname{Supp}(D))(k)} + O(1)$, where P_ν is the point in $X(\mathbb{C}_\nu)$ corresponding to P.

Unclear to me why there is a unique point P_ν corresponding to P.

We know that heights only carry meaningful arithmetic information up to $O(1)$ (in order to have functoriality); similarly, Weil functions will only be meaningful up to some variation, but not $O(1)$, as some will diverge. Recall that the components of the sums

$$h_k(x) = \sum_{\nu\in M_k} \log\max(1, \|x\|_\nu) = \sum_{\nu\in M_k} -\log\frac{\|x_0\|_\nu}{\max(\|x_0\|_\nu, \|x_1\|_\nu)}$$

are Weil functions for $D = (\infty)$. Let $a, b \in k$ with $a \neq 0$. Then $x \mapsto ax + b$ is an automorphism of $\mathbb{A}^1_k$, which extends to an automorphism of $\mathbb{P}^1_k$ taking $[x_0 : x_1]$ to $[x_0 : bx_0 + ax_1]$. This automorphism (call it φ) fixes the point $\infty = [0 : 1]$, so it fixes the divisor $D = (\infty)$, so $h_k(\varphi(P)) = h_k(P) + O(1)$ for all $P \in \mathbb{P}^1_k$.

We want to understand what φ does to the Weil function $-\log\frac{\|x_0\|_\nu}{\max(\|x_0\|_\nu,\|x_1\|_\nu)}$. Restricting to $\mathbb{A}^1$ (since the point ∞ is excluded from our discussion), we have that $\lambda_{D,\nu}(x) = \log\max(1, \|x\|_\nu)$ for all $x \in k$, and

$$\begin{aligned}\lambda_{D,\nu}(\varphi(x)) = \log\max(1, \|ax+b\|_\nu) \le \log\max(1, \|x\|_\nu) +& \\ \log\max(1, \|a\|_\nu) + \log\max(1, \|b\|_\nu) + N_\nu \log 2&\end{aligned}$$

We may similarly expand $\lambda_{D,\nu}(\varphi^{-1}(x))$, and this indicates that we should allow Weil functions to vary up to M_k-constants.

As we'll want to use compactness-type arguments going forward, note that $\mathbb{C}_\nu$ is not locally compact unless ν is archimedean. This follows form the fact that k_ν is infinite, so $\{x \in \mathbb{C}_\nu : \|x\|_\nu \leq 1\}$ has an open cover $\{\{x \in \mathbb{C}_\nu : \|x - y\|_\nu < 1\} : y \in \mathbb{C}_\nu, \|y\|_\nu \leq 1\}$ with no finite subcover.

Definition 26.1.1: ν-topology

Let $\nu \in M_k$. The *ν-topology* on $X(\mathbb{C}_\nu)$ is the coarsest topology such that for all Zariski-open $U \subseteq X$ $U(\mathbb{C}_\nu)$ is open, and, for all $f \in \mathcal{O}_X(U)$, the function $U(\mathbb{C}_\nu) \to \mathbb{C}_\nu$ induced by f is continuous.

Some facts: of ν is archimedean, then the ν-topology is the classical topology on the complex space $X(\mathbb{C})$. If Y is a subscheme of X (open or closed), then the relative topology on $Y(\mathbb{C}_\nu)$ induced by the ν-topology on $X(\mathbb{C}_\nu)$ is the same as the ν-topology on $Y(\mathbb{C}_\nu)$. All morphisms $X \to Y$ of varieties over k induce continuous maps $X(\mathbb{C}_\nu) \to Y(\mathbb{C}_\nu)$ in the ν-topology for all ν. For any open affine $U = \operatorname{Spec} A$ in X and any isomorphism $A \cong k[x_1, \cdots, x_n]/I$ over k, the ν-topology on $U(\mathbb{C}_\nu)$ is the same as the topology induced by the product topology on $\mathbb{A}^n(\mathbb{C}_\nu)$. The ν-topology on $\mathbb{A}^n(\mathbb{C}_\nu)$ is the same as the product topology on $\mathbb{C}_\nu^n$.

These facts about the ν-topology are stated probably out of order.

Proposition 26.1.2

If U is a dense open subset of X (in the Zariski topology), then $U(\mathbb{C}_\nu)$ is a dense open subset of $X(\mathbb{C}_\nu)$ (in the ν-topology).

Proof: We may assume that X is integral and affine, $X = \operatorname{Spec} A$. By Noether normalization, there exist $y_1, \cdots, y_d \in A$ such that $d = \dim A = \dim X$, and A is finite over $k[y_1, \cdots, y_d] \subseteq A$. This gives a finite surjection $\varphi : X \to \mathbb{A}_k^d$ (induced by the inclusion). This morphism is proper, so $\varphi(X \setminus U)$ is closed in $\mathbb{A}_k^d$, and $\varphi((X \setminus U) \times_k \mathbb{C}_\nu)$ is closed in $\mathbb{A}_{\mathbb{C}_\nu}^d$ (in the Zariski topology, and therefore also in the ν-topology). This is equal to $\varphi(X \setminus U) \times_k \mathbb{C}_\nu$, so, for dimension reasons, $\varphi(X \setminus U)(\mathbb{C}_\nu)$ cannot contain an open ball in $\mathbb{C}_\nu^d$, so its complement is dense in the ν-topology. ■

Why may we assume that X is integral and affine? Don't understand the dimension argument at the end of this proof.

As we have noted above, $\mathbb{C}_\nu$ is not locally compact for ν non-archimedean; in fact, for such ν, $\mathbb{C}_\nu$ is totally disconnected. Therefore, continuity is not actually a very useful property on $X(\mathbb{C}_\nu)$. We want some other property $\mathcal{P}$ of functions $X(\mathbb{C}_\nu) \to \mathbb{R}$ satisfying the following criteria:

It's not at all clear why this list of properties is what we want, but I assume it will turn out to be the right set of assumptions to make Weil functions work how we want them to.

1. All functions $X(\mathbb{C}_\nu) \to \mathbb{R}$ having property $\mathcal{P}$ are bounded
2. $-\log \|f\|_\nu$ has $\mathcal{P}$ for all $f \in K(X)$, all X
3. $\mathcal{P}$ is closed under addition, subtraction, multiplication, and composition of functions

The topology on $X(M)$ is the disjoint union topology of the ν-topologies on $X(\mathbb{C}_\nu)$ (e.g $U \subseteq X(M)$ is open iff $U \cap X(\mathbb{C}_\nu)$ is open in the ν-topology for all ν). For $P \in X(M)$, let $\nu(P)$ denote the unique $\nu \in M_k$ for which $P \in X(\mathbb{C}_\nu)$, and let $\|f(P)\|$ denote $\|f(P)\|_{\nu(P)}$ for all $P \in X(M)$, $f \in K(X)$.

Definition 26.1.3

Let X be an affine scheme of finite type over k, $x_1, \cdots, x_n$ a system of generators for the affine ring $\mathcal{O}(X)$ over k, γ an M_k-constant. Then set

$$B(X, x_1, \cdots, x_n, \gamma) = \{P \in X(M) : \log \|x_i(P)\| \leq \gamma_{\nu(P)} \text{ for all } i\}$$

For all $\nu \in M_k^\infty$, $B(X, x_1, \cdots, x_n, \gamma) \cap X(\mathbb{C}_\nu)$ is a bounded subset of $\mathbb{C}^n$, and all bounded subsets of $\mathbb{C}^n$ are contained in such intersections for some γ (fixing the x_i). Up to containment, this captures all bounded subsets of $X(\mathbb{C}_\nu)$, all $\nu \in M_k^\infty$.

At this point, we are now considering k to be a number field, a function field (in one variable as always), or a completed field E_ν where E is a number field or function field. For fields of this type, $M_{E_\nu} = \{\nu\}$, and M_{E_ν}-constants are just constants.

Definition 26.1.4

Let U be an open affine subset of X (not necessarily affine), $x_1, \cdots, x_n$ a system of generators for $\mathcal{O}(U)$ over k. A subset $E \subseteq X(M)$ is said to be *affine M-bounded* with respect to U and the x_i if $E \subseteq B(U, x_1, \cdots, x_n, \gamma)$ for some M_k-constant γ. E is affine M-bounded with respect to U if there exist x_i generating $\mathcal{O}(U)$ s.t the above criterion is satisfied.

Lemma 26.1.5

Let $V \subseteq U$ be open affine subsets of X, $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$ systems of generators for $\mathcal{O}(U)$ and $\mathcal{O}(V)$ respectively, over k. Then any affine M-bounded set with respect to V and the y_i is also M-bounded w.r.t U and the x_i.

Proof: Since $V \subseteq U$, $\mathcal{O}(U) \subseteq \mathcal{O}(V)$, so there exist polynomials $f_1, \cdots, f_n \in k[Y_1, \cdots, Y_m]$ s.t $x_i = f_i(y_1, \cdots, y_m)$ for all i. If E is affine M-bounded w.r.t V and the y_i, $E \subseteq B(V, y_1, \cdots, y_m, \gamma)$ for some M_k-constant γ. Therefore, $\|y_j(P)\| \leq e^{\gamma_{\nu(P)}}$ for all $P \in E$, all j, so that

$$\|x_i(P)\| = \|f_i(y_1(P), \cdots, y_m(P))\| \leq C_i e^{\deg(f_i)\gamma_{\nu(P)}} \leq e^{d\max(0,\gamma_{\nu(P)})+\gamma'_{\nu(P)}}$$

where $C_i = (\|\text{max coefficient of } f_i\|_{\nu(P)}) \cdot (\text{\# of terms of } f_i)^{N_{\nu(P)}}$, $d = \max_i \deg f_i$, and $\gamma'_\nu = \log \max_i C_i$. Therefore, $E \subseteq B(U, x_1, \cdots, x_n, d\max(0, \gamma) + \gamma')$.
■

Note that this lemma implies that the condition of being affine M-bounded with respect to U is independent of the choice of a finite generating set for $\mathcal{O}(U)$ over k (by taking $V = U$ in the above argument).

For intuition, when $k = \mathbb{C}$, a subset E of $X(\mathbb{C})$ is affine M-bounded with respect to an open affine $U \subseteq X$ iff the closure of E in $U(\mathbb{C})$ is compact.

Definition 26.1.6

Let $E \subseteq X(M)$. Given open affine subsets $U_1, \cdots, U_n$ of X, we say that E is M-bounded with respect to $U_1, \cdots, U_n$ if there is a decomposition $E = E_1 \cup \cdots \cup E_n$ where E_i is affine M-bounded with respect to U_i for all i. Fixing E, if there exist such U_i as described, then we say that E is M-bounded (without qualification).

This definition borders on meaninglessness for me. Hopefully this has some reasonable motivation that we'll discuss.

Example 26.1.7

Let $X = \mathbb{P}^n_k$. Then $X(M)$ is M-bounded.

Proof: Let $U_i = D_+(x_i)$ for $i = 0, \cdots, n$ be the standard open affine cover of $\mathbb{P}^n_k$. Let $P = [a_0 : \cdots : a_n] \in X(M)$, and pick $j \in \{0, \cdots, n\}$ such that $\|a_j\|_{\nu(P)} = \max(\|a_0\|_{\nu(P)}, \cdots, \|a_n\|_{\nu(P)})$. Then $\|(x_i/x_j)(P)\| \leq 1$ for all i, so $P \in B(U_j, x_0/x_j, \cdots, x_n/x_j, 0)$ and

$$X(M) \subseteq \bigcup_{j=0^n} B(U_j, x_0/x_j, \cdots, x_n/x_j, 0)$$

so $X(M)$ is M-bounded. ■

Example 26.1.8

Let Y be a variety over k and $X = \mathbb{P}^n_Y = \mathbb{P}^n_k \times_k Y$ for some $n \in \mathbb{N}$. Let $f : X \to Y$ be the canonical projection. If $E \subseteq Y(M)$ is M-bounded, then so is $f^{-1}(E)$ as a subset of $X(M)$.

Proof: It suffices to show that if E' is an affine M-bounded subset of Y with respect to some open affine $U \subseteq Y$, then $f^{-1}(E')$ is an M-bounded subset of $X(M)$. This follows as above (using the standard open affine cover), and the details are omitted here. ■

Theorem 26.1.9

Let U_i and V_j be two open affine covers of X. Then a subset E of $X(M)$ is M-bounded w.r.t the U_i iff it is M-bounded w.r.t the V_j.

This proof is only a sketch, and is completely meaningless to me. I don't know why being M-bounded is a meaningful adjective. Detailed proofs are in the handouts on Vojta's website.

Proof: In the case that X is affine, $n = 1$, $U_1 = X$, and the V_i are principal open affines $D(f_1), \cdots, D(f_m)$ with $f_i \in \mathcal{O}(X)$. The proof in this case is a homework exercise. If X is affine, $n = 1$, $U_1 = X$ and $V_1, \cdots, V_m$ are arbitrary open affines, then if E is affine M-bounded w.r.t the V_i, then it is affine M-bounded with respect to X by a previous lemma. In the other direction, we may reduce to the first case by covering each V_j with finitely many open affines (since the $D(f_i)$ form a base for the Zariski topology on X).

In the general case, we may reduce to the second case (where the V_i are general) by noting that $U_i \cap V_j$ is affine for all i, j (since X is separated), so $U_i \cap V_1, \cdots, U_i \cap V_m$ is an open affine cover of U_i for all i, and similarly $U_1 \cap V_j, \cdots, U_n \cap V_j$ is an open affine cover of V_j for all j. ■

Corollary 26.1.10

To verify that $E \subseteq X(M)$ is M-bounded, it suffices to check the condition for any open affine cover of X.

Corollary 26.1.11

Suppose X is affine. Then $E \subseteq X(M)$ is M-bounded iff it is M-bounded w.r.t X.

Proposition 26.1.12

Let $f : X \to Y$ be a morphism of k-varieties. If $E \subseteq X(M)$ is M-bounded, then so is its image $f(E) \subseteq Y(M)$.

Again, a sketch of a proof here.

Proof: Reduce to the case where Y and X are both affine, say $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, f corresponding to $\varphi : B \to A$. Let $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$ be systems of generators for A and B respectively, as k-algebras. Assume that $n \geq m$ and $x_i = \varphi(y_i)$ for all $i \leq m$. Then $E \subseteq B(X, x_1, \cdots, x_n, \gamma) \implies f(E) \subseteq B(Y, y_1, \cdots, y_m, \gamma)$. ■

We will state, without a full proof, some other facts about M-boundedness: if $f : X \to Y$ is proper and $E \subseteq Y(M)$ is M-bounded, then so is $f^{-1}(E)$ (when f is projective, we have already shown in a previous example that this holds over open affines of Y, hence over Y; in general, we use Chow's lemma and the above proposition). M-boundedness is preserved by subsets (hence by closed immersions), e.g, if E is M-bounded, then so is any subset of E. If $Y \subseteq X$ is a closed subvariety and $E \subseteq Y(M)$ is M-bounded as a subset of $X(M)$, then it is also M-bounded as a subset of $Y(M)$. The same holds for open immersions. M-boundedness is preserved under finite unions.

$f(E)$ is an abuse of notation since f is technically only defined on X; however, it has an obvious interpretation as the union of $\nu \in M_k$ of the base changes. In particular

$$f(E) := \cup_{\nu \in M_k} f_\nu(E \cap X(\mathbb{C}_\nu))$$

Let $\overline{\mathbb{R}}$ denote the extended real numbers with ±∞ adjoined, along with the obvious ordering.

Definition 26.1.13

Let $f : X(M) \to \overline{\mathbb{R}}$ be a function. We say that f is *locally M-bounded from below* if for all M-bounded subsets E of $X(M)$ there is an M_k-constant γ (valued in $\mathbb{R}$, not $\overline{\mathbb{R}}$) such that $f(P) \geq \gamma_{\nu(P)}$ for all $P \in E$. Locally M-bounded from above and locally M-bounded are defined similarly, *mutatis mutandis*.

Proposition 26.1.14

Let $f \in \mathcal{O}(X)$. Then the function $-\log \|f\| : X(M) \to \overline{\mathbb{R}}$ (with the convention $-\log 0 = +\infty$) is locally M-bounded from below. If $f \in \mathcal{O}(X)^\times$, then $-\log \|f\|$ is locally M-bounded.

Proof: Let $E \subseteq X(M)$ be an M-bounded set, $U_1, \cdots, U_n$ an affine open cover of X, and $E = E_1 \cup \cdots \cup E_n$ where E_i is affine M-bounded w.r.t U_i. We may therefore reduce to the affine case $X = U_i$. Then $E \subseteq B(X, x_1, \cdots, x_n, \gamma)$ for some x_i generating $\mathcal{O}(X)$ as a k-algebra and some M_k-constant γ. We may assume that $x_m = f$, so (by definition of $B(\cdots)$) $-\log \|f(P)\| \geq -\gamma_{\nu(P)}$ for all $P \in E$. With the first assertion shown, the second assertion by repeating this argument with $\frac{1}{f}$ in the place of f. ■

We are finally ready to define Weil functions:

Definition 26.1.15: Weil Functions

Let X be a variety over k. A *Weil function* on X is a pair (D, λ), where D is a Cartier divisor on X and $\lambda : (X \setminus \operatorname{Supp} D)(M) \to \mathbb{R}$ is a function that satisfies the following condition: there exists a collection (U_i, f_i) representing D and continuous locally M-bounded functions $\alpha_i : U_i(M) \to \mathbb{R}$ such that $\lambda(P) = -\log \|f_i(P)\| + \alpha_i(P)$ for all $P \in (U_i \setminus \operatorname{Supp} D)(M)$.

Incredibly contrived definition. No idea why it's useful.

We will usually refer to a Weil function (D, λ) by its component λ, usually written λ_D, and we will write $\lambda_{D,\nu}$ to denote $\lambda_D|_{(X \setminus \operatorname{Supp} D)(\mathbb{C}_\nu)}$.

The intuition we should have for Weil functions is that $\lambda_{D,\nu}$ grows like $-\log \|f_i\|_\nu$ near $\operatorname{Supp}(D)$ on $U_i(\mathbb{C}_\nu)$ for all i and ν, but with uniformity as ν varies (which is hard to describe).

Example 26.1.16

Let $f \in K(X)^\times$. Then the function $-\log \|f\|$ defines a Weil function for the principal divisor (f). It is called the principal Weil function for f.

