Algebraic Curves

Professor: H.W. Lenstra, Jr.

Math 274, Fall Semester, 1995

Head Scribe: Ezra Miller

The following notes are from the class *Algebraic Curves* given by Hendrik Lenstra at U.C. Berkeley in the fall of 1995. They are a concatenation of informal class notes taken by the students in the class. They have not been read by Professor Lenstra (or Ezra Miller), and Prof. Lenstra takes no responsibility for the contents.

Math 274: Algebraic curves.

H. W. Lenstra, Jr. (879 Evans, office hours MF 4:15–5:15, tel. 643–7857, e-mail hwl@math).
Fall 1995, MWF 3–4, 65 Evans.

This is an introductory course on algebraic curves over arbitrary fields. It is expected that it will be taught regularly in the future, as Math 255. The course occupies an intermediate position between Math 254 (Number theory) and Math 256 (Algebraic geometry). It is recommended for students who like to acquire a good understanding of a special class of varieties before embarking upon the more general and abstract approach of scheme theory that is offered in Math 256. Another major difference with Math 256 is that we shall work over base fields that are not necessarily algebraically closed, including number fields and finite fields. This will make the course attractive for students with an interest in the arithmetic aspects of algebraic geometry. Another link with number theory is found in the structural analogy between function fields of curves and number fields.

I expect to cover the following topics: algebraic curves, singularities, function fields, valuations, line bundles, the theorem of Riemann-Roch, Hurwitz's formula, curves of low genus, elliptic curves (merely scratching the surface here!), hyperelliptic curves, projective embeddings, the canonical curve, zeta functions of curves over finite fields; in addition, I hope to address a selection of the following: the Riemann hypothesis for curves over finite fields, applications to coding theory, construction of Jacobian varieties.

Each student who wishes to obtain credit for the course must participate in the "scribe" system, whereby each lecture is transcribed in plain TeX and made available to the other students (and, possibly, to future instructors of Math 255). In addition, there will be regular homework assignments. There will not be a final examination.

Prerequisites for the course are Math 250A and either Math 250B or the consent of the instructor. Familiarity with the basic properties of groups, rings, and fields is essential. Students not acquainted with slightly more advanced subjects such as modules, exact sequences, localization, tensor products, Galois theory, transcendence degree, and the language (*only* the language!) of categories, are expected to be willing and able to learn about these on the side. More advanced topics from algebra that are needed will be developed in class, including valuation theory. Prior exposure to algebraic number theory or algebraic geometry will not hurt, but will not be assumed.

Some of the literature on the subject, such as Hartshorne and Fulton below, emphasizes the geometric aspects and places the subject in the general context of solving systems of polynomial equations, often over algebraically closed fields. Other books, such as Artin and Stichtenoth, deal primarily with the algebraic aspects, notably the arithmetic of function fields. In the present course I will attempt to do justice to both points of view, much of the motivation being geometric and most proof techniques algebraic. There is no required textbook.

Literature:

R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Chapters I (especially section 6) and IV.

W. Fulton, *Algebraic curves, an introduction to algebraic geometry*, Benjamin, Reading, Mass., 1969.

E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, New York, 1967.

H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.

More literature may be given in class.

Lecture 1 (August 28, 1995).
Scribe: David Jones

How does this course (math 255?) compare with math 254 and 256?

Math 256 deals primarily with algebraically closed fields, $k = \overline{k}$.

Math 254 deals primarily with finite fields and algebraic number fields ($[k : \mathbf{Q}] < \infty$).

This class will deal with **Function fields of algebraic curves**, K/k.

In this course we will see the correspondence between algebraic curves and function fields. Algebraic curves will be vague and intuitive objects. Function fields will be rigorously developed.

Basic object of study. Fix a field k. A **function field** (of a curve over k) is a field extension K with $k \subset K$ such that:

1. K is finitely generated as a field extension of k;
2. tr.deg$(K/k) = 1$; (i.e. $\exists t \in K$ s.t. t is not alg.$/k$ and K is alg. $/k(t)$.)
3. $\overline{k} \cap K = k$ (inside $\overline{K}$).

Let k be any field.

"Curve over k" $\stackrel{\text{def}}{=}$ a one-dimensional variety over k.

But what are varieties and what does dimension mean?

For now we will assume $k = \overline{k}$.

An **algebraic set** is a subset V of k^n (for some $n \geq 0$) for which there exist $f_1, ..., f_m \in k[X_1, ..., X_n]$ such that $V = \{x = (x_i)_{i=1}^n \in k^n \mid f_1(x) = ... = f_m(x) = 0\}$.

Note: V is empty iff some linear combination of the f_i's gives 1.

Note: $x_1^2 + x_2^2 + 1 = 0$ has solutions over $\mathbf{C}$ but none over $\mathbf{R}$ so $k = \overline{k}$ is important.

A **morphism** $V \to V'$ is a map "given by n' polynomials, $g_1, ..., g_{n'}$ in n variables over k."

At this point, we have a category. Specifically, we have the notion of an isomorphism: a morphism such that there is another morphism in the opposite direction so that composition of the two in either direction is the identity.

Ex: Let $V : y^2 = x^3 - x$, $V' = k^1$. Define a map $V \to V'$ by $(x, y) \mapsto x$.

This morphism is certainly not an isomorphism because it is not even bijective.

Ex: Let $V : y = x^2$, $V' = k^1$. Define a map $V \to V'$ by $(x, y) \mapsto x$, and define another map by $V' \to V$ by $x \mapsto (x, x^2)$.

These two morphisms are inverses so each is an isomorphism and we should view the two varieties as being the same object.

We will eventually attach invariants to these varieties: one example is the genus. Two isomorphic varieties will then have the same genera.

Fix some variety V. The **coordinate ring** $A(V)$ of V is the ring of all morphisms $f : V \to k^1$.

Every $f \in A(V)$ is a polynomial in the n coordinates $x_1, ...x_n$. (Hence the name "coordinate ring".)

So we get a surjective map $k[X_1, ..., X_n] \to A(V)$. In fact, since the f_i's are 0 on V, we get a surjection $k[X_1, ..., X_n]/(f_1, ..., f_m) \to A(V)$.

The question we want to answer is...

Is this map an isomorphism?

Unfortunately, the answer is no.

Let R be a commutative ring, and let $I \subset R$ be an ideal. Then $\sqrt{I} = \{r \in R \mid \exists n \in \mathbf{Z}_{\geq 0} \text{ s.t. } r^n \in I\}$.

This definition gives us a map $k[X_1, ..., X_n]/\sqrt{(f_1, ..., f_m)} \xrightarrow{\sim} A(V)$.

Given a morphism $V \to V'$, we get a homomorphism (ring hom., identity on k) $A(V') \to A(V)$ given by $X_i \mapsto g_i(X_1, ..., X_n)$.

We also want our algebraic sets to be *irreducible*. What does this mean?

A non-empty algebraic set $V \subset k^n$ is **reducible** if there are algebraic sets $V_1, V_2 \subset k^n$ different from V such that $V = V_1 \cup V_2$. Otherwise, V is **irreducible**.

There is a theorem (depending on the polynomial ring being Noetherian) that every algebraic set can be written as a finite union of irreducible algebraic sets.

An irreducible algebraic set is called an **affine variety** (over k).

Exercise: V is irreducible $\iff$ $A(V)$ is a domain.

Next time we will consider:

1. Non-algebraically closed fields.
2. Dimensions of varieties
3. Non-affine varieties.

Lecture 2 (August 30, 1995).
Scribe: Ezra Miller

As usual we let k be a field and K be a function field over k.

Consider the case when $k = \overline{k}$. Then the set of (isomorphism classes of) affine varieties corresponds bijectively with the set of (isomorphism classes of) domains of finite type over k. In fact, the function which to each affine variety associates its function field is a contravariant functor, so a morphism $V \to V'$ corresponds to a homomorphism $A(V) \leftarrow A(V')$ fixing k. ("Contravariant" means that the arrows have been reversed.) We now consider what happens in the three cases mentioned at the end of Lecture 1.