Math 254B: Arakelov Theory **Spring 2021**

Lectures 23-25: 15-19 March

Professor Paul Vojta Abhishek Shivkumar

More on Weil Functions

As before, k is a number field, a function field, or the completion of a number field or function field. Recall Definition 26.1.15: we will primarily be discussing this definition today. Note that we usually restrict to X complete or projective, for certain technical reasons. Let L be a finite extension of k; if k is of the third type (the completion of a number field or function field), then L is also of this type. For all $\omega \in M_L$ and $\nu \in M_k$ with $\omega | \nu$, we have $\mathbb{C}_\omega \cong \mathbb{C}_\nu$ canonically (possibly with different norms), so we will identify $X_L(\mathbb{C}_\omega)$ with $X(\mathbb{C}_\nu)$ in the obvious way, and define $\lambda_{D,\omega} = [L_\omega : k_\nu]\lambda_{D,\nu}$ for all Weil functions λ_D, which produces a Weil function over L.

Still don't know why I am supposed to care about Weil functions. This has just been an endless chain of absurd adjectives and properties.

Proposition 27.1.1

Let (D, λ) be a Weil function on X, U an open subset of X, $f \in K(X)^\times$. Assume that $D|_U = (f)|_U$; then the function $\lambda + \log \|f\|$ on $(U \setminus \operatorname{Supp}(D))(M)$ extends uniquely to a continuous locally M-bounded function $\beta : U(M) \to \mathbb{R}$.

Proof: Let (U_i, f_i) and α_i represent (D, λ). For each i, $f_i/f \in \mathcal{O}(U \cap U_i)^\times$, so $-\log \|f_i/f\|$ is continuous and locally M-bounded on $(U \cap U_i)(M)$, as is $\alpha_i - \log \|f_i/f\|$. Also, for all P in $((U \cap U_i) \setminus \operatorname{Supp}(D))(M)$,

$$\alpha_i(P) - \log \|f_i(P)/f(P)\| = \alpha_i(P) - \log \|f_i(P)\| + \log \|f(P)\| = \lambda(P) + \log \|f(P)\|$$

so $\lambda + \log \|f\|$ extends to a continuous locally M-bounded function β_i on $(U \cap U_i)(M)$. This extension is unique since $(U \cap U_i) \setminus \operatorname{Supp}(D)$ is Zariski-dense in $U \cap U_i$, so $((U \cap U_i) \setminus \operatorname{Supp}(D))(M)$ is dense in $(U \cap U_i)(M)$ by a previous result. The β_i are compatible on the intersections of their domains, so they combine to give a unique continuous function $\beta : U(M) \to \mathbb{R}$ which is locally M-bounded as desired. ■

To show that β is locally M-bounded, note that $\beta|_{U_i(M)}$ is locally M-bounded for all i, and assume that all U_i are affine. Pass to a finite subcover of X; if $E \subseteq X(M)$ is M-bounded, then it is M-bounded w.r.t the U_i, and the rest is clear.

Corollary 27.1.2

If (D, λ) is a Weil function, then it satisfies the condition in the definition of Weil functions for all collections (U_i, f_i) representing D (e.g, the property of being a Weil function does not depend on any specific open cover representing D).

Properties of Weil Functions

Weil functions are additive, in the sense that if (D_1, λ_1) and (D_2, λ_2) are Weil functions on X, there is a natural way in which $(D_1 + D_2, \lambda_1 + \lambda_2)$ is also a Weil function on X. There is a slight problem here, in that the domain of $\lambda_1 + \lambda_2$ is $(X \setminus (\mathrm{Supp}(D_1) \cup \mathrm{Supp}(D_2)))(M)$ which may be a proper subset of $(X \setminus \mathrm{Supp}(D_1 + D_2))(M)$. For example, if X is regular, some prime divisors in D_1 may cancel in $D_1 + D_2$, when regarded as Weil divisors. To remedy this situation, we have the following lemma:

Lemma 27.2.1

Let $U \subseteq X$ be a dense open subset, $\lambda_0 : U(M) \to \mathbb{R}$ a function, D a Cartier divisor on X. Assume that $U \cap \mathrm{Supp}(D) = \emptyset$ and that there exists a collection (U_i, f_i) representing D such that the function $(\lambda_0 + \log \|f_i\|) : (U \cap U_i)(M) \to \mathbb{R}$ extends to a continuous locally M-bounded function $\alpha_i : U_i(M) \to \mathbb{R}$. Then λ_0 extends uniquely to a function $\lambda : (X \setminus \mathrm{Supp}(D))(M) \to \mathbb{R}$ such that (D, λ) is a Weil function.

The proof is left as an exercise, and is similar to the proof of the previous proposition.

Proposition 27.2.2

Let (D_1, λ_1) and (D_2, λ_2) be Weil functions on X. Then $\lambda_1 + \lambda_2 : (X \setminus (\mathrm{Supp}(D_1) \cup \mathrm{Supp}(D_2))(M) \to \mathbb{R}$ extends uniquely to a function $\lambda : (X \setminus \mathrm{Supp}(D_1 + D_2))(M) \to \mathbb{R}$ such that $(D_1 + D_2, \lambda)$ is a Weil function.

This follows directly from the previous lemma.

Weil functions are functorial, in the sense that if $f : X \to Y$ is a morphism of varieties, (D, λ) a Weil function on Y, with $f(X) \not\subseteq \mathrm{Supp}(D)$, then $(f^*D, \lambda \circ f)$ extends uniquely to a Weil function on X.

Proof: We apply the above lemma, and use the fact that if $V \subseteq Y$ is open, and $\alpha : V(M) \to \mathbb{R}$ is continuous and locally M-bounded, then $\alpha \circ f : f^{-1}(V)(M) \to \mathbb{R}$ is also continuous and locally M-bounded, which in turn uses the fact that if E is an M-bounded subset of $f^{-1}(V)(M)$, then $f(E)$ is an M-bounded subset of $V(M)$ (via some abuse of notation). ■

Weil functions additionally satisfy the criterion of normalization, meaning that on $X = \mathbb{P}^n_k$, with $n > 0$, $D = \mathrm{div}_{\mathcal{O}(1)}(x_0)$, with $\lambda : (D_+(x_0))(M) \to \mathbb{R}$ given by $-\log \frac{\|x_0\|}{\max(\|x_0\|,\cdots,\|x_n\|)}$ (which is independent of the choice of homogeneous coordinates $[x_0 : \cdots : x_n]$), we have that (D, λ) is a Weil function. To see this, let (U_i, f_i) be given by $U_i = D_+(x_i)$ and $f_i = \frac{x_0}{x_i}$ representing D. We want to show that

$$\lambda([x_0 : \cdots : x_n]) + \log \left\| \frac{x_0}{x_i} \right\| = \max_j - \log \left\| \frac{x_i}{x_j} \right\|$$

is continuous and locally M-bounded on $U_i(M)$ for all i. Here, each function $-\log\left\|\frac{x_i}{x_j}\right\|$ is continuous and locally M-bounded from above on $U_i(M)$ (regarded as a function from $U_i(M)$ to $\mathbb{R}\cup\{-\infty\}$), and locally M-bounded on $(U_i\cap U_j)(M)$. We want the following lemma:

Here, $\overline{\mathbb{R}}$ refers to $\mathbb{R}\cup\{\pm\infty\}$.

Lemma 27.2.3

Let $V_1,\cdots,V_m$ be an open cover of a variety Y over k, and let $f_1,\cdots,f_m : Y(M)\to\overline{\mathbb{R}}$ be functions such that f_j is locally bounded from above for all j, and $f_j|_{V_j(M)}$ is locally bounded. Let $f = \max_i f_i$, then f is locally M-bounded.

The proof will be given as a homework exercise.

Applying this lemma with $Y = U_i$ for all i, the normalization criterion follows.

Finally, note that $((f), -\log\|f\|)$ is a Weil function on X for all $f\in K(X)^\times$, so Weil functions in fact satisfy all of the properties of our height functions from the height machine.

Proposition 27.2.4: Linear Equivalence

Let (D_1,λ_1) and (D_2,λ_2) be Weil functions on X, with $D_1\sim D_2$, say $D_1-D_2=(f)$ for some $f\in K(X)^\times$. Then $\lambda_1-\lambda_2+\log\|f\|$ extends uniquely to a continuous locally M-bounded function on $X(M)$.

Proof: By linearity, $\lambda_1-\lambda_2+\log\|f\|$ extends uniquely to a function $\lambda : X(M)\to\mathbb{R}$ such that $(0,\lambda)$ is a Weil function. The Cartier divisor 0 is represented by the single element collection $(X,1)$, so by the definition of Weil functions, λ is continuous and locally M-bounded on $X(M)$. ■

In this corollary, M_k-constants are regarded as functions on $X(M)$ where $\gamma(P)=\gamma_\nu$ for all $P\in X(\mathbb{C}_\nu)$.

Corollary 27.2.5

If X is a complete variety (so $X\to\operatorname{Spec}k$ is proper), (D,λ_1), (D,λ_2) Weil functions on X, then there exist M_k-constants γ and γ' such that $-\gamma'\le\lambda_1-\lambda_2\le\gamma$ on $(X\setminus\operatorname{Supp}D)(M)$.

Proof: By the linear equivalence property with $f=1$, $\lambda_1-\lambda_2$ extends to a continuous locally M-bounded function $\lambda : X(M)\to\mathbb{R}$. Since $X\to\operatorname{Spec}k$ is proper, and $(\operatorname{Spec}k)(M)$ is affine M-bounded (since it is contained in $B(\operatorname{Spec}k,1,0)$), $X(M)$ is M-bounded, so we get γ and γ' straight from the definition of the locally M-bounded function λ. ■

Definition 27.2.6

Let $\lambda : X(M)\to\overline{\mathbb{R}}$ be a function. We say that $\lambda = O_{M_k}(1)$ if there exist M_k-constants γ,γ' such that

$$-\gamma'_{\nu(P)}\le\lambda(P)\le\gamma_{\nu(P)}$$

for all $P \in X(M)$, e.g, $-\gamma' \le \lambda \le \gamma$. We say that $\lambda \le O_{M_k}(1)$ if $\lambda \le \gamma$ for some M_k-constant γ, and similarly define the condition $\lambda \ge O_{M_k}(1)$.

In this language, the above corollary states that $\lambda_2 - \lambda_1 = O_{M_k}(1)$.

Weil Functions and Heights

Definition 27.3.1

Let (D, λ) be a Weil function on X (usually complete), $P \in (X \setminus \operatorname{Supp} D)(k)$, $\nu \in M_k$. Then the point $P_\nu \in (X \setminus \operatorname{Supp} D)(\mathbb{C}_\nu)$ is the point given by the composite morphism $\operatorname{Spec} \mathbb{C}_\nu \to \operatorname{Spec} k \to X \setminus \operatorname{Supp} D$ over k.

Moreover, if L is a finite extension of k, $P \in (X \setminus \operatorname{Supp} D)(L)$, $\omega \in M_L$, then the composite function $\operatorname{Spec} \mathbb{C}_\omega \to \operatorname{Spec} L \to X \setminus \operatorname{Supp} D$ over k defines a point $P_\omega \in (X \setminus \operatorname{Supp} D)(\mathbb{C}_\omega)$, and we write $\lambda_\omega(P) = \lambda(P_\omega)$.

Vojta says something about how D was unnecessary for this discussion, and we could've had $P \in X(k)$ or $X(L)$ respectively. I don't understand where we get a morphism $\operatorname{Spec} k \to X$.

Definition 27.3.2

Let k be a number field or a function field, and let (D, λ) be a Weil function on X. Let $P \in (X \setminus \operatorname{Supp} D)(\overline{k})$, and choose a finite extension L of k such that $P \in (X \setminus \operatorname{Supp} D)(L)$. Then we define

$$h^\circ_{\lambda,k}(P) = \frac{1}{[L:k]} \sum_{\omega \in M_L} \lambda_\omega(P)$$

If L' is a finite extension of L, $\omega \in M_L$, then $\lambda_{\omega'} = [L'_{\omega'}, L_\omega]\lambda_\omega$ for all $\omega' \in M_{L'}$ lying over ω, so

$$\sum_{\substack{\omega' \in M_{L'} \\ \omega' | \omega}} \lambda_{\omega'}(P) = \sum_{\substack{\omega' \in M_{L'} \\ \omega' | \omega}} [L'_{\omega'} : L_\omega]\lambda_\omega(P) = [L' : L]\lambda_\omega(P)$$

so the value $h^\circ_{\lambda,k}(P)$ does not depend on the choice of L.

We have been doing variations of this definition for forty pages.

If (D, λ_1) and (D, λ_2) are Weil functions (with the same divisor D), and X is complete, then $-\gamma' \le \lambda_1 - \lambda_2 \le \gamma$ for some M_k-constants γ and γ', and therefore $-|\gamma'| \le h^\circ_{\lambda_1,k} - h^\circ_{\lambda_2,k} \le |\gamma|$ by summing over these inequalities. Therefore, $h^\circ_{\lambda_1,k} = h^\circ_{\lambda_2,k} + O(1)$.

Lemma 27.3.3

Let k (a number or function field), X, and (D, λ) be as above, $f \in K(X)^\times$. Let $(D+(f), \lambda')$ be the Weil function uniquely determined by $\lambda' = \lambda - \log \|f\|$. Then $h^\circ_{\lambda,k}(P) = h^\circ_{\lambda',k}(P)$ for all $P \in (X \setminus (\operatorname{Supp} D \cup \operatorname{Supp}(f))(\overline{k})$ (with no $O(1)$ term).

The proof boils down to applying the product formula on $f(P)$.

Definition 27.3.4

Let k, X, and (D, λ) be as above, $P \in X(\overline{k})$, $f \in K(X)^\times$ s.t $P \notin \operatorname{Supp}(D+(f))$. Let $(D+(f), \lambda')$ be the Weil function corresponding to the sum $(D, \lambda) + ((f), -\log \|f\|)$ on X and define $h_{\lambda,k}(P) = h^\circ_{\lambda',k}(P)$. This is independent of the choice of f by the above lemma, and produces a function $h_{\lambda,k} : X(\overline{k}) \to \mathbb{R}$.

Proposition 27.3.5: Normalization

Let $X = \mathbb{P}^n_k$, $D = (x_0)$, $\lambda(P) = -\log \frac{\|x_0\|}{\max(\|x_0\|, \cdots, \|x_n\|)}$ for all $P \in (X \setminus \operatorname{Supp} D)(M)$. Then $h_{\lambda,k} = h_k$.

Proposition 27.3.6: Linear Equivalence

If (D_1, λ_1) and (D_2, λ_2) are Weil functions on X, $D_1 \sim D_2$, then $h_{\lambda_1,k} = h_{\lambda_2,k} + O(1)$. Moreover, if $\lambda_2 = \lambda_1 - \log \|f\|$ where $D_2 = D_1 + (f)$ $(f \in K(X)^\times)$, then $h_{\lambda_1,k} = h_{\lambda_2,k}$ with no $O(1)$.

Proof: The first assertion follows from the fact that $\lambda_1 = \lambda_2 + O_{M_k}(1)$ (which we proved earlier). The second assertion follows from the above lemma. ■

The proofs of functoriality and additivity (the remaining properties from the height machine) are left as exercises (these results do not have $O(1)$ terms). Next, we want to show that Weil functions relative to a given divisor exist.

Theorem 27.3.7: Existence

Let X be a projective variety over k and let D be a Cartier divisor on X. Then there is a function $\lambda : (X \setminus \operatorname{Supp} D)(M) \to \mathbb{R}$ such that (D, λ) is a Weil function.

Proof: By a previous lemma, we may write $\mathcal{O}(D) \cong \mathcal{M} \otimes \mathcal{N}^\vee$ where $\mathcal{M}$ and $\mathcal{N}$ are gbgs line sheaves on X. Let $\underline{s} = (s_0, \cdots, s_n)$ and $\underline{t} = (t_0, \cdots, t_m)$ be generating systems of global sections for $\mathcal{M}$ and $\mathcal{N}$ respectively. Assume that s_0 and t_0 are not identically zero, and let $\Phi_{\underline{s}} = [s_0 : \cdots : s_n] : X \to \mathbb{P}^n_k$. Then $\Phi^*_{\underline{s}}\mathcal{O}(1) \cong \mathcal{M}$ and $\Phi_{\underline{s}}(x) \nsubseteq \operatorname{Supp}(x_0)$, so the Weil function $-\log \frac{\|x_0\|}{\max(\|x_0\|, \cdots, \|x_n\|)}$ on $\mathbb{P}^n_k$ pulls back to give a Weil function (D_1, λ_1) on X, where $D_1 = (s_0)$. Similarly, we may obtain (D_2, λ_2) on X with

$\underline{t}$, where $D_2 = (t_0)$. Since $\mathcal{O}(D) \cong \mathcal{M} \otimes \mathcal{N}^\vee$, we have $D \sim D_1 - D_2$ so $D = D_1 - D_2 + (f)$ for some $f \in K(X)^\times$. By additivity of Weil functions, $\lambda_1 - \lambda_2 - \log \|f\|$ extends to a function $\lambda : (X \setminus \operatorname{Supp} D)(M) \to \mathbb{R}$ such that (D, λ) is a Weil function on X as desired. ■

Corollary 27.3.8

By the height machine for divisors, if (D, λ) is a Weil function on X, then $h_{\lambda,k}$ is a height function for D, for all projective varieties X over k.

Since

$$-\log \frac{\|x_0\|}{\max(\|x_0\|, \cdots, \|x_n\|)} = \max\left\{-\log \left\|\frac{x_0}{x_i}\right\| : 0 \le i \le n\right\}$$

we have that

$$\lambda_1 = \max\left\{-\log \left\|\frac{s_0}{s_i}\right\| : 0 \le i \le n\right\} \text{ and } \lambda_2 = \max\left\{-\log \left\|\frac{t_0}{t_j}\right\| : 0 \le i \le m\right\}$$

in the above proof; this combines to give

$$\lambda = \min_j \max_i \left(-\log \left\|f \frac{s_0}{s_i} \frac{t_j}{t_0}\right\|\right)$$

Since $D = D - 1 - D - 2 + (f) = (s_0) - (t_0) + (f) = \left(\frac{fs_0}{t_0}\right)$, we can let $1_D = \frac{fs_0}{t_0}$ (with $(1_D) = D$), so that

$$\lambda = \min_j \max_i \left(-\log \left\|\frac{1_D t_j}{s_i}\right\|\right)$$

Theorem 27.3.9: min-max

Let D be a Cartier divisor on a projective variety X over k. Then there exist effective Cartier divisors $X_1, \cdots, X_n$, $Y_1, \cdots, Y_m$ on X such that $\cap_i \operatorname{Supp} X_i = \cap_j \operatorname{Supp} Y_j = \emptyset$ and $D + X_i \sim Y_j$ for all i, j. Moreover, for any such collection of X_i and Y_j, $f_{ij} \in K(X)^\times$ such that $(f_{ij}) = D + X_i - Y_j$, then the function $\lambda = \min_i \max_j(-\log \|f_{ij}\|)$ extends to a function $\lambda : (X \setminus \operatorname{Supp} D)(M) \to \mathbb{R}$ such that (D, λ) is a Weil function on X.