1. General k: We relax the conditions on k, and no longer require it to be algebraically closed. It is possible now to get different equations over k which, from the point of view of solutions in k, look exactly the same. However, we don't want to call two curves such as $x^2 + y^2 + 1 = 0$ and $x^4 + y^4 + 1 = 0$ isomorphic simply because k is too small to get enough solutions (the example to be thinking about is $k = \mathbf{R}$). There are a number of suggestions we could entertain to try to squeeze out an appropriate definition of a variety.

Suggestion 1. Use as a definition the one involving domains of finite type over k.

Suggestion 2. Agree that the coefficients of your polynomial lie in k, while your zero sets lie in $\overline{k}$.

Suggestion 3. View the zeros as lying in *any* extension field L/k. A variety V becomes a recipe

$$L \mapsto V(L) \subset L^n$$

for producing a zero set given any L/k. A morphism of $\{L \mapsto V(L)\}$ to $\{L' \mapsto V(L')\}$ would consist of maps $f : L \to L'$ and $g : V(L) \to V(L')$ such that $f(L) \mapsto g(V(L))$. This is the basis for scheme theory.

For general k, one often requires the variety V not just to be irreducible (so $A(V)$ is a domain) but **absolutely irreducible**, so that in fact $\overline{k} \otimes_k A$ is a domain.

Example: Consider the curve $x^2 + y^2 = 0$. Then $A = \mathbf{Q}[X,Y]/(x^2 + y^2)$ is a domain, while

$$\overline{\mathbf{Q}} \otimes_{\mathbf{Q}} A = \overline{\mathbf{Q}}[X,Y]/(x^2 + y^2) \cong \overline{\mathbf{Q}}[X,Y]/(x + yi) \times \overline{\mathbf{Q}}[X,Y]/(x - yi)$$

is not. One could require $L \otimes_k A$ to be a domain for all L/k, but it is an interesting exercise in commutative algebra to show that $\overline{k}$ suffices.

2. Dimension: We have a couple of possibilities for defining dimension.

Suggestion 1. We can use the transcendence degree $tr.deg._k Q(A)$ of the quotient field of A over k.

Suggestion 2. Do it the scheme-theoretic way: look at the spectrum of A. Then the dimension is defined in terms of the longest sequence of irreducible subsets of $Spec(A)$ (in the Zariski topology). This is what is known as the **Krull dimension** of a ring A, i.e. the supremum over $n \in \mathbf{Z}$ for which there exist prime ideals $\mathfrak{p}_i$ with $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ in A (the containments here are strict). Note: It is possible to construct Noetherian rings with infinite Krull dimension.

We will stick to the first definition, and to those objects with dimension 1. The fact that $dim \geq 1$ means that A has a nonzero prime ideal, so that A is not a field. That $dim \leq 1$ implies that any nonzero prime ideal is maximal.

Example: $\overline{k} \otimes_k k[X] = \overline{k}[X]$ with no relations. For those that like relations, we could just as easily have used $k[X,Y]/(Y)$ in place of $k[X]$.

The word "curve" will always refer to the case when $dim = 1$.

If $dim(A) = 0$ then A is a field containing k. Now $k \subset A$ is a field extension that as a ring is generated by some finite set over k, which happens only when $[A : k]$ is finite. Keep in mind that taking reciprocals is not allowed, since we're generating A as a ring, not as a field. But if we want $\overline{k} \otimes_k A$ to be a domain, then of necessity, $k = A$ in this case.

Example: $k = \mathbf{Q}$, $A = \mathbf{Q}(i) = \mathbf{Q}[x]/(x^2+1)$. Then $i \otimes 1 - 1 \otimes i$ is a zero divisor, since

$$\begin{aligned}(i \otimes 1 - 1 \otimes i)(i \otimes 1 + 1 \otimes i) &= (i^2 \otimes 1) - (1 \otimes i^2) \\ &= ((-1) \otimes 1) - (1 \otimes (-1)) \\ &= -(1 \otimes 1) + (1 \otimes 1) \\ &= 0.\end{aligned}$$

More generally,

$$\overline{\mathbf{Q}} \otimes_{\mathbf{Q}} A = \overline{\mathbf{Q}}[x]/(x^2+1) \cong \overline{\mathbf{Q}}[x]/(x+i) \times \overline{\mathbf{Q}}[x]/(x-i)$$

in this example.

Example: $y^2 = x^3 - x$. Then $A = k[x,y]/(y^2 - x^3 + x)$. Note that this example is somewhat analogous to $\mathbf{Z}[\sqrt{d}]$, with d squarefree. In the present case we have $k[x][\sqrt{y}] = k[x][\sqrt{x^3 - x}]$. When we draw the "picture" of the curve, we frequently use affine space, but it is usually nicer to add a point at infinity. In the case of this curve over $\mathbf{C}$, we get a torus. For elliptic curves, this allows us to make the curve into a group.

Lecture 3 (September 1, 1995).

Scribe: Lawren Smitline

Recall: k is *any* field.

Last time, we saw the correspondence between $\{$(absolutely irreducible) affine varieties over $k\}$ and $\{$domains A of finite type over $k\}$. For such A, $\bar{k} \otimes_k A$ is also a domain.

The dimension of a variety is 1 if and only if the transcendence degree of $Q(A)$ is 1.

Intuition about gluing affine varieties together:

An important characteristic of the global topology of a differentiable manifold is that it is defined in terms of local homeomorphisms to Euclidean spaces.

$\mathbf{P}^n(k) = \{[x_0, \ldots, x_n] : \exists i,\ x_i \neq 0\} = k^{n+1} - \{\mathbf{0}\}/$ (scalar multiplication).

For example, $\mathbf{P}^1(k) = \{[x, y] : x, y \in k,\ (x, y) \neq (0, 0)\} = \{[x, 1]\} \cup \{[1, 0]\}$.

How can we obtain $\mathbf{P}^1$ by gluing?
Geometrically, we have $\mathbf{P}^1 - \{\infty\} = \mathbf{A}^1 \supset \mathbf{A}^1 - \{0\} \subset \mathbf{A}^1 \cup \{\infty\} - \{0\} = \mathbf{P}^1 - \{0\}$.
Algebraically, $k[x] \subset k[x, x^{-1}] \supset k[x^{-1}]$.

Now we have to fix a problem. Entire functions on compact varieties are constant. For example, maps from $\mathbf{C} \cup \{\infty\} \to \mathbf{C}$ are constant.

We also don't want to see the "scars" from the gluing.

Notice that all the rings we want to glue together correspond to coordinate rings giving the same field of fractions.
We pick a point, P on each piece $\mathbf{A}^1 \cup \{\infty\} - \{0\},\ \mathbf{A}^1, \mathbf{A}^1 \cup \{\infty\}$.
WOLOG, $P = 3$. We have $3 : k[x] \to k$, with kernel $(x - 3)$ and also the map $3 : k[x^{-1}] \to k$, with kernel $(x^{-1} - \frac{1}{3})$.

The local rings on the affine pieces agree.

A **local ring** is a ring R such that $R - R^\times$ is an ideal. R is local if R has exactly one maximal ideal.

If A is a ring and $\mathfrak{p}$ is a prime ideal, then let $A_\mathfrak{p}$ be the ring $(A - \mathfrak{p})^{-1}A$.

$\mathbf{A}^n(k) = k^n \subset \mathbf{P}^n(k)$, by $(x_1, \ldots, x_n) \mapsto (1, x_1, \ldots, x_n)$. In the study of projective varieties, we examine only zero sets of homogeneous polynomials.

A variety is an absolutely irreducible integral separated scheme of finite type over k.
Question: Is a variety over k always quasiprojective?
Question: Given a function field, is there a curve you can deduce?

Suppose $k = \bar{k}$. Then there is a (contravariant functor?) correspondence between smooth projective curves over k and finitely generated field extensions K over k of transcendence degree 1.

Problems with smoothness when one has singularities:

For example, the curve $y^2 = x^3 + x^2$ has a cusp, or at least the real part does.

If $k = \bar{k}$, then a point P on a curve is smooth iff the local ring at P is a *discrete valuation ring.*

Tune in next time for "a new beginning". We'll see that certain fields correspond to curves and points on the curves correspond to local rings.