Theorem 27.3.10

Let X be a variety over k, D, and $D_1, \cdots, D_n$ Cartier divisors on X. Assume that $D_i - D$ is effective for all i, and $\cap_i \operatorname{Supp}(D_i - D) = \emptyset$. Let $\lambda_1, \cdots, \lambda_n$ be Weil functions for $D_1, \cdots, D_n$ respectively. Then $\min_i \lambda_i$ is a Weil function for D.

The proof is in a handout.

Math 254B: Arakelov Theory **Spring 2021**

Lecture 26-31: 29 March - 9 April

Professor Paul Vojta Abhishek Shivkumar

Even More on Weil Functions

Not really a definition but my own shorthand: a *Vojta field* is a number field, function field, or a completion of a number field or function field at a place.

Proposition 28.1.1

Let X be a proper variety over k a Vojta field, (D, λ) a Weil function on X. Assume that the (Cartier) divisor D is effective. Then $\lambda \geq -O_{M_k}(1)$.

Proof: Let (U_i, f_i) represent D, and assume that the set I is finite. For all i, we have $\lambda(P) = -\log \|f_i(P)\| + \alpha_i(P)$ with $\alpha_i : U_i(M) \to \mathbb{R}$ continuous and locally M-bounded. Since D is effective, $f_i \in \mathcal{O}(U_i)$, so $-\log \|f_i\|$ is locally M-bounded from below on $U_i(M)$; therefore, $\lambda|_{U_i(M)}$ extended to a function $U_i(M) \to \mathbb{R} \cup \{\infty\}$ is locally M-bounded from below. Therefore, λ (extended to a function $X(M) \to \mathbb{R} \cup \{\infty\}$) is locally M-bounded from below, so, since X is complete, $\lambda \geq -\gamma$ for some M_k-constant γ. ■

Corollary 28.1.2

For such (D, λ), $h_{\lambda,k} \geq -O(1)$ for all $P \in (X \setminus \operatorname{Supp} D)(\overline{k})$.

This also shows why $h_{\mathcal{L},k}(P) \geq -O(1)$ for all $P \in X(\overline{k})$ outside of the base locus of $\mathcal{L}$, which is the positivity property of heights.

Proposition 28.1.3

Let (D, λ) be a Weil function on a normal variety X. Then if $\lambda \geq O_{M_k}(1)$, then D is effective. Moreover, if $\lambda = O_{M_k}(1)$, then $D = 0$.

Proof: The proof of the first part is in a handout; the second part follows by applying the first part to (D, λ) and $(-D, -\lambda)$. ■

Example 28.1.4

Let X be the affine curve $y^2 = x^3$ (e.g the cuspidal cubic), and let $\overline{X}$ be its projective closure in $\mathbb{P}^2_k$ given by $y^2 z = x^3$ in homogeneous coordinates. Let $f = 1 + \frac{y}{x} \in K(X)$, $D = (f)$, $\lambda = -\log \|f\|$. Then (D, f) is a Weil function on $\overline{X}$. Since $\overline{X} \setminus X$ is a single point $[0 : 1 : 0]$, we will use affine coordinates to refer to points on X and ∞ to refer to $[0 : 1 : 0]$.

Note that f vanishes at $(1, -1)$, and that this is a simple zero, because $\left(1-\frac{y}{x}\right)f = 1-\frac{y^2}{x^2} = 1-x$ and $1-\frac{y}{x}$ does not vanish at $(1,-1)$. f has a pole at ∞, which is similarly a simple pole. f is undefined at $(0,0)$. Let D' be the Cartier divisor represented by $\{(V_1, f), (V_2, 1)\}$, where $V_1 = \overline{X} \setminus \{(0,0)\}$ and $V_2 = \overline{X} \setminus \{(1,-1), \infty\}$. $D \neq D'$ since D may be represented by $\{(V_1, f), (V_2, f)\}$, and $f \notin \mathcal{O}_{\overline{X}}(V_2)^\times$ (due to being undefined at $(0,0)$). We claim that λ is a Weil function for D'.

On V_1, this is trivial since $\alpha_1 = 0$. On V_2, we must show that $-\log\|f\|$ is continuous and locally M-bounded. The normalization of X is $\tilde{X} = \mathbb{A}^1_k$, via the map $t \mapsto (t^2, t^3)$ inducing a map $\mathbb{A}^1_k = \operatorname{Spec} k[t] \xrightarrow{\varphi} X$, where f pulls back to $1+t$. Now $\varphi^{-1}(V_2) = \mathbb{A}^1_k \setminus \{t = -1\} = \operatorname{Spec} k\left[t, \frac{1}{1+t}\right]$, so $\varphi^* f \in \mathcal{O}_{\tilde{X}}(\varphi^{-1}(V_2))^\times = k\left[t, \frac{1}{1+t}\right]^\times$. Therefore, $-\log\|\varphi^* f\|$ is continuous and locally M-bounded on $\varphi^{-1}(V_2)(M)$, so $-\log\|f\|$ is continuous (because $\varphi_\nu : (\varphi^{-1}(V_2))(\mathbb{C}_\nu) \to V_2(\mathbb{C}_\nu)$ is a homeomorphism in the ν-topology for all ν), and locally M-bounded (since φ is finite and therefore proper). Therefore, both (D, λ) and (D', λ) are Weil functions on $\overline{X}$, but $D \neq D'$. Since the normalization of X is $\operatorname{Spec} k[t]$, the divisors D and D' both pull back to the divisor $t = -1$ on $\mathbb{A}^1_k$.

Proposition 28.1.5

Let X be a complete variety over a number field or function field k, (D, λ_1) and (D, λ_2) Weil functions on X. Then if $S \subseteq M_k$ is any subset, $\lambda_S := (X \setminus \operatorname{Supp} D)(M) \to \mathbb{R}$ given by

$$\lambda_S(P) = \begin{cases} \lambda_1(P) & \text{if } \nu(P) \notin S \\ \lambda_2(P) & \text{if } \nu(P) \in S \end{cases}$$

Then (D, λ_S) is a Weil function on X. Moreover, the set

$$\{\nu \in M_k : \lambda_1|_{(X \setminus \operatorname{Supp} D)(\mathbb{C}_\nu)}(P) \neq \lambda_2|_{(X \setminus \operatorname{Supp} D)(\mathbb{C}_\nu)}(P)\}$$

is finite.

Proof: The first part is trivial, the second part has already been shown. ∎

Morally, this result and the one below show us how to cut and paste Weil functions.

Proposition 28.1.6

Let X be a complete variety over a number field or function field k, (D, λ) a Weil function on X. Let $\nu \in M_k$, $X_\nu = X \times_k k_\nu$, D_ν the pullback of D to X_ν. We identify $X_\nu(\mathbb{C}_\nu)$ with $X(\mathbb{C}_\nu)$ in the obvious way, so $X_\nu(M) = X_\nu(\mathbb{C}_\nu) = X_\nu(\mathbb{C}_\nu) \subseteq X(M)$ (where $X_\nu(M) = X_\nu(\mathbb{C}_\nu)$ since $M_{k_\nu} = \{\nu\}$). Then $(D_\nu, \lambda|_{X_\nu(M)})$ is a Weil function on X_ν. Moreover, if (D_ν, λ_1) is a Weil function on X_ν, with $\lambda_2 : (X \setminus \operatorname{Supp} D)(M) \to \mathbb{R}$ given by

$$\lambda_2(P) = \begin{cases} \lambda_1(P) & P \in X_\nu(M) \\ \lambda(P) & \text{else} \end{cases}$$

Then (D, λ_2) is a Weil function on X.

Proof: The proof follows immediately from definitions. ■

Models

As shorthand for what follows, if k is a number field, then Y will always refer to $\operatorname{Spec} \mathcal{O}_k$. If k is as function field in one variable over a "constant field" F, then Y is the unique (up to isomorphism) nonsingular projective curve over F, with F-isomorphism $k \xrightarrow{\sim} K(Y)$. If k is a completion of a number field or function field k_0 at a place $\nu \in M_{k_0}$, then Y is understood to be $\operatorname{Spec} A_\nu$ where A_ν is the valuation ring of k_ν if ν is non-archimedean, or $\operatorname{Spec} k$ if ν is archimedean.

The only example I can really keep in my head: $F = \mathbb{Q}$, $k = \mathbb{Q}_p$, $Y = \operatorname{Spec} \mathbb{Z}_p$, with $K(Y) \cong \mathbb{Q}_p$ over $\mathbb{Q}$, and apparently $\operatorname{Spec} \mathbb{Z}_p$ is a curve over $\mathbb{Q}_p$ or $\mathbb{Q}$.

In each of the above cases, $K(Y) \cong k$ (over F, if necessary), canonically. From now on, when considering models, we will exclude $k = \mathbb{R}$ or $k = \mathbb{C}$, in which case $\dim Y = 1$ in all cases.

Definition 28.2.1: Models

Let V be a variety over k. Then a *model* for V over Y is a separated, finite type morphism $\pi : X \to Y$ together with an isomorphism $i : V \xrightarrow{\sim} X_k := X \times_Y \operatorname{Spec} k$ such that all associated points of X lie on X_k (i.e X is integral, X_k is reduced, so X is reduced, and X has only one irreducible component, so only one associated point).

The associated points of a Noetherian scheme X that is reduced or Cohen-Macaulay are just the generic points of irreducible components of X; I don't think we will require anything more general than this.

Definition 28.2.2

A model $\pi : X \to Y$ is projective (resp. proper) if the morphism π is projective (resp. proper). Such models exist only if V is projective (resp. complete).

One may similarly define affine and quasi-projective models.

Example 28.2.3

1. $\mathbb{P}^n_Y$ is a projective model for $\mathbb{P}^n_k$ for all $n \geq 0$.
2. $\mathbb{A}^n_Y$ is a model for $\mathbb{A}^n_k$ for all $n \geq 0$.
3. Let $\mathcal{E}$ be a vector sheaf of rank $n+1$ over Y. Then $\mathbb{P}(\mathcal{E}) = \operatorname{Proj}(\operatorname{Sym} \mathcal{E})$ (as in Hartshorne, not Vakil) is a model for $\mathbb{P}^n_k$.

4. $\mathbb{P}^n_{Y\setminus Z}$ is a model for $\mathbb{P}^n_k$ over Y where Z is a finite set of closed points of Y. It is not projective or proper, unless $Z = \emptyset$.

5. If k is the completion of a number field or function field k_0 at a place $\nu \in M^0_{k_0}$, then $\mathbb{P}^n_k$ is a model for $\mathbb{P}^n_k$ (this is a special case of the above, with Z the closed point of Y since $Y = \operatorname{Spec} k$).

Proposition 28.2.4

If V is a projective variety over k, then it has a projective model.

Proof: Fix a closed embedding $V \subseteq \mathbb{P}^n_k$. Topologically, V is a subset of $\mathbb{P}^n_Y$ via $i : \mathbb{P}^n_k \hookrightarrow \mathbb{P}^n_Y$. Let X be the closure of V in $\mathbb{P}^n_Y$, with reduced induced subscheme structure. Since the topology on $\mathbb{P}^n_k$ is the relative topology from $\mathbb{P}^n_Y$, $X \cap \mathbb{P}^n_k = V$ as sets. Since X is reduced, so is X_k (by looking at the local rings), so $V \to X_k$ is an isomorphism (Hartshorne II Ex. 3.11c). Since X is reduced and has only one irreducible component, it has no associated points other than the generic point of X_k, and is therefore a (projective) model for V. ■

Proposition 28.2.5

Let X be a model (over Y) of a variety V (over k), V' a closed subvariety of V, X' the closure of V' in X (via $i : V \xrightarrow{\sim} X_k$) with reduced induced subscheme structure. Then X' is a model for V'; if the model X is projective (resp. proper), then so is X'.

Proof: For the first assertion, the same proof as above works, and the second assertion is immediate. ■

Corollary 28.2.6

Any affine variety over k has a model over Y.

Proposition 28.2.7

Let X and V be as above, and let V' be an open subvariety of V. Then $X' := X \setminus \overline{(V \setminus V')}$ is a model for V'.

The proof is left as an exercise.

Corollary 28.2.8

Any quasi-projective variety over k has a model over Y.

Proposition 28.2.9

Let V be any variety over k a number field, function field, or the completion of a number field or function field at a non-archimedean place ν. Then V has a model over $Y = \operatorname{Spec} A_\nu$.

The following proof is a sketch. The details of this construction are fleshed out in Lemma 2.8 of the Chapter 3 handout.

Proof: Let $U_1, \cdots, U_n$ be open affines in V that cover V. Let $X_1, \cdots, X_n$ be models for $U_1, \cdots, U_n$, respectively, over Y. The gluing data for combining the U_i to get V (cf. Hartshorne II Ex. 2.12) extend to give valid gluing data for combining $X_1, \cdots, X_n$ into one scheme outside of proper Zariski-closed subsets disjoint from $U_1, \cdots, U_n$ resp. Therefore we may eliminate finitely many closed fibers over Y, and then glue the X_i to get a scheme X over Y whose generic fiber is isomorphic (over k) to V. To ensure separatedness, we exclude more closed fibers. ■

Proposition 28.2.10

Let V be as above, D, $\mathcal{L}$, or $\mathcal{E}$ be a Cartier divisor, line sheaf, or vector sheaf on V respectively. Then X may be constructed so that D, $\mathcal{L}$, or $\mathcal{E}$ extends to the same type of object on X.

The idea of the proof is the same as above and is left as an exercise. The following corollary is of this proof strategy, not necessarily of the proposition itself.

Corollary 28.2.11

Given Cartier divisors $D_1, \cdots, D_n$, line sheaves $\mathcal{L}_1, \cdots, \mathcal{L}_m$, and vector sheaves $\mathcal{E}_1, \cdots, \mathcal{E}_p$ on V, X may be constructed so that all of these extend to X.

There are two proof methods for this result that we will briefly outline: the first method handles all of the objects (divisors, vector sheaves) simultaneously; the second proceeds sequentially by constructing a model for each given object (such that the object extends to the model). Then, with the models $X_1, \cdots, X_{n+m+p}$ with isomorphisms $i_j : V \xrightarrow{\sim} (X_j)_k$ for all j, we let X be the closure of the image of the morphism $(i_1, \cdots, i_{n+m+p}) : V \to \prod_j X_j$ (taking the product over Y). Then X is a model for V and the projections $X \to X_j$ can be used to pull back the extended objects to X.

Vojta discusses some finer points of the construction here; he is testing us here, waiting for someone to doubt his divinity by asking what we're actually working towards. O, ye of little faith.

Method 1 and Method 2 need not give the same model, but this does not matter because none of this matters.

We now want to prove the existence of proper models.

Theorem 28.2.12: Nagata

Let X be a scheme, separated and of finite type over a Noetherian scheme S. Then there exists a proper S-scheme $\overline{X}$ and an open embedding $X \hookrightarrow \overline{X}$ over S with schematically dense image. Moreover, given finitely many Cartier divisors, etc., on X, $\overline{X}$ can be chosen so that these objects extend to $\overline{X}$ as the same types of objects.

According to Deligne, the condition of Noetherianity on S can be weakened to quasi-compactness and quasi-separatedness.

Note that a variety V over k is not of finite type over Y unless M_k is finite. This is an obstruction to directly applying Nagata's theorem, but can be resolved, as we will discuss. Also note that an open subset U of a Noetherian scheme X is schematically dense iff it contains all associated points of X (Chapter 0, Prop 3.2 in the handout or Vakil 5.5.4).

Theorem 28.2.13

Every complete variety over k has a proper model over Y, and the statement of the previous corollary holds.

Proof: Let V be a complete variety over k. By Proposition 28.2.9, V has a model X_0 over Y. This is separated of finite type, so by Nagata's theorem, there exists a proper scheme X over Y and an open immersion $X_0 \hookrightarrow X$ with schematically dense image. Then all associated points of X lie in x_0, hence in $(X_0)_k \subseteq X_k$. Now we have $i : V \xrightarrow{\sim} (X_0)_k \hookrightarrow X_k$; since V is proper over k, its image in X_k is proper over k, so it is closed in X_k, and is therefore equal to X_k since it contains the dense open subset $(X_0)_k$. Therefore $(X_0)_k = X_k$, so $i : V \to X_k$ is an isomorphism, and X is the desired proper model. ■

Cartier divisors and vector sheaves extend in this situation using the earlier corollary and Nagata's theorem.

Models and Rational/Algebraic Points

Example 28.3.1

Let $k = \mathbb{Q}$ with $Y = \operatorname{Spec} \mathbb{Z}$, $V = \mathbb{A}^1_{\mathbb{Q}}$ with model $\mathbb{A}^1_{\mathbb{Z}}$. Fix $\frac{2}{3} \in \mathbb{Q}$ which is a point in $\mathbb{A}^1_{\mathbb{Q}}$ corresponding to the maximal ideal $\left(x - \frac{2}{3}\right)$. The closure of this point in $\mathbb{A}^1_{\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[x]$ is the maximal ideal $(3x - 2)$. Similarly, $20 \in \mathbb{Q}$ is the maximal ideal $(x - 20)$ which is unchanged when passing from $\mathbb{Q}$ to $\mathbb{Z}$. These rational points on $\mathbb{A}^1_{\mathbb{Q}}$ give rational sections of the map $\pi : \mathbb{A}^1_{\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[x] \to Y = \operatorname{Spec} \mathbb{Z}$.

Recall that a Weil divisor is effective if all of its coefficients are nonnegative.

Definition 28.3.2

An effective Weil divisor $\sum_Y n_Y Y$ is *reduced* if $n_Y \leq 1$ for all Y.

Theorem 28.3.3: Roth

Let k be a number field or a function field of characteristic 0, S a finite subset of M_k, D a reduced effective divisor on $\mathbb{P}^1_k$, λ_D a Weil function for D, $\epsilon > 0$, and $c \in \mathbb{R}$. Then the inequality

$$\sum_{\nu \in S} \lambda_{D,\nu}(P) \leq (2 + \epsilon) h_k(P) + c$$

holds for all but finitely many $P \in (\mathbb{P}^1_k \setminus \operatorname{Supp} D)(k)$.

Since we're in a new lecture here, note again that k is always a number field, function field, or the completion thereof at a non-archimedean place, and Y is defined as far above. $\pi : X \to Y$ is a model for a variety V over k.

Lemma 28.3.4

Let $P \in X_k(k) = X(k)$, then, there exists a unique rational section $s : Y \dashrightarrow X$ of π such that $s(\eta) = P$ where η is the unique generic point of Y. The image of s (taken with the largest possible domain) is the closure of $\{P\}$ in X. Moreover, if π is proper, then s is a regular section $s : Y \to X$.

Didn't follow much of this proof.

Proof: Let E be the closure of $\{P\}$ in X. Note that $E \cap X_k = \{P\}$. One inclusion is obvious, the other follows from the fact that P is a closed point in X_k and $X_k \setminus \{P\} = U \cap X_k$ for some open set $U \subseteq X$ not containing P (as the topology on X_k is induced by the topology on X, seeHartshorne II Ex 3.10). Therefore, $E \subseteq X \setminus U$ and $E \cap X_k \subseteq (X \setminus U) \cap X_k = \{P\}$.

Moreover, E is irreducible since it is the closure of a point, so it corresponds to an integral subscheme E_{red} of X, whose generic point is P. Therefore, $K(E) = \kappa(P) = k = K(Y)$ so there exists a rational map $Y \dashrightarrow E \hookrightarrow X$ with image contained in E, whose inverse as a rational map is $\pi|_E : E \to Y$. Any two such rational sections must coincide, by the valuative criterion of separatedness, so the existence of a unique such s follows.

To see that the image of s is equal to E, by Nagata's Theorem, there exists an open embedding $X \hookrightarrow \overline{X}$ overY with dense image (so $\overline{X}$ is a model for Y over $\overline{X}_k$) such that $\overline{X}$ is proper over Y. Let $\overline{E} = \overline{\{P\}}$ (taking the closure in $\overline{X}$); this gives a regular section $s : Y \to \overline{X}$ with $s(\eta) = P$ which then gives a rational section $s|_{s^{-1}(X)} : Y \dashrightarrow X$. This has image $\overline{E} \cap X = E$, which is therefore closed in X.

If π is proper, $s : Y \dashrightarrow X$ extends to a morphism by the valuative criterion of properness (see Stacks 0BX7). This extended map has image contained in E, so its image is in fact equal to E (since id_Y is proper, the image of a proper scheme is closed). ■

Things fall apart; the centre cannot hold; Mere anarchy is loosed upon the world, The blood-dimmed tide is loosed, and everywhere The ceremony of innocence is drowned;

Definition 28.3.5

An integral closed subscheme (or irreducible closed subset) $Z \subseteq X$ is *vertical* if it is contained in a closed fiber of $\pi : X \to Y$ and *horizontal* if not. In the latter case, $\pi|_Z$ is dominant.

Corollary 28.3.6

There exists a canonical bijection between $X(k)$ and the set of rational sections of π.

Proof: We have a map from $X(k)$ to the set of rational sections of π by the above lemma. This correspondence is surjective because it has inverse $s \mapsto s(\eta)$. The uniqueness result in the lemma implies that this correspondence is bijective. ■

Surely some revelation is at hand; Surely the Second Coming is at hand.

Lemma 28.3.7

Let L be a finite extension of k and let Y' be the integral closure of Y in L. Then Y' is obtained from L in the same way as Y is obtained from k, e.g, the construction of Y commutes with integral closure over field extensions.

Proof: If k is a number field, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_k$ in L, from which the result is immediate. If k is a function field, Y' is a normal curve over F whose function field is L. If k is the completion of a number field or function field k_0 at a non-archimedean place ν, the integral closure in L of the valuation ring of k is the valuation ring of L (this is Hensel's lemma, see Neukirch II 4.7). Further note that if $k = \mathbb{R}$ or $\mathbb{C}$, this result is trivial. ■

Proposition 28.3.8

Let L and Y' be as in the above lemma. Then the map

$$\{\text{rational maps } Y' \dashrightarrow X \text{ over } Y\} \to X_k(L)$$

given by the $s \mapsto s(\eta')$ (where η' is the generic point of Y') is bijective. Its inverse is given by extending $P \in X_k(L) = X(L)$ to a rational map $s : Y' \dashrightarrow X$.

That twenty centuries of stony sleep Were vexed to nightmare by a rocking cradle, And what rough beast, its hour come round at last, Slouches towards Bethlehem to be born?

Proof: The map is injective by the valuative criterion of separatedness. The map is surjective: let $X' = X \times_Y Y'$ and let $P \in X(L)$. Then, by the universal property of products, there exists a unique map Q making the following diagram commute:

$$\begin{tikzcd}
\operatorname{Spec} L \arrow[dr, dashed, "Q"] \arrow[drr, bend left, "P"] \arrow[ddr, bend right] & & \\
& X' \arrow[r] \arrow[d] & X \arrow[d] \\
& Y' \arrow[r] & Y
\end{tikzcd}$$

There exists a unique rational section $s' : Y' \to X'$ such that the image of Q equals $s'(\eta')$. Composing with the projection $X' \to X$ gives a rational map $s : Y' \dashrightarrow X$ over Y such that $s(\eta) = P$. The inverse is well-defined by the valuative criterion of separatedness. ■

Definition 28.3.9: S-integral points

Let V be an affine variety over k, $i : V \hookrightarrow \mathbb{A}^n_k$ a closed embedding over K, $S \subseteq M_k$ a nonempty finite set containing all archimedean places of k. Let $R \subseteq k$ be the subring $\{a \in k : \|a\|_\nu \leq 1 \text{ for all } \nu \in M_k \setminus S\}$. Then a rational point $P \in V(k)$ is *S-integral* relative to

i if all coordinates of $i(P)$ lie in R. An algebraic point $P \in V(\overline{k})$ is *S-integral* relative to i if all coordinates of $i(P)$ are integral over R (note that R is integrally closed so S-integral rational points are S-integral algebraic points). Equivalently, P is S-integral if for some (and therefore for all) finite extensions L of k such that $P \in V(L)$, all coordinates of $i(P)$ lie in

$$\{\alpha \in L : \|\alpha\|_\omega \leq 1 \text{ for all } \omega \in M_L \text{ lying over some } \nu \in M_k \setminus S\}$$

Note that this definition depends on i.

Example 28.3.10

Let $k = \mathbb{Q}$, $S = \{\infty\}$, $V = \mathbb{A}^1_{\mathbb{Q}}$, and let P be the point $\frac{2}{3}$. Then $R = \mathbb{Z}$, and P is not integral with respect to the identity map on $\mathbb{A}^1_{\mathbb{Q}}$, but it is integral w.r.t the multiplication by 6 map from $\mathbb{A}^1_{\mathbb{Q}}$ to itself. In fact, for all algebraic points $P \in V(k)$, there exists an affine embedding $i : V \hookrightarrow \mathbb{A}^n_k$ such that P is S-integral w.r.t i (here we can see this by clearing denominators).

Apparently the following definition is due to Serre, who enjoyed murdering orphans in his spare time.

Definition 28.3.11

A set $\Sigma \subseteq V(k)$ is *S-quasi-integral* if there exists a closed embedding $i : V \hookrightarrow \mathbb{A}^n_k$ such that the denominators of coordinates of $i(P)$ are bounded independently of P, e.g, there exists $c \in k^\times$ independent of P such that all coordinates of $i(P)$ lie in $c^{-1}R$ for all $P \in \Sigma$.

As stated above, all finite sets are S-quasi-integral; this is also true, but more nontrivial for infinite sets. This notion is independent of the choice of i:

Proposition 28.3.12

Let V be an affine variety over k, and let $i : V \hookrightarrow \mathbb{A}^n_k$, $j : V \hookrightarrow \mathbb{A}^m_k$ be closed embeddings over k. Then for all $c \in k^\times$ there exists $c' \in k^\times$ such that the set

$$\{P \in V(\overline{k}) : P \text{ is integral w.r.t } c' \cdot j\}$$

contains the set

$$\{P \in V(\overline{k}) : P \text{ is integral w.r.t } c \cdot i\}$$

The proof is omitted but may be assigned as homework.

It is sometimes useful to define integral points on varieties that are not affine (and not projective), e.g, $\mathbb{A}^1 \times \mathbb{P}^1$, or some moduli spaces. As the above definition is not the final definition, to motivate the ultimate definition we have the following:

Proposition 28.3.13

Let S, R, and $i : V \hookrightarrow \mathbb{A}^n_k$ be as above. Let X be the model of V obtained by taking the closure of the image of i is $\mathbb{A}^n_Y$. Let $U = \operatorname{Spec} R \subseteq Y$ (an open subscheme), then a point $P \in V(k)$ is S-integral w.r.t i iff the rational section $s : Y \dashrightarrow X$ corresponding to P extends to a regular map $U \to X$. Equivalently, by abuse of notation, $P \in X(U)$.

There is no real direction here, neither lines of power nor cooperation. Decisions are never really made – at best they manage to emerge, from a chaos of peeves, whims, hallucinations and all around assholery.

Proof: Let $P \in V(k)$, and write $i(P) = (a_1, \cdots, a_n) \in k^n$. Then the map $s : Y \dashrightarrow \mathbb{A}^n_Y$ corresponding to P is represented by the morphism $\operatorname{Spec} A \to \mathbb{A}^n_Y$ corresponding to the homomorphism $A[x_1, \cdots, x_n] \to A$ over A with $x_i \mapsto a_i$ for all i on some nonempty open affine $\operatorname{Spec} A$ in Y, and where U is one of these open affines iff $a_i \in R$ for all i iff P is S-integral w.r.t i. A similar argument works for $P \in V(\bar{k})$. ■

Definition 28.3.14

Let S and R be as above. A point $P \in V(k)$ is *S-integral with respect to X* if the rational section $s : Y \dashrightarrow X$ corresponding to P is regular on $U = \operatorname{Spec} R$, i.e, if $P \in X(\operatorname{Spec} R) = X(R)$.

Note that we do not require X to be a proper model, so $\pi : X \to Y$ may not be surjective. If $\pi(X) \not\supseteq \operatorname{Spec} R$, then $X(R)$ will be be empty. If X is a proper model, then all $P \in X(k)$ are integral w.r.t X, by the valuative criterion of properness, or the result from Stacks 0BX7.

The following is essentially Fermat's Last Theorem over certain function fields.

Theorem 28.3.15: Silverman

Let F be a field of characteristic 0, $n \geq 3$ an integer. Suppose $a, b, c \in F[t]$ with $(a, b, c) = (1)$ in $F[t]$ and $a^n + b^n + c^n = 0$. Then $a, b, c \in F$ (equivalently, $h_k([a : b : c]) = 0$).

Proof: We may assume that F is algebraically closed. Let $Y = \mathbb{P}^1_F$ (this is our "usual" Y as above), with $K(Y) = k$. Let V be the curve $x^n + y^n + z^n = 0$ in $\mathbb{P}^n_k$, X_0 the curve $x^n + y^n + z^n = 0$ in $\mathbb{P}^n_F$, and let $X = X_0 \times_F Y$, with projections $p : X \to X_0$ and $\pi : X \to Y$. Since $V \cong X_0 \times_F k$, π is a proper model for V.

Polynomials $a, b, c \in F[t]$, not all zero, with $a^n + b^n + c^n = 0$ define a point $P \in X(k)$, hence a section $\sigma : Y \to X$ of π (which is regular, not rational, since π is proper). We may assume that $(a, b, c) = (1)$ in $F[t]$ (i.e they are relatively prime), then $h_k(P) = \max(\deg a, \deg b, \deg c)$ (by direct computation), so $h_k(P) = 0 \iff a, b, c \in F$.

Then, $p \circ \sigma$ gives a morphism $Y = \mathbb{P}^1_F \to X_0$. We can describe this map concretely as follows: closed points $y \in Y$ are elements of F since F is algebraically closed, and $p \circ \sigma$ takes y to $[a(y) : b(y) : c(y)] \in X_0(F)$ (since the three are relatively prime, they are not simultaneously zero). If a, b, c are not all constant, $p \circ \sigma$ is nonconstant. But $\mathbb{P}^1_F$ has genus 0, and X_0 has genus greater than 0 (by the genus-degree formula), which is a contradiction, as there exist nonzero differentials on X_0 (since $h^0(X_0, \omega_{X_0}) = g > 0$) which would pullback to give nonzero differentials on $\mathbb{P}^1_F$; no such nonzero differentials exist, as $\omega_{\mathbb{P}^1_F} \cong \mathcal{O}(-2)$. ■

The reason this argument fails in the number field case is that the constructions corresponding to X_0, $\operatorname{Spec} F$, and $p : X \to X_0$ do not exist or do not have the same properties in the case of number fields.

Before Wiles resolved Fermat's Last Theorem, there was effort spent on trying to find an analogue for $\operatorname{Spec} F$ in the number field case (such as "black dot" and "white dot," apparently).

Let k be a number field or function field, Y a model for k (as above). Let ν be a non-archimedean place of k, and let R_ν be the valuation ring of $\mathbb{C}_\nu$. What do Cartier divisors on $\operatorname{Spec} R_\nu$ look like? Of course, we can describe Cartier divisors on any scheme in terms of an open cover and rational functions, but $\operatorname{Spec} R_\nu$ is equivalent (as a topological space) to the Sierpiński space of two points, one open (the generic point (0)), one closed (the unique maximal), so any open cover might as well be $\{\operatorname{Spec} R_\nu\}$ itself, since any open set must contain the generic point, and the closed point on its own is a closed set. Therefore, the group of Cartier divisors on $\operatorname{Spec} R_\nu$ is $\operatorname{CDiv}(\operatorname{Spec} R_\nu) \cong \mathcal{K}^\times(\operatorname{Spec} R_\nu)/\mathcal{O}(\operatorname{Spec} R_\nu)^\times = \mathbb{C}_\nu^\times / R_\nu^\times$; the latter group is the valuation group of $\mathbb{C}_\nu$, which in turn is isomorphic to $\mathbb{Q}$.

Let V be a complete variety over k, and let $\pi : X \to Y$ be a proper model for V over Y. Since π is a proper model, $X(\mathbb{C}_\nu) = X(R_\nu)$ (from the valuative criterion of properness), and let D be a Cartier divisor on X, $P \in (X \setminus \operatorname{Supp} D)(\mathbb{C}_\nu) = (V \setminus \operatorname{Supp} D_k)(\mathbb{C}_\nu)$ where D_k is D restricted to the generic fiber. Note that $(V \setminus \operatorname{Supp} D)(\mathbb{C}_\nu) \neq (X \setminus \operatorname{Supp} D)(R_\nu)$ because $X \setminus \operatorname{Supp} D$ is not generally proper.

P gives a morphism $\varphi_P : \operatorname{Spec} R_\nu \to X$ over Y (with image not contained in $\operatorname{Supp} D$) so we have a Cartier divisor $\varphi_P^* D$ on $\operatorname{Spec} R_\nu$ (which is a rational number as above). Also, we could have a rational (or algebraic) point $P \in V(k) = X(k)$; this gives a section $\sigma : Y \to X$, and this gives a point in $X(\mathbb{C}_\nu)$ since $k \subseteq \mathbb{C}_\nu$ so again we have a divisor $\sigma^* D$ in $\operatorname{Spec} R_\nu$ (which comes from a divisor on $\operatorname{Spec} A_\nu$, where A_ν is the valuation ring of k_ν). In that case, the corresponding rational number is an integer.

Imagine a French chef so thoroughly obsessed with *mise en place* that he required you to prep the ingredients for every meal you would ever cook in the rest of your life before allowing you to begin cooking. What a wacky concept with no relation to any current context.

Let D be represented by pairs (U_i, f_i) where U_i is open in X and $f_i \in K(X)^\times = K(V)^\times$ for all i. Pick i such that $P \in U_i$, then $\varphi_P^* D$ is the principal divisor $(\varphi_P^* f_i)$ on $\operatorname{Spec} R_\nu$. For any other choice of i, say j, with $P \in U_j$, $f_i/f_j \in \mathcal{O}(U_i \cap U_j)^\times$, so $\varphi_P^* f_i / \varphi_P^* f_j \in R_\nu^\times$, so $\|\varphi_P^* f_i\| = \|\varphi_P^* f_j\|$, e.g, $\|\varphi_P^* f_i\|$ is independent of the choice of i, so $\|\varphi_P^* D\|$ is well-defined.

Definition 28.3.16

Let D' be a Cartier divisor on $\operatorname{Spec} R_\nu$. Then $\|D'\| := \|f\|$ for any choice of pair $(\operatorname{Spec} R_\nu, f)$ representing D'.

Recall that k_ν has a discrete valuation $\nu : k_\nu^\times \twoheadrightarrow \mathbb{Z}$ and let $\|\alpha\|_\nu := c^{-\operatorname{ord}_\mathfrak{p} \alpha}$ (where ν is archimedean) for all $\alpha \in k_\nu^\times$ where $\operatorname{ord}_\mathfrak{p}$ is taken w.r.t the valuation ring A_ν and its maximal ideal $\mathfrak{p}$, and $c > 1$ is a fixed constant. So our rational number is $-\log_c \|\varphi_P^* D\|$. In the case of function fields and completed fields, we take $c = e$ (as a convention), and this rational number is $-\log \|\varphi_P^* D\|$. For number fields, we let $c = |\mathcal{O}_k/\mathfrak{p}|$ (as in the p-adic valuation and norm).

Math 254B: Arakelov Theory **Spring 2021**

Lectures 32-34: 12-16 April

Professor Paul Vojta Abhishek Shivkumar

The Weil-Cartier-Vojta Axis of Evil

Today we will show that a Cartier divisor D on X defines a Weil function on V for $D|_V$ (identifying V with X_k), except that the Weil function will only cover non-archimedean places.

Definition 29.1.1

Let S be a subset of M_k. Then $V(S) := \coprod_{\nu\in S} V(\mathbb{C}_\nu) \subseteq V(M)$ and $X(S) = \coprod_{\nu\in S} X(\mathbb{C}_\nu) \subseteq X(M)$ with $X(S) = V(S)$ and $X(M) = V(M)$ via the identification of V with X_k. A subset $E \subseteq V(S)$ is M-bounded if it is M-bounded as a subset of $V(M)$ and likewise for $E \subseteq X(S)$ (via $X(S) = V(S)$ as above). A function $f : V(S) \to \overline{\mathbb{R}}$ is locally M-bounded from below if for all M-bounded subsets $E \subseteq V(S)$ there exists an M_k-constant γ such that $f(P) \geq -\gamma_{\nu(P)}$ for all $P \in E$. One may define local M-boundedness from above and without qualification similarly.