Lecture 4 (September 6, 1995).
Scribe: Nick Meyer

Today we will begin exploring the correspondence between certain fields and curves; we will find that points on the curve correspond to local rings of the field. In short, $P \in C \longleftrightarrow \mathcal{O}_P \subset K(C) = K$.

Valuation rings:

Definition: Let K be a field. A **valuation ring of** K is a subring $R \subset K$ such that $\forall x \in K - R, x^{-1} \in R$. A **valuation ring of** K/k is a valuation ring of K such that $k \subset R$. Finally, a **valuation ring** is a domain that is a valuation ring of its field of fractions.

Example: $R = K$. The "trivial" valuation ring.

Definition: A **discrete valuation ring** of K is a valuation ring R of K for which K^*/R^* is infinite cyclic as a group.

Example: $k \subset R = k[[t]] \subset K = k((t))$, where $k[[t]]$ and $k((t))$ are the power and Laurent series rings in t, respectively. Note that $R^* = \{f \in R \mid f(0) \neq 0\}$; $K^* = t^{\mathbf{Z}} \cdot R^*$; $R - \{0\} = t^{\mathbf{Z}\geq 0} \cdot R^*$.

It turns out that K^*/R^* is a totally ordered abelian group, with $aR^* \geq bR^*$ if $aR \subseteq bR$. In fact, K^*/R^* is **torsion-free**.

Properties of valuation rings:

Proposition: Any valuation ring R is **local**; i.e., it has exactly one maximal ideal. This maximal ideal is, of course, $R - R^*$.

Proof: It suffices to prove that $R - R^*$ is an ideal. This is quite easy. First, it's nonempty, since $0 \notin R^*$. Second, if $a \in R - R^*, r \in R$, then $ra \notin R^*$, obviously. Finally, $a, b \in R - R^* \Rightarrow a + b \in R - R^*$. (Proof: $a + b = a(1 + b/a)$. If $b/a \in R$, then we're fine; if b/a is not in R, a/b is, and since $a + b = b(1 + a/b)$, we're still fine).

All valuation rings are local, but not all local rings are valuation rings; for example, $k[x, y]_{<x,y>}$ is local, but is not a valuation ring.

Proposition: Let R be a ring. Then R is a discrete valuation ring (d.v.r.) iff R is a principal ideal domain with, up to multiplication by units, exactly one prime element.

Proof:

($\Leftarrow$): $R - 0 = R^* \times \pi^{\mathbf{Z}\geq 0}$, where π is our prime element. Note that this is a unique decomposition, since R is a p.i.d., by assumption. Then $K^* = R^* \times \pi^{\mathbf{Z}}$ is the unique decomposition in the field of fractions.

($\Rightarrow$): $K^*/R^* = (\pi R^*)^{\mathbf{Z}}$, where π is the generator of the infinite cyclic group K^*/R^*. We can choose either π or π^{-1} to be in R; WLOG, choose $\pi \in R$. Note that $\pi \notin R^*$. Now $\pi_n \in R \iff n \geq 0$.

This fact can be useful. For example: let $I \subset R$ be any nonzero ideal. Pick an element $u \cdot \pi^n \in I$ with n as small as possible. Then $u \cdot \pi^n$ divides any element of I. So $I = R \cdot u \cdot \pi^n = R \cdot \pi^n$.

Example: $\mathbf{Z}_{(37)} = n/m : n, m, \in \mathbf{Z}, m \notin 37\mathbf{Z}$ is a discrete valuation ring.

Example: Let k be a field, t a transcendental over k. We will proceed to describe all valuation rings of $k(t)$ over k.

Let $k \subset R \subset k(t)$ be a valuation ring.

Case 1: $t \in R$. Then $\begin{array}{ccc} k[t] & \subset & R \\ \cup & & \cup \\ \mathfrak{p} & \subset & \mathfrak{m} \end{array}$

where $\mathfrak{m}$ is the maximal ideal of R, and $\mathfrak{p} = k[t] \cap \mathfrak{m}$ is a prime ideal of $k[t]$. Notice that $k[t] - \mathfrak{p} = S \subset R^* \Rightarrow k[t]_{\mathfrak{p}} = S^{-1}k[t] \subset R$.

Case 1a: $\mathfrak{p} = 0$. Then $k[t]_{\mathfrak{p}} = k(t) \subset R \subset k(t)$.

Case 1b: $\mathfrak{p} = (f), f \in k[t]$, f an irreducible polynomial. Then $k[t]_{(f)}$, the localization of $k[t]$ at (f), is a d.v.r. contained in R. So $k(t)^*/k[t]^*_{(f)}$ is infinite cyclic, and maps surjectively onto $k(t)^*/R^*$. The torsion-freeness of $k(t)^*/R^*$ means that this map is an isomorphism; therefore $k[t]_{(f)} = R$.

Case 2: $t \notin R$. Then $u - 1/t \in R - R^*$. We have $\begin{array}{ccc} k[u] & \subset & R \\ \cup & & \cup \\ (u) & \subset & \mathfrak{m} \end{array}$.

So $R = k[u]_{(u)} = \{d(u)/h(u) | d(0)/h(0) \text{is well-defined}\} = \{f/g : f, g \in k[t], \deg f \leq \deg g\}$ ($\iff$ $f(\infty)/g(\infty)$ well-defined).

Proposition: Every non-trivial valuation ring R of $k(t)$ over K is discrete. Also, the set of those R's is isomorphic to the set of monic irreducible polynomials in $k[t]$, plus ∞.

We now quickly explain why these objects are called valuation rings. The natural mapping $K^* \to K^*/R^* \equiv \mathbf{Z}$ induces a map $v : R - 0 \to \mathbf{Z} \geq 0$. ($v(0)$ is defined to be $+\infty$). It can be easily seen that $v(a + b) \geq \min v(a), v(b)$. In the case where the d.v.r. R corresponds to an irreducible polynomial f, $v(r \in R)$ counts the number of factors of f in r. Where r corresponds to the point "at infinity", $v(g/h) = \deg h - \deg g$.

Lecture 5 (September 8, 1995).
Scribe: Matt Baker

Today we're going to prove some theorems.

Recall: $K \supset R$ valuation ring.

Problem: Given $K \subset L$ an extension of fields, $R \subset K$ a valuation ring, is there a valuation ring T of L such that $T \cap K = R$?

It turns out that such T exists, and we will try to characterize what properties it has.

Theorem 1: If K is a field with valuation ring R, and $L \supset K$ is a field extension, then $\exists$ a valuation ring T of L with $T \cap K = R$.

For the proof of this, let K be a field, Ω an algebraically closed field, and let Σ be the set of all pairs (B, g), where B is a subring of K and $g : B \to \Omega$ is a ring homomorphism. Since this will all be rather vacuous if $\Sigma = \emptyset$, one can check as an exercise that $\Sigma = \emptyset \Leftrightarrow$ char $\Omega \neq$ char $K > 0$. We put a partial order on Σ by saying that $(B, g) \leq (B', g')$ if $B \subset B'$ and $g' \mid_B = g$. If $\Sigma \neq \emptyset$, then Zorn's Lemma tells us that Σ has at least one maximal element (T, h). Now we apply the following Theorem:

Theorem 2: If (B, g) is maximal then B is a valuation ring of K with maximal ideal equal to $\ker(g)$.

Now we have a map $g : R \to \overline{R/\mathfrak{m}} = \Omega$, and we can assume that $R \subset T \subset L$, and $h : T \to \Omega$ is an extension of g. If $x \in (K \cap T) - R$, then $x^{-1} \in \mathfrak{m}$, so $g(x^{-1}) = 0$, hence $h(x^{-1}) = 0$ and $h(x)$ has trouble defining itself. We conclude that such troublesome x's in $(K \cap T) - R$ cannot actually exist, so we must have $T \cap K = R$. Thus the second theorem implies the first, and we have reduced the problem to establishing Theorem 2. To do so, we first need a lemma:

Lemma: Let B be a local subring of a field K, with maximal ideal $\mathfrak{m} \subset B$, and let $x \in K^*$. Then $\mathfrak{m}[x] \neq B[x]$ or $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.