A partial Weil function on V over S is a pair (D, λ) consisting of a Cartier divisor D on V and a function $\lambda : (V \setminus \operatorname{Supp} D)(S) \to \mathbb{R}$ that satisfies all of the conditions for a Weil function but with M replaced by S. Finally, Weil functions on X and partial Weil functions on X are defined similarly. using $X(S) = V(S)$ (and D may be a divisor on X, in which case $D|_{X_k}$ is used).

I have not absorbed one iota of this information.

Definition 29.1.2

Assume that V is complete and that $\pi : X \to Y$ is proper. Let D be a Cartier divisor on X. Then we define $\lambda_D : (X \setminus \operatorname{Supp} D)(M_k^0) \to \mathbb{R}$ by $\lambda_D(P) = -\log \|\varphi_P^* D\|$, where $\varphi_P : \operatorname{Spec} R_\nu \to X$ extends to $P : \operatorname{Spec} \mathbb{C}_\nu \to X$, where R_ν is the valuation ring of $\mathbb{C}_\nu$.

Proposition 29.1.3

Let V, $\pi : X \to Y$, D, and λ_D be as above. Then λ_D is a partial Weil function for D over M_k^0.

Proof: Let $i : V \to X$ be the map $V \xrightarrow{\sim} X_k \to X$ and let D be represented by (U_j, f_j) on X. Then $(i^{-1}(U_j), i^* f_j)$ represents $i^* D$ on V, and

$-\log\|\varphi_P^* D\| = -\log\|f_j(P)\|$ for all $P \in U_j(\mathbb{C}_\nu) \setminus \operatorname{Supp} D$ and all j.

We need to show that $\lambda_D + \log\|f_j\|$ extends to a continuous locally M-bounded function on $U_j(M_k^0)$ for all j. Pick $\nu \in M_k^0$ and note that $U_j(R_\nu) \subset U_j(\mathbb{C}_\nu)$. However, $U_j(R_\nu)$ is a clopen subset of $X(\mathbb{C}_\nu)$; closed because, assuming U_j is affine, it is given by $\|x_l\|_\nu \leq 1$ for all l, and open because if $P \in U_j(R_\nu)$, then so is an open neighborhood of P (with radius 1). Also, $\lambda_{D,\nu} + \log\|f_j\|_\nu$ extends to a continuous function on $U_j(R_\nu)$ for all j (namely, 0). Since $U_j(\mathbb{C}_\nu) = \bigcup_{j'} U_{j'}(R_\nu) \cap U_j(\mathbb{C}_\nu)$ and

$$\lambda_{D,\nu} + \log\|f_j\|_\nu = -\log\|f_{j'}\|_\nu + \log\|f_j\|_\nu = -\log\|f_{j'}/f_j\|_\nu$$

is continuous on $U_{j'}(\mathbb{C}_\nu) \cap U_j(\mathbb{C}_\nu) \supseteq U_{j'}(R_\nu) \cap U_j(\mathbb{C}_\nu)$, so $\lambda_{D,\nu} + \log\|f_j\|_\nu$ is continuous on $U_j(\mathbb{C}_\nu)$.

Local M-boundedness is quite involved to prove; see the Chapter 3 handout, lemma 5.8. ■

Lemma 29.1.4

Let $k = \mathbb{R}$, $\mathbb{C}$, or a number field, ν an archimedean place of k. Let V be a complete variety over k, and D a Cartier divisor on V. Then there exists a partial Weil function for D over $\{\nu\}$ on V.

Proof: Let D be represented by (U_i, f_i). We may assume that the index set for i is finite. Let $\{\varphi_i : X(\mathbb{C}_\nu) \to \mathbb{R}\}$ be a continuous (or C^∞) partition of unity with $\operatorname{Supp}\varphi_i \Subset U_i(\mathbb{C}_\nu)$ (where $U \Subset V$ means that there exists K compact such that $U \subseteq K \subseteq V$) for all i. Then $\sum_i \varphi_i \cdot (-\log\|f_i\|)$ is such a partial Weil function. ■

Theorem 29.1.5

Let k be a Vojta field, let V be a complete variety over k, D a Cartier divisor on V. Then there exists a Weil function for D on V.

Proof: If $M_k^0 \neq \emptyset$, then there exists (by Nagata) a proper model $\pi : X \to Y$ for V (with Y as usual) such that D extends to a Cartier divisor $\tilde{D}$ on X. Then (by the above proposition) there exists a partial Weil function on V for D over M_k^0.

For all $\nu \in M_k^\infty$, there exists a partial Weil function on V for D over $\{\nu\}$ (by the above lemma). These (finitely many) partial Weil functions combine to give a Weil function for D over M_k. ■

We need V to be complete because it is assumed to be complete in the proposition. Otherwise, the model X might be missing a whole closed fiber, so λ_D would not be defined on $(X \setminus \operatorname{Supp} D)(\mathbb{C}_\nu)$ in that case. Of course, you can always embed a non-complete variety into a complete variety in such a way that the divisor extends.

Definition 29.1.6: Integrality

Let k be a number field or function field, or the completion of a number field or function field k_0 at a non-archimedean place ν, and Y as usual for k. Let $S \subseteq M_k$ be a finite subset containing M_k^∞. Let V be a variety over k embedded as an open subscheme of a complete variety $\overline{V}$ over k, such that $\overline{V} \setminus V$ is the support of an effective Cartier divisor D on $\overline{V}$. Let λ_D be a partial Weil function for D on $\overline{V}$ over some $S' \supseteq M_k \setminus S$. Then a point $P \in V(k)$ is (S, λ_D)-integral if $\lambda_{D,\nu}(P) \leq 0$ for all $\nu \in M_k \setminus S$ and λ_D-integral if it is (M_k^∞, λ_D)-integral.

Deeply cursed definition.

Proposition 29.1.7

With $k, Y, S, V, \overline{V}$, and D as above, let $\overline{\pi} : \overline{X} \to Y$ be a proper model for $\overline{V}$ over Y such that D extends to an effective Cartier divisor $\overline{D}$ on $\overline{X}$, and $X = \overline{X} \setminus \operatorname{Supp} D$. Then X is a model for V (which may omit entire fibers of $\overline{\pi}$ but this is unavoidable). Let λ_D be the partial Weil function for $\overline{D}$ over M_k^0 defined above; then a point $P \in V(k)$ is integral w.r.t the model X iff it is λ_D-integral.

Proof: Let $\sigma : Y \to \overline{X}$ be the regular section of $\overline{\pi}$ corresponding to P. Then P is integral w.r.t X iff

$$\sigma(Y) \subseteq X \iff \sigma(Y) \cap \operatorname{Supp} D = \emptyset \iff \sigma^* D = 0 \iff \\ \lambda_{D,\nu}(P) = 0 \text{ for all } \nu \in M_k^0 \iff P \text{ is } \lambda_D\text{-integral}$$

Note that $\lambda_{D,\nu} \geq 0$ everywhere on its domain since D is effective. ■

Note that there is a similar definition of S-integrality w.r.t X and a similar proposition is true for this definition. We may also repeat this definition for algebraic integral points.

Heights via Models

Until further notice, k is a function field in one variable, Y is a smooth projective curve over F where $k = F(t)$ and $k(Y) \cong k$ over F (as usual). Let $\pi : X \to Y$ be a proper model for a complete variety $V \cong X_k$, and let D be a Cartier divisor on X. Let $P \in V(k)$, and let $\sigma : Y \to X$ be the corresponding section of π. Let λ_D be the Weil function defined above (note that $M_k^\infty = \emptyset$). Then

$$h_{\lambda_D}(P) = \sum_{\nu \in Y \setminus \{\eta\}} \lambda_{D,\nu}(P) = \sum_\nu - \log \|f_i(P)\|_\nu = \sum_\nu n_\nu(- \log \|\pi_\nu\|_\nu)$$

where η is the generic point of Y, since closed points of Y correspond to places of k, $\sigma^* D = \sum_\nu n_\nu \cdot [\nu]$ as a Weil divisor, and π_ν is a uniformizer at

ν.

The first equality above is by definition of h_{λ_D}. The second equality follows by representing D by a collection (U_i, f_i) and for each ν choose i such that $\sigma(\nu) \in U_i$; in detail, let R_ν be the valuation ring of $\mathbb{C}_\nu$, $\tau_\nu : \operatorname{Spec} R_\nu \to X$ the composite map $\operatorname{Spec} R_\nu \to Y \xrightarrow{\sigma} X$, and choose i such that $\sigma(\nu) \in U_i$, then the Cartier divisor $\tau_\nu^* D$ on $\operatorname{Spec} R_\nu$ is represented by the single pair $(\operatorname{Spec} R_\nu, \tilde{f})$ where $\tilde{f} = \tau_\nu^* f_i$. Then $\tilde{f} = f_i(P)$, so $\|\tau_\nu^* D\| = \|\tau_\nu^* f_i\| = \|f_i(P)\|_\nu$ so $\lambda_{D,\nu}(P) = -\log\|\tau_\nu^* D\| = -\log\|f_i(P)\|_\nu$ by definition of $\lambda_{D,\nu}$. The third equality is by defining $n_\nu = \nu(f_i(P))$ where $\nu : \mathbb{C}_\nu^* \to \mathbb{Q}$ comes from the valuation $\nu : k_\nu^* \twoheadrightarrow \mathbb{Z}$ which has $\nu(\pi_\nu) = 1$ by the definition of a uniformizer. So $\|f_i(P)\|_\nu = \|\pi_\nu\|^{n_\nu}$ because $f_i(P)/\pi_\nu^{n_\nu}$ is a unit in R_ν.

By definition of $\|\cdot\|_\nu$, $\|\pi_\nu\|_\nu = e^{[\kappa(\nu):F]}$ where $\kappa(\nu)$ is the residue field of k_ν, so $\sum_\nu n_\nu(-\log\|\pi_\nu\|_\nu) = \sum n_\nu \deg\nu$ where by definition $\deg\nu = [\kappa(\nu) : F]$ and this equals $\deg(\sigma^* D)$ by the definition of the degree of a divisor on a nonsingular curve (Vakil 18.4.1, page 479).

Lemma 29.2.1

In the above situation, $h_{\lambda_D}(P) = \deg\sigma^* D$ for all $P \in V(k)$ such that $P \notin \operatorname{Supp} D$ (so $\sigma(Y) \not\subseteq \operatorname{Supp} D$ on X).

If $P \in \operatorname{Supp} D$, then we defined $h_{\lambda_D}(P)$ to be $h_{\lambda_1}(P)$ where λ_1 is a Weil function for a divisor D_1 on V such that $P \notin \operatorname{Supp} D_1$ and $D_1 = D + (f_1)$, and $\lambda_1 = \lambda_D - \log\|f_1\|$. We showed that this is well-defined because if f_2 is another such function, D_2, λ_2 similarly defined, then $h_{\lambda_1}(P) - h_{\lambda_2}(P) = \sum_\nu -\log\|(f_1/f_2)(P)\|_\nu = 0$ by the product formula (note that $P \notin \operatorname{Supp}\operatorname{div}(f_1/f_2) = \operatorname{Supp} D_1 - D - 2$).

We can work similarly here, using the following lemma:

Lemma 29.2.2

Let D be a principal (Cartier) divisor on X, say $D = (f)$ with $f \in K(X)^\times = K(V)^\times$. Then λ_D (as defined last time) is equal to $-\log\|f\|$, and $h_{\lambda_D}(P) = 0$ for all $P \in (V \setminus \operatorname{Supp} D)(k)$.

Proof: The first claim is immediate from the second equality in the above discussion, since in this case, D is represented by the collection (X, f), so $f_i = f$ for all ν. For the second claim, note that

$$h_{\lambda_D}(P) = \deg\sigma^* D = \deg\sigma^*(f) = \deg f(P) = 0$$

where the final equality is by the product formula. ■

Theorem 29.2.3

$h_{\lambda_D}(P) = \deg \sigma^* \mathcal{O}(D)$ for all $P \in V(k)$ (including $P \in \operatorname{Supp} D(k)$) where $\sigma : Y \to X$ is the section corresponding to the rational point P as usual.

Proof: Find $f \in K(X)^\times = K(V)^\times$ such that $P \notin \operatorname{Supp}(D + (f))$. Then

$$h_{\lambda_D}(P) = h_{\lambda_{D+(f)}}(P) = \deg \sigma^*(D+(f)) = \deg \sigma^* \mathcal{O}(D+(f)) = \deg \sigma^* \mathcal{O}(D)$$

where the final equality is by the fact that $\mathcal{O}(D + (f)) \cong \mathcal{O}(D)$, the first equality by the definition of h_{λ_D} (specifically linearity), and the intermediate equalities follow by above results. ■

Definition 29.2.4

Let $\mathcal{L}$ be a line sheaf on X. Then $h_{\mathcal{L}}(P) := \deg \sigma^* \mathcal{L}$ for all $P \in V(k)$ where $\sigma : Y \to X$ corresponds to P.

The desired additivity and functoriality properties follow easily: if $\mathcal{L}$ and $\mathcal{M}$ are line sheaves on X, then

$$h_{\mathcal{L}\otimes\mathcal{M}}(P) = \deg \sigma^*(\mathcal{L} \otimes \mathcal{M}) = \deg(\sigma^*\mathcal{L} \otimes \sigma^*\mathcal{M}) = \\ \deg \sigma^*\mathcal{L} + \deg \sigma^*\mathcal{M} = h_{\mathcal{L}}(P) + h_{\mathcal{M}}(P)$$

for all $P \in V(k)$. For functoriality, let $f_k : V \to W$ be a morphism over k of complete varieties over k. Let X and Z be models (over Y) for V and W respectively. In general, f_k only extends to a rational map $X \dashrightarrow Z$, so let X' be the closure of the graph of this rational map. This too is a model for V, and $f_k : V \to W$ extends to a morphism $f : X' \to Z$ over Y, and there is also a morphism $X' \to X$. Let $P \in V(k)$, $\mathcal{M}$ a line sheaf on Z. Then $f_0(P) \in W(k)$, and we have $h_{\mathcal{M}}(f_0(P)) = h_{f^*\mathcal{M}}(P)$ for all P. To see this, let $\sigma : Y \to X'$ and $\tau : Y \to Z$ be sections corresponding to P and $f_k(P)$, respectively. Then $\tau = f \circ \sigma$, and

This discussion is the Last Year at Marienbad of mathematics.

$$h_{\mathcal{M}}(f_k(P)) = \deg \tau^*\mathcal{M} = \deg \sigma^* f^* \mathcal{M} = h_{f^*\mathcal{M}}(P)$$

NOte that everything done so far works for algebraic points (rather than just rational points) using the bijection between $V(L)$ and $\operatorname{Hom}_Y(Y', X)$ for a proper model X for V over Y.

Number Fields

Let k be a number field, $Y = \operatorname{Spec} \mathcal{O}_k$ as usual. As before, and unless stated otherwise, V is a complete variety over k and $\pi : X \to Y$ is a proper model for V over Y. We'd like to extend the model Y to something incorporating all of the archimedean places of k, but we don't know how to yet. Instead, we'll add structure to the line sheaves on X.

Definition 29.3.1

Let V be a variety over $\mathbb{C}$, $\mathcal{L}$ a line sheaf on V. A *metric* on $\mathcal{L}$ is a norm $\|\cdot\|$ on each fiber $\mathcal{L}_x$ of $\mathcal{L}$ at $x \in V(\mathbb{C})$ such that if $\{b_x\}$ is a basis for $\mathcal{L}_x$, then $\|zb_x\| = c_x\|z\|$ for all $z \in \mathbb{C}$ where c_x is a chosen positive real number. A metric on $\mathcal{L}$ is *continuous* (resp *smooth*) at $x \in V(\mathbb{C})$ if there exists a holomorphic section s of $\mathcal{L}$ over some open neighborhood U of x (in the classical topology, i.e, ν-topology) which does not vanish at x, and such that the function $P \mapsto \|s(P)\|$ is continuous at x (resp smooth).

If V is singular, then smoothness can be defined, but it's tricky.

For a vector sheaf $\mathcal{E}$ on V, you would define a (positive definite) hermitian inner product on $\mathcal{E}_x$ for all $x \in V(\mathbb{C})$ varying continuously or smoothly with x. This reduces to the above definition when $\mathcal{E}$ is a line sheaf, so metrics on $\mathcal{L}$ are often called hermitian metrics.

Example 29.3.2

Let $\mathbb{P}^n_{\mathbb{C}} = \operatorname{Proj} \mathbb{C}[z_0, \cdots, z_n]$, $s = a_0z_0 + \cdots + a_nz_n$ a global section of $\mathcal{O}(1)$ with $a_i \in \mathbb{C}$. Let $P = [p_0 : \cdots : p_n]$ be a point in $\mathbb{P}^n_{\mathbb{C}}$. We can define the *Fubini-Study metric* on $\mathcal{O}(1)$, given by

$$\|s\|_{\mathrm{FS}}(P) := \frac{|a_0p_0 + \cdots + a_np_n|}{\sqrt{\|p_0\|^2 + \cdots + \|p_n\|^2}}$$

another metric on $\mathcal{O}(1)$ is given by

$$\|s\|_{\max}(P) : \frac{|a_0p_0 + \cdots + a_np_n|}{\max \|p_0\|, \cdots, \|p_n\|}$$

The former is smooth and continuous, the latter only continuous (and not smooth).

Math 254B: Arakelov Theory **Spring 2021**

Lectures 35-37: 19-23 April

Professor Paul Vojta Abhishek Shivkumar

Metrics

Proposition 30.1.1

Let V be a variety over $\mathbb{C}$, $\mathcal{L}$ a line sheaf on V. Then there exists a smooth metric on $\mathcal{L}$.

We won't give a full proof here, but the idea is to embed V into a complete variety to which $\mathcal{L}$ extends, and use a smooth partition of unity.

For the rest of the course, we will be using the following convention which is dominant in Arakelov theory: if k is a number field, then $M_k^\infty = \operatorname{Hom}(k, \mathbb{C})$ and $M_k = M_k^\infty \coprod M_k^0$, and for any $\nu \in M_k^\infty$ corresponding to $\sigma : k \hookrightarrow \mathbb{C}$, $\|x\|_\nu = |\sigma(x)|$ for all $x \in k$. We still have a product formula in this case, as each complex place (in the previous sense) is now two complex places (conjugate pairs).

Definition 30.1.2: Arithmetic Varieties

An *arithmetic variety* is an integral scheme X, flat and projective over $\operatorname{Spec}\mathbb{Z}$. In this situation, flatness is equivalent to the unique generic point of X mapping to the generic point of $\operatorname{Spec}\mathbb{Z}$. X is *generically smooth* if its generic fiber $X_\mathbb{Q}$ is smooth (equivalently, its generic fiber is a regular scheme since we are working in characteristic 0). An arithmetic variety X is generically smooth iff $X(\mathbb{C})$ is a complex manifold (not necessarily connected).

I don't see how $X(\mathbb{C})$ is going to be a complex manifold without passing to the analytification or something like that. Does he mean "possesses a complex structure"?

For the rest of today, X is an arithmetic variety.

Definition 30.1.3: Metrized Line Sheaves

A continuously (resp. smoothly) *metrized line sheaf* on X is a pair $\mathcal{L} = (\mathcal{L}_{\text{fin}}, \|\cdot\|_\mathcal{L})$ where $\mathcal{L}_{\text{fin}}$ is a line sheaf on X (without metric) and $\|\cdot\|_\mathcal{L}$ is a continuous (resp. smooth) hermitian metric on $(\mathcal{L}_{\text{fin}})_\mathbb{C}$ (which is the pullback of $\mathcal{L}_{\text{fin}}$ to $X_\mathbb{C} = X \times_k \mathbb{C}$).

A more common notation in the literature of Arakelov theory is $\overline{\mathcal{L}} = (\mathcal{L}, \|\cdot\|_\mathcal{L})$ or $\overline{\mathcal{L}} = (\mathcal{L}, h)$.

Let k be a number field, V a projective variety over k, X a model for V over $Y = \operatorname{Spec} \mathcal{O}_k$. Then X is an arithmetic variety via $X \to Y \to \operatorname{Spec} \mathbb{Z}$ and is generically smooth iff V is nonsingular. Thus we can see that our notion of arithmetic variety extends in a natural way to number fields other than $\mathbb{Q}$. Since $k \cong \mathcal{O}_k \otimes_\mathbb{Z} \mathbb{Q}$ as a $\mathbb{Q}$-algebra, by transitivity of base extension (Hartshorne p.89),

$$X_\mathbb{Q} = X \times_\mathbb{Z} \mathbb{Q} \cong X \times_{\mathcal{O}_k} (\mathcal{O}_k \times_\mathbb{Z} \mathbb{Q}) \cong X \times_{\mathcal{O}_k} k = X_k$$

so $X(\mathbb{C}) = X_\mathbb{Q}(\mathbb{C})$ since there exists a unique map $\operatorname{Spec} \mathbb{C} \to \operatorname{Spec} \mathbb{Q}$.

Consider the following diagram:

$$\begin{tikzcd}
\operatorname{Spec} \mathbb{C} \arrow[r] \arrow[dr, "\sigma\in M_k^\infty"] \arrow[ddr, "\exists!"'] & X_\mathbb{Q} \cong X_k \arrow[d] \\
& \operatorname{Spec} k \arrow[d] \\
& \operatorname{Spec} \mathbb{Q}
\end{tikzcd}$$

$\operatorname{Hom}(\operatorname{Spec} \mathbb{C}, \operatorname{Spec} k) \cong \operatorname{Hom}(k, \mathbb{C}) = M_k^\infty$, so we can partition $X(\mathbb{C})$ into a disjoint union based on the corresponding map $\operatorname{Spec} \mathbb{C} \to \operatorname{Spec} k$, e.g, $X(\mathbb{C}) = \coprod_{\sigma : k \hookrightarrow \mathbb{C}} X_\sigma(\mathbb{C})$ where $X_\sigma = X \times_k \mathbb{C}$, regarding $\operatorname{Spec} \mathbb{C}$ as a scheme over $\operatorname{Spec} k$ via σ. Then assuming that X_k is geometrically integral over k), each $X_\sigma(\mathbb{C})$ is a connected complex space (or, a connected complex manifold if X is generically smooth).

In the above notation, $X_\sigma = X \times_k \mathbb{C}$, and if $\mathcal{L}$ is a line sheaf on X, then $\mathcal{L}_\sigma$ is the restriction of $\mathcal{L}_\mathbb{C}$ to X_σ, or, equivalently, the pullback of $\mathcal{L}$ to X_σ. Likewise, if $\mathcal{L}$ is a metrized line sheaf on X, then $\mathcal{L}_\sigma$ is the pullback of $\mathcal{L}_{\text{fin}}$ to X_σ with the accompanied pullback metric. Therefore, giving a continuous (resp. smooth) hermitian metric on $\mathcal{L}$ is equivalent to giving continuous (resp. smooth) hermitian metrics on $\mathcal{L}_\sigma$ for all σ.

Proposition 30.1.4

Let $\mathcal{L}$ be a continuously metrized line sheaf on a complex variety V, let s be a nonzero rational section of $\mathcal{L}$, $D = \operatorname{div}_\mathcal{L}(s)$, $\lambda_D : (V \setminus \operatorname{Supp} D)(\mathbb{C}) \to \mathbb{R}$ the function $P \mapsto -\log \|s(P)\|$. Then λ is a Weil function for D.

Proof: D is represented by (U_i, f_i); fix some such i. Then $\operatorname{div}(s)|_{U_i} = (f_i)|_{U_i}$ so $\operatorname{div}_\mathcal{L}(s/f_i) = 0$, e.g, s/f_i extends to a generator of $\mathcal{L}|_{U_i}$. Then for all $P \in U_i \setminus \operatorname{Supp} D$,

$$\lambda(P) = -\log \|s(P)\| = -\log |f_i(P)| - \log \|(s/f_i)(P)\|$$

and $\alpha_i := -\log \|s/f_i\|$ extends to a continuous function $U_i(\mathbb{C}) \to \mathbb{R}$. It is also (automatically) locally M-bounded. ■

Note that if $\mathcal{L}$ is smoothly metrized, then α_i is smooth on $U_i(\mathbb{C})$.

Definition 30.1.5

A Weil function λ is *smooth* if for all i (as above), the α_i in the definition of λ are smooth. Similarly, if λ is a Weil function on a variety over a number field, then it would be smooth if this condition holds at all archimedean places of the number field.

Note that this imposes a condition at all points of $U_i(\mathbb{C})$, so it is strictly stronger than saying $\lambda|_{(V\setminus \operatorname{Supp} D)(\mathbb{C}_\nu)}$ is smooth for all $\nu \in M_k^\infty$.

Proposition 30.1.6

Let D be a Cartier divisor on a complex variety V. Then, giving a continuous metric on $\mathcal{O}(D)$ is equivalent to giving a Weil function for D. Moreover, the metric is smooth iff the Weil function is smooth.

The proof is left as an exercise.

Let k be a number field, $Y = \operatorname{Spec} \mathcal{O}_k$, V a projective variety over k, and let $\pi : X \to Y$ be a projective model for V (and therefore X is an arithmetic variety when regarded as a scheme over $\operatorname{Spec} \mathbb{Z}$). The preceding proposition carries over to give the following:

Proposition 30.1.7

If D is a Cartier divisor on X, then giving a (continuous) metric on $\mathcal{O}(D)_\infty$ (resp $\mathcal{O}(D)_\sigma$ for any $\sigma \in M_k^\infty$) is equivalent to giving a partial Weil function for D (i.e for $D_k := D|_{X_k}$) over M_k^∞ (resp over $\{\sigma\}$). Again, this metric is smooth iff the partial Weil function is smooth.

This leads us to defining arithmetic Cartier divisors:

Definition 30.1.8: Arithmetic Cartier Divisors

An *arithmetic Cartier divisor* on X is an ordered pair $D = (D_{\text{fin}}, g_D)$ where D_{fin} is a Cartier divisor on X and $\frac{1}{2}g_D$ is a smooth partial Weil function for $D_{\mathbb{Q}}$ on $X_{\mathbb{Q}} = X \times_{\mathbb{Z}} \mathbb{Q}$ over $M_{\mathbb{Q}}^\infty$ (or, equivalently, a smooth partial Weil function for $D_k = (D_{\text{fin}})_k$ on $X_k \cong V$ over M_k^∞). Often we will omit the name “Cartier.”

The factor of $\frac{1}{2}$ is added above for compatibility with Arakelov theory.

Definition-Proposition 30.1.9: Arithmetic Pic

$\hat{\operatorname{Pic}}(X)$ is the group of smoothly metrized line sheaves on X, with group operation

$$(\mathcal{L}_{\text{fin}}, \|\cdot\|_{\mathcal{L}}) \cdot (\mathcal{M}_{\text{fin}}, \|\cdot\|_{\mathcal{M}}) = (\mathcal{L}_{\text{fin}} \otimes \mathcal{M}_{\text{fin}}, \|\cdot\|_{\mathcal{L}} \cdot \|\cdot\|_{\mathcal{M}})$$

and inverses given by duals in the obvious way.

Somewhere in the definition of $\hat{\operatorname{Pic}}$, we use the fact that $X(\mathbb{C}) = \coprod_{\sigma \in M_k^\infty} X_\sigma(\mathbb{C})$.

Definition-Proposition 30.1.10

$\mathrm{C\hat{D}iv}(X)$ is the group of arithmetic Cartier divisors on X, with componentwise addition (extending the g_D part as appropriate). A divisor $D \in \mathrm{C\hat{D}iv}(X)$ gives rise to a metrized line sheaf $\mathcal{O}(D) \in \mathrm{C\hat{D}iv}(X)$ in an obvious way, giving a group homomorphism $\mathrm{C\hat{D}iv}(X) \to \mathrm{P\hat{i}c}(X)$ which is surjective.

Here and below we are just stating lots of facts without any proof.

Definition-Proposition 30.1.11

A pair $(\mathcal{L}, s)$ where $\mathcal{L} \in \mathrm{P\hat{i}c}(X)$ and s is a nonzero rational section of $\mathcal{L}_{\mathrm{fin}}$ gives rise to an arithmetic divisor $\mathrm{div}_{\mathcal{L}}(s)$ on X. Again, the set of such pairs form an abelian group in the obvious manner (tensoring sections together), and $(\mathcal{L}, s) \mapsto \mathrm{div}(s)$ is a surjective group homomorphism. As a special case of this, when $\mathcal{L} = \mathcal{O}_X$, we get principal Cartier divisors $(f) = \mathrm{div}_{\mathcal{O}_X}(f)$ for all $f \in K(X)^\times$; $K(X)^\times \to \mathrm{C\hat{D}iv}(X)$ is a group homomorphism (not surjective), so we have a concept of linear equivalence on $\mathrm{C\hat{D}iv}(X)$. For all $D \in \mathrm{C\hat{D}iv}(X)$, $\mathcal{O}(D)$ has a nonzero rational section 1_D (equal to $1_{D_{\mathrm{fin}}}$, a nonzero rational section of $\mathcal{O}(D)_{\mathrm{fin}} = \mathcal{O}(D_{\mathrm{fin}}) \in \mathrm{Pic}(X)$); and $\mathrm{div}_{\mathcal{O}(D)}(1_D) = D$ as arithmetic divisors.

For all $(\mathcal{L}, s)$ as above, there exists a canonical isomorphism $\mathcal{O}(\mathrm{div}_{\mathcal{L}}(s)) \xrightarrow{\sim} \mathcal{L}$ taking $1_{\mathrm{div}_{\mathcal{L}}(s)}$ to s. If $f : X_1 \to X_2$ is a morphism of arithmetic varieties, then we have pullback homomorphisms $f^* : \mathrm{P\hat{i}c}(X_2) \to \mathrm{P\hat{i}c}(X_1)$ and

$$f^* : \{D \in \mathrm{C\hat{D}iv}(X_2) : f^* D_{\mathrm{fin}} \text{ is defined}\} \to \mathrm{C\hat{D}iv}(X_1)$$

compatible with the maps $\mathrm{C\hat{D}iv}(X_i) \to \mathrm{P\hat{i}c}(X_i)$ and

$$\{(\mathcal{L}_i, s_i) : \mathcal{L}_i \in \mathrm{P\hat{i}c}(X_i) \text{ and } s_i \text{ is a nonzero rational section of } \mathcal{L}_i\} \to \mathrm{C\hat{D}iv}(X_i)$$

Since X is integral, the sequence

$$1 \to \mathcal{O}_X(X)^\times \to K(X)^\times \to \mathrm{C\hat{D}iv}(X) \to \mathrm{P\hat{i}c}(X) \to 1$$

is exact, and compatible with the same sequence without hats. All of the above can be done when you relax the smoothness conditions to continuity (throughout). Moreover, all of the above can also be done in the case of varieties over $\mathbb{C}$.

Briefly, let k, Y, V, and $\pi : X \to Y$ be as in the function field case. Then a Cartier divisor D on X gave a Weil function λ_D for D_k“$='' D|_V$ on V, and $h_{\lambda_D}(P) = \deg \sigma^* D$ for all $P \in V(k)$ with corresponding section $\sigma : Y \to X$, under the assumption that $P \notin \mathrm{Supp}\, D$. Also $h_{\lambda_D}(P) = \deg \sigma^* \mathcal{O}(D)$ with P, σ as before, but now allowing $P \in \mathrm{Supp}\, D$. It is this latter behavior that we want to extend to the number field case.

Definition 30.1.12

Let D be an arithmetic divisor on an arithmetic variety X. Then we defined a partial Weil function λ_D^0 for $D_k = (D_{\text{fin}})_k$ over M_k^0. We also have a partial Weil function $\frac{1}{2}g_D$ for D_k over M_k^∞; we may glue these to obtain a full Weil function λ_D for D_k.

Let $P \in (V \setminus \operatorname{Supp} D_k)(k)$ and let $\sigma : Y \to X$ be the corresponding section. We want to look at the values of $\lambda_{D,\nu}(P)$ for all $\nu \in M_k$. Over M_k^0, $\sigma^* D_{\text{fin}}$ on Y is defined, and we can write it as a Weil divisor (i.e a sum over closed points) $\sigma^* D_{\text{fin}} = \sum_{y\in Y} n_y \cdot y$. Let $\nu \in M_k^0$, $y \in Y$ the corresponding closed point, $\mathfrak{p} \subset \mathcal{O}_k$ the corresponding prime ideal, $n_\nu = n_y$, p the rational prime below ν ($(p) = \mathfrak{p} \cap \mathbb{Z}$), $f_\nu = f_{\nu/\mathbb{Q}}$, so that the residue field $\kappa(y) = \mathcal{O}_k/\mathfrak{p}$ has p^{f_ν} elements. Let D_{fin} be represented by (U_i, f_i) and choose i such that $\sigma(y) \in U_i$. Then $\lambda_{D,\nu}^0(P) = -\log \|f_i(P)\|_\nu = n_\nu \log([\mathcal{O}_k : \mathfrak{p}_\nu])$.

Over M_k^∞, we have that $\nu \in M_k^\infty$ corresponds to $\tau : k \hookrightarrow \mathbb{C}$. Then $\lambda_{D,\nu}(P) = \frac{1}{2}g_D(P_\tau)$, where $P_\tau \in V(\mathbb{C}_\nu) = X(\mathbb{C}_\nu) = X_\tau(\mathbb{C})$ is the map $\operatorname{Spec}\mathbb{C}_\nu = \operatorname{Spec}\mathbb{C} \xrightarrow{\tau} \operatorname{Spec} k \xrightarrow{P} X$ over Y. So, what is $h_\lambda(P) = \sum_{\nu\in M_k} \lambda_{D,\nu}(P)$? Over function fields, it was equal to $\deg \sigma^* D$; we want to find a similar formula for our number field case.

Now Y is an arithmetic variety (an integral scheme, flat, projective over $\operatorname{Spec}\mathbb{Z}$ (this is an easy exercise)), and a model over $\operatorname{Spec}\mathbb{Z}$ for the $\mathbb{Q}$-variety $\operatorname{Spec} k$, so $\sigma : Y \to X$ is a morphism (over $\operatorname{Spec}\mathbb{Z}$) of arithmetic varieties, so we have an arithmetic divisor $\sigma^* D$ on Y (since $P \in \operatorname{Supp} D_k$). This arithmetic divisor is equal to $(\sigma^* D_{\text{fin}}, g_{\sigma^* D})$ where $g_{\sigma^* D}$ is a function $Y(\mathbb{C}) \setminus \operatorname{Supp}(\sigma^* D_{\text{fin}})_{\mathbb{Q}} \to \mathbb{R}$ defined by $g_D \circ \sigma$ (where $Y(\mathbb{C}) = M_k^\infty$, and $\operatorname{Supp}(\sigma^* D_{\text{fin}})_{\mathbb{Q}} = \emptyset$ since $\operatorname{Supp}\sigma^* D_{\text{fin}}$ does not contain the generic point of Y). We make the following definition, after which we will try to make sense of it:

Definition 30.1.13: Degree

The *degree* of an arithmetic divisor $E = (E_{\text{fin}}, g_E)$ is the (real) number

$$\deg E = \frac{1}{2} \sum_{\nu \in M_k^\infty} g_E(\nu) + \sum_{\nu\in M_k^0} n_\nu \log([\mathcal{O}_k : \mathfrak{p}_\nu])$$

where n_ν and $\mathfrak{p}_\nu$ are as above. This is often denoted $\hat{\deg} E$.

Proposition 30.1.14

For all $\alpha \in k^\times$, the degree of the principal arithmetic divisor (α) on Y is

$$\sum_{\nu\in M_k^\infty} (-\log|\tau(\alpha)|) + \sum_{\nu\in M_k^0} (-\log\|\alpha\|_\nu) = 0$$

where $\log|\tau(\alpha)| = \log\|\alpha\|_\nu$, $\tau : k \hookrightarrow \mathbb{C}$ corresponds to ν.

How did we get $\frac{1}{2}g_{(\alpha)}(\nu) = -\log|\tau(\alpha)|$? We defined the principal arithmetic divisor (f) on X for all $f \in K(X)^\times$ as a special case $\mathcal{L} = \mathcal{O}_X$ of $\operatorname{div}_{\mathcal{L}}(s)$ for metrized line sheaves $\mathcal{L}$ on X and their nonzero rational sections s. In particular, $\operatorname{div}_{\mathcal{L}}(s) = (\operatorname{div}_{\mathcal{L}_{\text{fin}}}(s), g)$ where $\frac{1}{2}g$ is some partial Weil function for $\operatorname{div}_{\mathcal{L}_{\text{fin}}}(s)$ over M_k^∞.

Above, we stated that giving a smooth metric on $\mathcal{O}(D)_\infty$ (the pullback of $\mathcal{O}(D)$ to $X(\mathbb{C})$) is equivalent to giving a smooth partial Weil function for D over M_k^∞. Here D was a non-arithmetic Cartier divisor on X, so in our case, D is an arithmetic divisor on X. So the metric on $\mathcal{L} \cong \mathcal{O}(\operatorname{div}_{\mathcal{L}}(s))$ gives a smooth partial Weil function for $\operatorname{div}_{\mathcal{L}_{\text{fin}}}(s)$ over M_k^∞, and that is out function $\frac{1}{2}g$. The partial Weil function is $-\log\|s(\cdot)\|$.

So, the function g for a principal arithmetic divisor (f) on X (with $f \in K(X)^\times$) is $-\log|f(\cdot)|$. Further specializing to $X = Y$, and $f = \alpha \in K(X)^\times = K(Y)^\times = k^\times$, $g(\nu) = -\log\|\alpha\|_\nu = -\log|\tau(\alpha)|$.

The appropriate punishment for Arakelov theory is the death penalty.

Note that if $D, E \in \widehat{\text{CDiv}}(Y)$, then $\deg(D+E) = \deg(D) + \deg(E)$ (trivial to verify).

Corollary 30.1.15

For all $D \in \widehat{\text{CDiv}}(Y)$, $\deg D$ depends only on its linear equivalence class.

Then, we have:

Definition 30.1.16

Let $\mathcal{L}$ be a metrized line sheaf on Y. Then $\deg\mathcal{L} = \deg(\operatorname{div}_{\mathcal{L}}(s))$ for any nonzero rational section s of $\mathcal{L}$.

This is well-defined because for any s, s' as above, their divisors differ by a principal divisor (s/s'), and nonzero rational sections exist. Again, $\deg : \widehat{\text{Pic}}(Y) \to \mathbb{R}$ is a surjective group homomorphism.

Math 254B: Arakelov Theory **Spring 2021**

Lecture 38-42: 26 April - 5 May

Professor Paul Vojta Abhishek Shivkumar

Wrapping up Heights

As above, k is a number field, $Y = \operatorname{Spec} \mathcal{O}_k$, V is a projective variety over k, $\pi : X \to Y$ is a projective model for V (and also an arithmetic variety).

Definition 31.1.1

Let $P \in V(k)$, $\sigma : Y \to X$ the corresponding section of π. Let D be an arithmetic divisor on X, λ_D its associated Weil function. Then $h_D(P) = h_{\lambda_D}(P)$ which is equal to $\deg \sigma^* D$ if $P \notin \operatorname{Supp} D$, and is equal to $\deg \sigma^* \mathcal{O}(D)$ unconditionally.

Let $\mathcal{L}$ be a metrized line sheaf on X. Then $h_{\mathcal{L}}(P) = \deg \sigma^* \mathcal{L}$ so that $h_{\mathcal{L}}(P) = h_D(P)$ if $\mathcal{L} \cong \mathcal{O}(D)$.

The usual height machine equivalences apply: for $\mathcal{L}, \mathcal{M} \in \widehat{\operatorname{Pic}}(X)$, $h_{\mathcal{L} \otimes \mathcal{M}}(P) = h_{\mathcal{L}}(P) + h_{\mathcal{M}}(P)$ for all $P \in V(k)$ (additivity). This follows essentially by linearity of degree:

$$h_{\mathcal{L} \otimes \mathcal{M}}(P) = \deg \sigma^*(\mathcal{L} \otimes \mathcal{M}) = \deg \sigma^* \mathcal{L} + \deg \sigma^* \mathcal{M} = h_{\mathcal{L}}(P) + h_{\mathcal{M}}(P)$$

For $f : V_1 \to V_2$, a morphism of projective k-varieties, X_1 and X_2 projective models for V_1 and V_2 respectively, and assume that f extends to a morphism $f : X_1 \to X_2$ over Y. Let $\mathcal{L}$ be a metrized line sheaf on X_2, then $h_{f^*\mathcal{L}}(P) = h_{\mathcal{L}}(f(P))$ for all $P \in V_1(k)$ (functoriality). To see this, let $\sigma_1 : Y \to X_1$ correspond to $P \in V_1(k)$, then $\sigma_1 = f \circ \sigma_1 : Y \to X_2$ corresponds to $f(P) \in X_2(k)$, and $h_{f^*\mathcal{L}} = \deg \sigma^* f^* \mathcal{L} = \deg \sigma_2^* \mathcal{L} = h_{\mathcal{L}}(f(P))$.

For $n \in \mathbb{N}$, $X = \mathbb{P}^n_Y$, $\mathcal{L} = \mathcal{O}(1)$, with $\|s(P)\|_\sigma = \frac{|a_0p_0 + \cdots + a_np_n|}{\max(|p_0|, \cdots, |p_n|)}$ for all $\sigma : k \hookrightarrow \mathbb{C}$ in M_k^∞, where $P = [p_0 : \cdots : p_n] \in \mathbb{P}^n_{\mathbb{C}}$ and $s = a_0x_0 + \cdots + a_nx_n \in H^0(\mathbb{P}^n_{\mathbb{C}}, \mathcal{O}(1))$. Then $h_{\mathcal{L}}(P) = h_k(P)$ for all $P \in V(k)$ (where $V = \mathbb{P}^n_k$). The proof of this is left as an exercise.

We return to heights of algebraic points. Let L/k be a finite extension, $Y_L = \operatorname{Spec} \mathcal{O}_L$. Then there is a canonical bijection $X(Y_L) \to X(L)$ over Y, given by restricting to the generic point of Y_L. So, for all $P \in V(L)$ we have (canonically) a map $\sigma : Y_L \to X$ over Y, and we'd like to define $h_{\mathcal{L}}(P) = \frac{\deg \sigma^* \mathcal{L}}{[L:k]}$. This is because we can let $X_L = X \times_Y Y_L$; then the generic fiber of $\pi_L : X \times_Y Y_L \to Y_L$ is isomorphic (over L) to $V_L := V \times_k L$, and $\pi_L : X_L \to Y_L$ is a model for V_L. Note that V_L need not be a variety over L since V need not be geometrically integral, so this would require a more general definition of model. Then $P \in V_L(L)$ corresponds to a section $\sigma_L : Y_L \to X_L$ of π_L and $q \circ \sigma_L = \sigma$. Then $\sigma^*\mathcal{L} = \sigma_L^*(q^*\mathcal{L})$, so

$$\frac{\deg \sigma^*\mathcal{L}}{[L:k]} = \frac{\deg \sigma_L^* q^*\mathcal{L}}{[L:k]} = \frac{h_{q^*\mathcal{L}}(P)}{[L:k]}$$

In order to do this, we need to check the following:

Proposition 31.1.2

Let k, Y, L, Y_L, and $\rho : Y_L \to Y$ be as above. Then $\deg \rho^* D = [L : k] \deg D$ for all $D \in \mathrm{C\hat{D}iv}(Y)$.

Proof: For all $\nu \in M_k$, let $\deg_\nu D$ denote the contribution to $\deg D$ at ν. For $\nu \in M_k^0$, $\deg_\nu D = -\log \|f\|_\nu$ where $(f) = D$ in some open neighborhood of the point $y \in Y$ corresponding to ν. Note that $f \in k^\times$. Then

$$\sum_{\omega \in M_L, \omega|\nu} \deg_\omega \rho^* D = \sum_{\omega|\nu} -\log \|f\|_\omega = \sum_{\omega|\nu} -\log \|f\|_\nu^{e_\omega f_\omega} = \left(\sum_{\omega|\nu} e_\omega f_\omega\right)(-\log \|f\|_\nu) = [L:k]\deg_\nu D$$

For $\nu \in M_k^\infty$, this equals $\frac{1}{2} g_D(\nu)$, since for all $\sigma : k \hookrightarrow \mathbb{C}$, $Y_\sigma(\mathbb{C})$ is exactly one point, and

$$\sum_{\omega|\nu} \deg_\omega \rho^* D = \sum_{\omega|\nu} \frac{1}{2} g_{\rho^* D}(\omega) = \sum_{\omega|\nu} \frac{1}{2} g_D(\nu) = [L:k]\deg_\nu D$$

since the number of $\omega|\nu$ is $[L : k]$ for any ν.

Putting these cases together,

$$\deg \rho^* D = \sum_{\nu \in M_k} \sum_{\omega|\nu} \deg_\omega \rho^* D = [L:k] \sum_{\nu \in M_k} \deg_\nu D = [L:k]\deg D$$

■

Definition 31.1.3

Let $P \in V(\bar{k})$, L a finite extension of k such that $P \in V(L)$. Let $Y_L = \operatorname{Spec} \mathcal{O}_L$ as always, and let $\sigma_L : Y_L \to X$ correspond to the point $P : \operatorname{Spec} L \to X$. Let D be an arithmetic divisor on X and assume that $P \notin \operatorname{Supp} D$, then $h_D(P) = \frac{1}{[L:k]} \deg \sigma_L^* D$. Note that if λ_D is the Weil function on V associated to D, then $h_D(P) = h_{\lambda_D}(P)$. We may remove the assumption that $P \notin \operatorname{Supp} D$ by replacing D with D' which is linearly equivalent to D.

Let $\mathcal{L}$ be a metrized line sheaf on X. Then $h_{\mathcal{L}}(P) = \frac{\deg \sigma^*\mathcal{L}}{[L:k]}$. Both of these definitions are independent of the choice of $\mathcal{L}$. For a, this follows by the above proposition, for bm this follows from the similar fact that $\deg p^*\mathcal{L} = [L : k] \deg \mathcal{L}$ for all $\mathcal{L} \in \hat{\operatorname{Pic}}(Y)$ which is proved by finding D such that $\mathcal{L} = \mathcal{O}(D)$.

The height machine holds for algebraic points as well. Also, $h_{\mathcal{L}}(P) = h_{\mathcal{L}_k,k}(P) + O(1)$ for all $\mathcal{L} \in \hat{\operatorname{Pic}}(X)$, all $P \in V(\overline{k})$ by comparing the two height machines.

Intersection Theory

We follow Hartshorne's Appendix A in our discussion here. Let k be an algebraically closed field.

Definition 31.2.1

Let X be a quasi-projective variety over k. A *cycle* of codimension p on X is an element of the free abelian group $Z^p(X)$ on the set of (integral) closed codimension p subvarieties of X.

Let $f : X \to X'$ be a morphism of quasi-projective varieties over k, $Y \subseteq X$ a closed subvariety. Then we let $f_*(Y) = [K(Y) : K(f(Y))]\overline{f(Y)}$ if $\dim f(Y) = \dim Y$, and 0 otherwise. This is an element of $Z^{\dim X' - \dim Y}(X')$. This extends by linearity to a well-defined group homomorphism $f_* : Z^p(X) \to Z^{p+\dim X' - \dim X}(X')$.

If X is a nonsingular variety, $p \in \mathbb{Z}_{>0}$, $i : V \hookrightarrow X$ a closed subvariety of codimension $p-1$, $f : \tilde{V} \to V$ the normalization of V, $g \in K(V)^\times = K(\tilde{V})^\times$. Then (g) is a Weil divisor on $\tilde{V}$, so $(g) \in Z^1(\tilde{V})$, so $(i \circ f)_*((g)) \in Z^p(x)$. Let $\operatorname{Rat}^p(X)$ be the subgroup of $Z^p(X)$ generated by $(i \circ f)_*((g))$ for all such V, i, f, g as above, $\operatorname{Rat}^0(X) = (0)$. For all $p \in \mathbb{N}$, we say that two cycles in $Z^p(X)$ are rationally equivalent if they differ by an element of $\operatorname{Rat}^p(X)$. Set $\operatorname{CH}^p(X) = Z^p(X)/\operatorname{Rat}^p(X)$, the *Chow Group* in codimension p of X, and $\operatorname{CH}(X) := \bigoplus_p \operatorname{CH}^p(X)$.

For $p \in \mathbb{N}$, $d = \dim X - p$. Then $Z_d(X) = Z^p(X)$, $\operatorname{Rat}_d(X) = \operatorname{Rat}^p(X)$, $\operatorname{CH}_d(X) = \operatorname{CH}^p(X)$. f_* maps $Z_d(X)$ to $Z_d(X')$.

Example 31.2.2

$\operatorname{CH}^0(X) = \mathbb{Z}$, generated by $[X]$ (the fundamental class), since X is the only closed subvariety of codimension 0. $\operatorname{CH}^1(X) = \operatorname{Cl}(X)$ (the class group of X).

Example 31.2.3

$\mathrm{CH}_d(\mathbb{P}^n) \cong \mathbb{Z}$ for all $0 \le d \le n$, all n. This isomorphism is given by taking the degree (in terms of hyperplane intersections).

Let X be a nonsingular variety over k, Y, Z closed subvarieties of X. Then all irreducible components W of $Y \cap Z$ have $\operatorname{codim} W \le \operatorname{codim} Y + \operatorname{codim} Z$. This follows from the general Hauptidealsatz.

Definition 31.2.4

Closed subvarieties Y and Z of X *meet properly* if all irreducible components W of $Y \cap Z$ satisfy $\operatorname{codim} W = \operatorname{codim} Y + \operatorname{codim} Z$. If Y and Z meet properly, then their intersection cycle $Y.Z$ is the cycle $\sum_W i(Y, Z; W) \cdot W$ where

$$i(Y, Z; W) = \sum_{i=0}^{\infty} (-1)^i \operatorname{length} \operatorname{Tor}_i^A(A/a, A/b)$$

where $A = \mathcal{O}_{a,W}$, and a, b are the ideals in A of Y and Z respectively. $Y.Z \in Z^{p+q}(X)$ where $p = \operatorname{codim} Y$, $q = \operatorname{codim} Z$. Cycles $Y \in Z^p(X)$ and $Z \in Z^q(X)$ meet properly if $Y = \sum n_i Y_i$, $Z = \sum m_j Z_j$, where Y_i and Z_j meet properly for all i, j. If so, then $Y.Z$ is defined by bilinearity.

Theorem 31.2.5: Chow's Moving Lemma

Let X be a nonsingular quasi-projective variety over k. Then every rational equivalence class in X is big enough to contain a cycle that meets any other cycle properly. Therefore, an intersection product on $\mathrm{CH}(X)$ is well-defined.

Theorem 31.2.6: The BIG Theorem

Let C be the category of nonsingular quasi-projective varieties over k. Then, with the above definitions, for all $X \in C$, the intersection pairing on X is well-defined (as a bilinear map $\mathrm{CH}^p(X) \times \mathrm{CH}^p(X) \to \mathrm{CH}^p(X)$), commutative, associative, and makes $\mathrm{CH}(X)$ a graded ring with unit $[X]$.

Let $f : X \to X'$ be a morphism in C, Γ_f the graph of f, $\varphi : X \times X' \to X$, $\psi : X \times X' \to X'$ the projections. For prime cycles Y' In X', let $f^*(Y') = \varphi_*(\Gamma_f.\psi^{-1}(Y')) = \varphi_*(\Gamma_f.(X \times Y'))$. Then f^* givves a well-defined functorial graded homomorphism $\mathrm{CH}(X') \to \mathrm{CH}(X)$.

Let $f : X \to X'$ be a morphism in C. Then f_* is a well-defined homomorphism of graded groups, shifting degrees by $\dim X' - \dim X$.

If $f : X \to X'$ is a proper morphism in C, then $f_*(Y.f^*Z) = f_*(Y).Z$ for all $Y \in \mathrm{CH}(X)$, $Z \in \mathrm{CH}(X')$.

Reduction to the diagonal: $Y.Z = \Delta^*(Y \times Z)$ where $\Delta : X \to X \times X$ is the diagonal, for all prime cycles $Y, Z \in \mathrm{CH}(X)$.

Let $Y \subseteq X$ be a closed subvariety of X, Z an effective Cartier divisor on X. If Y and Z meet properly, then $Y.Z$ is i_* of i^*Z on Y, where $i : Y \hookrightarrow X$ is the inclusion map.

Note that, in the above, we allowed X to be quasi-projective, but usually, X should be projective. $\mathrm{CH}^p(\mathbb{A}^n) = 0$ for all p, n since rational equivalence allows us to move all subvarieties to infinity (which therefore vanish).

Let $d = \dim X$, then $\mathrm{CH}^d(X)$ is the free group on the set of closed points of X up to equivalence, and we have a linear map $\deg : \mathrm{CH}^d(X) \to \mathbb{Z}$ given by $P \mapsto 1$ for all $P \in X(k)$, or more generally, $P \mapsto [\kappa(P) : k]$ if k is not algebraically closed. This is the same as the map $\mathrm{CH}^d(X) \xrightarrow{\pi_*} \mathrm{CH}^0(\operatorname{Spec} k) \cong \mathbb{Z}$ where $\pi : X \to \operatorname{Spec} k$ is the structural map. For the degree to be well-defined, X must be projective.

We want to extend intersection theory to arithmetic varieties. Some difficulties arise: namely, that Chow's lemma doesn't extend since many residue fields are finite. Moreover, we need to accommodate archimedean places in order for deg to be well-defined. We will have $\hat{\mathrm{CH}}^d(X) \xrightarrow{\pi_*} \hat{\mathrm{CH}}^1(\operatorname{Spec} \mathbb{Z}) = \hat{\mathrm{CDiv}}(\operatorname{Spec} \mathbb{Z}) \xrightarrow{\deg} \mathbb{R}$. Another issue is that we don't have resolution of singularities in characteristic p or for arithmetic varieties (mixed characteristic) when $\dim \leq 3$. This version of intersection theory is useful in the function field case, provided we address the resolution of singularities in char p, $\dim > 3$.

The connection to K-theory might be Bloch's formula. Tensoring by $\mathbb{Q}$ seems related to Grothendieck-Riemann-Roch.

Arakelov intersection theory avoids these difficulties. The lack of a moving lemma is resolved by using some clever extensions of intersection theory using K-theory. The issue of singularities is resolved by working in $\mathrm{CH}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ which can handle singular varieties. The issue of infinite places is resolved by using complex differential geometry on $X_\sigma(\mathbb{C})$ for all $\sigma \in M_k^\infty$ (or, equivalently, on $X(\mathbb{C}) = \coprod_\sigma X_\sigma(\mathbb{C})$).

Complex Differential Forms

Elements of $\hat{\mathrm{CH}}^p(X)$ will have archimedean components constructed using complex differential forms on $X_\sigma(\mathbb{C})$ for all σ.

Recall that $z = x + iy$, $\overline{z} = x - iy$, $dz = dx + idy$, $d\overline{z} = dx - idy$. We have that $x = \frac{z+\overline{z}}{2}$ and $y = \frac{z-\overline{z}}{2i}$, $dx = \frac{dz+d\overline{z}}{2}$, $dy = \frac{dz-d\overline{z}}{2i}$. Moreover, we have that $\frac{\partial}{\partial z} = \frac{1}{2}\left(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}\right)$ and $\frac{\partial}{\partial \overline{z}} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right)$. If $\Omega \subseteq \mathbb{C}$ is open, $f : \Omega \to \mathbb{C}$ is a function, f is holomorphic iff f is differentiable and $\frac{\partial f}{\partial \overline{z}} = 0$ (this is just the Cauchy-Riemann criterion).

For differentiable $f : \Omega \to \mathbb{C}$, define $\partial f = \frac{\partial f}{\partial z} dz$ and $\overline{\partial} f = \frac{\partial f}{\partial \overline{z}} d\overline{z}$. These are one forms on Ω. Note that

$$df = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy = (\partial + \overline{\partial}) f$$

by routine manipulations, so $d = (\partial + \overline{\partial})$.

I think we're trying to get to Dolbeault cohomology or Hodge theory or something.

This discussion was for one complex variable; for $\Omega \subseteq \mathbb{C}^n$, fix coordinate functions $z_1, \cdots, z_n$, write $z_k = x_k + iy_k$, $\overline{z_k} = x_k - iy_k$, $\partial f = \sum_i \frac{\partial f}{\partial z_i} dz_i$, and $\overline{\partial} f = \sum_i \frac{\partial f}{\partial \overline{z}_i} d\overline{z}_i$. For $I = (i_1, \cdots, i_p)$ a p-tuple of indices with $i_1 < \cdots < i_p$, then $dz_I = dz_{i_1} \wedge \cdots \wedge dz_{i_p}$ and $d\overline{z}_I = d\overline{z}_{i_1} \wedge \cdots \wedge d\overline{z}_{i_p}$. $\wedge$ is anticommutative in degree 1, so $dz_i \wedge d\overline{z}_j = -d\overline{z}_j \wedge dz_i$, $dz_i \wedge dz_j = -dz_j \wedge dz_i$, etc. Therefore, $dz_I \wedge d\overline{z}_J = (-1)^{pq} d\overline{z}_J \wedge dz_I$ where $J = (j_1, \cdots, j_q)$, I as above.

Definition 31.3.1

A *complex* (p,q)*-form* on $\Omega \subseteq \mathbb{C}^n$ is a sum $\sum_{I,J} \Psi_{IJ} dz_I \wedge d\overline{z}_J$ where the sum is over all p-tuples I, q-tuples J as above, and $\Psi_{IJ} : \Omega \to \mathbb{C}$ is a function for all I, J. The form is continuous, smooth, C^1, C^2, etc. if all of the Ψ_{IJ} have the same property respectively.

∂f as above is $(1,0)$-form, $\overline{\partial} f$ is a $(0,1)$-form. f itself is $(0,0)$-form. Note that ∂ of a (p,q)-form is naturally a $(p+1,q)$-form, and $\overline{\partial}$ of a (p,q)-form is a $(p,q+1)$-form, e.g

$$\partial\left(\sum_{I,J} \Psi_{IJ} dz_I \wedge d\overline{z}_j\right) = \sum_{I,J} (\partial \Psi_{IJ}) \wedge dz_I \wedge d\overline{z}_J$$

Again, $d = \partial + \overline{\partial}$ is the usual d from real analysis, and a real operator. Also, define $d^c = \frac{i}{4\pi}(\overline{\partial} - \partial)$ which is also a real operator. Then

$$dd^c = \frac{i}{4\pi}(\partial + \overline{\partial})(\overline{\partial} - \partial) = \frac{i}{2\pi}\partial\overline{\partial}$$

where we distribute the product and use the fact that $\partial^2 = \overline{\partial}^2 = 0$ by anticommutativity of $\wedge$ (and anticommutativity of ∂ with $\overline{\partial}$).

This smells like "f holomorphic $\implies \log|f|$ harmonic" or something like that.

Proposition 31.3.2

If $f : \Omega \to \mathbb{C}$ is holomorphic, then $-dd^c \log|f|^2 = 0$.

Proof:

$$-dd^c \log|f|^2 = -\frac{i}{2\pi}\partial\overline{\partial}\log|f|^2 = -\frac{i}{2\pi}(\partial(\overline{\partial}\log f) - \overline{\partial}(\partial \log \overline{f})) = 0$$

where both terms on the right hand side vanish since they are ∂ or $\overline{\partial}$ of an antiholomorphic or holomorphic function respectively. ■

Proposition 31.3.3: Chain Rule

Let $\Omega, \Omega' \subseteq \mathbb{C}^n$ be open sets, with complex coordinates $z_1, \cdots, z_n$ and $w_1, \cdots, w_n$ respectively. Let $g : \Omega' \to \Omega$, $f : \Omega \to \mathbb{C}$ be differentiable functions. Then

$$\frac{\partial}{\partial w_j}(f \circ g)(P) = \sum_{i=1}^{n} \frac{\partial f}{\partial z_i} g(P) \frac{\partial g_i}{\partial w_j}(P) + \sum_{i=1}^{n} \frac{\partial f}{\partial \overline{z_i}} g(P) \frac{\partial \overline{g}_i}{\partial w_j}(P)$$

for all j, all $P \in \Omega'$, and similarly with w_j replaced by $\overline{w_j}$ throughout. If g is holomorphic, then one of the sums vanishes (since the partials with respect to $\overline{z_i}$ vanish.)

g_i is the i^{th} coordinate of g.

Definition 31.3.4: Pullbacks

With notation as above,

$$g^*(df) = d(f \circ g) = \sum_{j=1}^{n} \sum_{i=1}^{n} \frac{\partial f}{\partial z_i} \frac{\partial g_i}{\partial w_j} + \frac{\partial f}{\partial \overline{z_i}} \frac{\partial \overline{g}_i}{\partial w_j} dw_j + \sum_{j=1}^{n} (\cdots) d\overline{w}_j$$

so $g^*(dz_i) = dg_i$ and $g^*(d\overline{z}_i) = d\overline{g}_i$. If g is holomorphic, then $g^*(dz_i) = \partial g_i$ and $g^*(d\overline{z}_i) = \overline{\partial} \overline{g}_i$.

Note that pullbacks are functorial, e.g, $(g \circ f)^* = h^* g^*$.

Lemma 31.3.5

$g^* d = dg^*$, e.g, g^* and d commute as operators. Equivalently, $g^* d\psi = dg^* \psi$ for all (p, q)-forms or n-forms ψ. Also, if g is holomorphic, then $g^* \partial = \partial g^*$, $g^* \overline{\partial} = \overline{\partial} g^*$.

Recall that a complex manifold is defined similarly to a real manifold, but with open subsets homeomorphic to open subsets of $\mathbb{C}^n$ and with holomorphic (rather than simply analytic or differentiable) transition maps.

Proof: The first equality follows from differential geometry, the second and third follow from splitting the first equality into components of degrees $(1, 0)$ and $(0, 1)$. ■

Corollary 31.3.6

d, ∂, and $\overline{\partial}$ are well-defined operators on forms on a complex manifold, and the concept of a (p, q)-form is well-defined on a complex manifold.

In polar coordinates $z = re^{i\theta}$ (in one complex variable), $d^c = \frac{r}{4\pi} \frac{\partial}{\partial r} \otimes d\theta - \frac{1}{4\pi r} \frac{\partial}{\partial \theta} \otimes dr$.

Example 31.3.7

$$dd^c|z|^2 = dd^c r^2 = d\left(\frac{r}{4\pi}2rd\theta\right) = \frac{1}{2\pi}d(r^2d\theta) = \frac{r}{\pi}dr \wedge d\theta$$

Then we can integrate:

$$\int \alpha(z)dd^c|z|^2 = \int_\theta \int_r \alpha(z)\frac{r}{\pi}drd\theta$$

This involved choosing an orientation $dr \wedge d\theta$ to $drd\theta$; the former anticommutes and the latter commutes.

In rectangular coordinates,

$$dd^c|z|^2 = \frac{i}{2\pi}\partial\overline{\partial}(z\overline{z}) = \frac{i}{2\pi}\partial(zd\overline{z}) = \frac{i}{2\pi}dz \wedge d\overline{z}$$

Writing $dz = dx + idy$, we have that

$$dd^c|z|^2 = \frac{i}{2\pi}(dx + idy) \wedge (dx - idy) = \frac{1}{\pi}dx \wedge dy$$

Lemma 31.3.8: Integral Table

Let Ω be an open neighborhood of 0 in $\mathbb{C}$, and let $\alpha, \beta : \Omega \setminus \{0\} \to \mathbb{C}$ be smooth functions. If $\alpha = -c \log|z|^2 + \tilde{\alpha}$ where c is a constant and $\lim_{z\to 0}\tilde{\alpha}(z)$ converges, and β extends to a smooth function on Ω, then $\alpha dd^c\beta$ is absolutely integrable in a neighborhood of 0, and $\lim_{\epsilon\to 0^+}\int_{|z|=\epsilon}\alpha d^c\beta = 0$.

If $\lim_{z\to 0}\alpha(|z|)$ converges, $\beta = -\log|z|^2 + \tilde{\beta}$ where $\tilde{\beta}$ extends to a smooth function on Ω, then $\alpha dd^c\beta$ is absolutely integrable in a neighborhood of 0, and $\lim_{\epsilon\to 0^+}\int_{|z|=\epsilon}\alpha d^c\beta = -\alpha(0)$.

Proof: Absolute integrability of $\alpha dd^c\beta$ boils down to absolute integrability of $-\log|z|^2$, which is equivalent to (in polar coordinates) $\int_0^{2\pi}\int_0^\rho(-\log r^2)rdrd\theta < \infty$ for some small $\rho \leq 1$, and this is true because $(-\log r^2)r \to 0$ as $r \to 0^+$. For the second assertion,

$$\lim_{\epsilon\to 0^+}\int_{|z|=\epsilon}\alpha dd^c\beta = \lim_{\epsilon\to 0^+}\int_{|z|=\epsilon}\alpha\left(\frac{r}{4\pi}\frac{\partial\beta}{\partial r}\right)d\theta = 0$$

where the final equality is due to the fact that $dr|_{|z|=\epsilon} = 0$ and $\frac{\alpha r}{4\pi} \to 0$, while $\frac{\partial\beta}{\partial r}$ is bounded.

For the second part, by the above, we may assume that $\tilde{\beta} = 0$, so $\beta = -\log|z|^2$. Then $dd^c\beta = 0$, so we get absolute integrability of $\alpha dd^c\beta$. Since $\beta = -\log r^2$, $d^c\beta = -\frac{d\theta}{2\pi}$, and therefore

$$\lim_{\epsilon\to 0^+}\int_{|z|=\epsilon}\alpha d^c\beta = -\lim_{\epsilon\to 0^+}\int_{|z|=\epsilon}\alpha\frac{d\theta}{2\pi} = -\alpha(0)$$

where the second equality is by the fact that the second integral is essentially the average of α on the circle $|z| = \epsilon$, which converges to $\alpha(0)$ as $\epsilon \to 0$ (up to sign). ■

Definition 31.3.9

Let X be a smooth complex projective curve, $D = \sum_P n_P P$ a divisor on X, and let Σ be a subset of $X(\mathbb{C})$ containing $\operatorname{Supp} D$. Let $g : \Sigma \to \mathbb{C}$ be a function, then $g(D) = \sum_P n_P g(P)$. A *metrized* divisor on X is a pair $D = (D_{\text{fin}}, g_D)$ where D_{fin} is a divisor on X and $\frac{1}{2}g_D$ is a smooth Weil function for D on X. For metrized divisors D, E on X, we say that D and E intersect properly if $\operatorname{Supp} D_{\text{fin}} \cap \operatorname{Supp} E_{\text{fin}} = \emptyset$. If D and E intersect properly, then their *local intersection pairing* is

$$\langle D.E\rangle = g_D(E) + \int_{X(\mathbb{C})\setminus(\operatorname{Supp} D_{\text{fin}} \cap E_{\text{fin}})} g_E dd' g_D$$

By the above lemma, the integral in this expression converges absolutely.

Proposition 31.3.10

Let D and E be metrized divisors on X, and assume that they meet properly. Then $\langle D.E\rangle = \langle E.D\rangle$.

Proof: By linearity, we may assume that D and E are distinct prime divisors P and Q respectively.. What if $D_{\text{fin}} = 0$ and $g_D \neq 0$? Then g_D is a smooth function on all of $X(\mathbb{C})$, and we may write $D = D_1 - D_2$ where $D_{1,\text{fin}} = D_{2,\text{fin}} = P$ for some $P \notin \operatorname{Supp} E_{\text{fin}}$, and $g_{D_1} - g_{D_2} = g_D$. We need to show that

$$g_P(Q) - g_Q(P) = \int_{X(\mathbb{C})\setminus(P\cup Q)} g_P dd^c g_Q - g_Q dd^c g_P$$

We will do this by evaluating

$$\int_{X(\mathbb{C})\setminus(P\cup Q)} d(g_P d^c g_Q - g_Q d^c g_P)$$

in two different ways. First, we may evaluate this expression directly using $dg_P \wedge d^c g_Q = dg_Q \wedge d^c g_P$; to see that this holds, write

$$dg_P \wedge d^c g_Q = (\partial g_P + \overline{\partial} g_P) \wedge \frac{i}{4\pi}(\overline{\partial} g_Q - \partial g_Q) =$$
$$\frac{i}{4\pi}(\partial g_P \wedge \overline{\partial} g_Q - \partial g_P \wedge \partial g_Q + \overline{\partial} g_P \wedge \overline{\partial} g_Q - \overline{\partial} g_P \wedge \partial g_Q)$$

The middle two terms in the above expansion vanish for degree reasons, so the resulting expression is symmetric in P and Q, so

$$\int_{X(\mathbb{C})\setminus(P\cup Q)} d(g_P d^c g_Q - g_Q d^c g_P)$$

Expanding $\int_{X(\mathbb{C})\setminus(P\cup Q)} d(g_P d^c g_Q - g_Q d^c g_P)$ using this identity produces the right hand side of the claim.

Let $\varphi : U \to \mathbb{C}$ and $\psi : V \to \mathbb{C}$ be holomorphic local coordinate maps, where U and V are neighborhoods of P and Q respectively, with $\varphi(P) = \psi(Q) = 0$. Let $X_\epsilon := X(\mathbb{C}) \setminus (\varphi^{-1}(D_\epsilon) \cup \psi^{-1}(D_\epsilon))$ where D_ϵ is the open ball of radius ϵ centered at 0. Then

$$\int_{X(\mathbb{C})\setminus(P\cup Q)} d(g_P d^c g_Q g_Q d^c g_P) = \lim_{\epsilon\to 0^+} \int_{X_\epsilon} d(g_P d^c g_Q g_Q d^c g_P)$$

By Stokes' theorem, the latter term is equal to

$$-\lim_{\epsilon\to 0^+} \left(\int_{|\varphi|=\epsilon} + \int_{|\psi|=\epsilon} \right) (g_P d^c g_Q - g_Q d^c g_P)$$

where the minus sign comes from orientation. The integral table lemma tells us that this expression is in turn equal to $g_P(Q) - g_Q(P)$, from which the result follows. ■

Definition 31.3.11: Arithmetic Surfaces

An *arithmetic surface* is an arithmetic variety of dimension 2. It is *generically smooth* (resp. *regular*) if it has that property as an arithmetic variety (resp. scheme). Note that regular implies generically smooth.

Definition 31.3.12

Let X be an arithmetic surface. Then $X_\mathbb{C} = X \times_\mathbb{Z} \mathbb{C}$. Let D be an arithmetic divisor on X. Then $D_\mathbb{C}$ is the metrized divisor $(D'_\mathbb{C}, g_D)$ where $D'_\mathbb{C}$ is the restriction of D_{fin} to $X_\mathbb{C}$.

Definition 31.3.13

Let X be a regular arithmetic surface. Note that we have resolution of singularities in mixed characteristic when $\dim X \leq 3$ so regularity is not an essential restriction. Let D and E be arithmetic divisors on X that intersect properly (so D_{fin} and E_{fin} intersect properly, which implies $D_\mathbb{C}$ and $E_\mathbb{C}$ intersect properly). Then the *intersection number* $(D.E)$ is defined to be

$$(D.E) = \deg(D_{\text{fin}}.E_{\text{fin}}) + \frac{1}{2}\langle D_\mathbb{C}.E_\mathbb{C}\rangle$$

where $\langle D_\mathbb{C}.E_\mathbb{C}\rangle$ is summed over the irreducible components of $X_\mathbb{C}$, and $D_{\text{fin}}.E_{\text{fin}} \in Z^2(X)$ is defined to be

$$\sum_{x\in \operatorname{Supp} D_{\text{fin}} \cap \operatorname{Supp} E_{\text{fin}}} i(D_{\text{fin}}, E_{\text{fin}}; x) \cdot x$$

where $i(D_{\text{fin}}, E_{\text{fin}}; x)$ is defined bilinearly as follows: let D and E be prime Weil divisors on X, locally defined by $f, g \in \mathcal{O}_{X,x}$ respectively at x; then $i(D,E;x) = \sum(-1)^i \operatorname{Tor}_i^{\mathcal{O}}(\mathcal{O}/(f), \mathcal{O}/(g))$ where $\mathcal{O} = \mathcal{O}_{X,x}$. However since $\mathcal{O}/(f)$ has a free resolution $\mathcal{O} \to \mathcal{O} \xrightarrow{\cdot f} \mathcal{O} \to \mathcal{O}/(f) \to 0$, $\operatorname{Tor}_i = 0$ for all $i > 1$ and since f is a nonzerodivisor in $\mathcal{O}/(g)$, $\operatorname{Tor}_1 = 0$. So $i(D,E;x) = \operatorname{length}(\mathcal{O}/(f) \otimes_{\mathcal{O}} \mathcal{O}/(g)) = \operatorname{length}(\mathcal{O}/(f,g))$. Also $\deg(\sum n_x \cdot x) = \sum n_x \log|\kappa(x)|$.

In order for this to make sense, we need the following:

Proposition 31.3.14

Let D be an arithmetic divisor on X, $f \in K(X)^\times$. If D and (f) intersect properly, then $(D.(f)) = 0$.

Proof: It will suffice to prove this when $D = (Z, 0)$ where Z is an irreducible component of a fiber of $X \to \operatorname{Spec} \mathbb{Z}$ and in the case where $D_{\text{fin}} = P$ where $P \in X(\overline{\mathbb{Q}})$ and $\frac{1}{2} g_D$ is any smooth Weil function for P. ■

What a beautiful result to end on. Really made the climb worth the effort.