Proof: Suppose the lemma is false. Then

$$1 = u_0 + u_1 x + \cdots + u_m x^m, u_i \in \mathfrak{m}$$

$$1 = v_0 + v_1 x^{-1} + \cdots + v_n x^{-n}, v_i \in \mathfrak{m}.$$

Assume that the above m, n are minimal. Also, WLOG, assume that $n \leq m$. Multiplying the second equation by x^n, we have

$$v_1 x^{n-1} + v_2 x^{n-2} + \cdots + v_n = (1 - v_0) x^n,$$

where $1-v_0$, not living in the maximal ideal, is forced to be in B^*. Therefore we can divide the equation through by $(1-v_0)$ to get a new equation:

$$v_1' x^{n-1} + v_2' x^{n-2} + \cdots + v_n' = x^n.$$

Multiplying this through by x^{m-n} gives the relation

$$v_1' x^{m-1} + \cdots + v_n' x^{m-n} = x^m.$$

Now if we plug the left-hand-side of this expression into our putatively minimal equation involving x^m, we get a new equation which contradicts the minimality of m. This proves the lemma.

Proof of Theorem 2(See also Atiyah-MacDonald, p.65):

Since $g(B)$ is a subring of a field and therefore an integral domain, the ideal $\mathfrak{m} = \ker(g)$ is prime. Now if $s \in B - \mathfrak{m}$, then $g(s)$ will not be zero, so we can extend g to a homomorphism $g' : B_{\mathfrak{m}} \to \Omega$ by putting $g'(b/s) = g(b)/g(s)$ for all $b \in B, s \in B - \mathfrak{m}$. But the pair (B, g) was chosen to be maximal, so we must have $B = B_{\mathfrak{m}}$, and therefore B is a local ring with $\mathfrak{m}$ as its maximal ideal. It remains to show that if $x \neq 0$ is an element of K, then either $x \in B$ or $x^{-1} \in B$. Since we now know that B is a local ring, we can apply our lemma, and we see that we may as well assume that the ideal $\mathfrak{m}[x]$ is not equal to $B' = B[x]$. So then $\mathfrak{m}[x]$ is contained in a maximal ideal $\mathfrak{m}'$ of B', and it must be the case that $\mathfrak{m}' \cap B = \mathfrak{m}$, since it is a proper ideal of B and contains $\mathfrak{m}$. Therefore the embedding of B in B' induces an embedding of the field $k = B/\mathfrak{m}$ into the field $k' = B'/\mathfrak{m}'$. In addition, we have $k' = k[\overline{x}]$, where $\overline{x}$ is the image of x in k', hence $\overline{x}$ is algebraic over k and k' is then a finite algebraic extension of k. Now since $\mathfrak{m}$ is the kernel of g, we get an induced embedding $\overline{g} : k \to \Omega$. Since Ω is algebraically closed, we can extend $\overline{g}$ to an embedding $\overline{g}'$ of k' into Ω. If we now compose $\overline{g}'$ with the natural homomorphism from B' to k', we get a new map $g' : B' \to \Omega$ which extends g. Since (B, g) was chosen to be maximal, we must have $B' = B$, hence $x \in B$ as desired.

One application of these results is in the following useful theorem.

Theorem: Let A be a subring of a field K. Then the integral closure of A in K is equal to the intersection of all the valuation rings of K containing A.

Pf: "$\subset$": Suppose x is in the integral closure of A in K. Then we can write $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, with $a_i \in A$. We want to know that $x \in$ any R. Now the $x = 0$ case is trivial. Otherwise, divide the above equation by x^{n-1} to get

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

Therefore $x \in A[x^{-1}]$. Now pick any valuation ring R, and we have two cases. If $x \in R$, then we're done. If $x^{-1} \in R$, then $x \in A[x^{-1}] \subset R$, so we're also done. That finishes off one direction.

"$\supset$": Suppose we have some x which is NOT integral over A. We would like to construct an R which 'misses' x. To do this, we look at $A[x^{-1}]$. Now it cannot be that $x \in A[x^{-1}]$, or else multiplying by an appropriate power of x gives an integrality relation for x. Therefore x^{-1} is not in $A[x^{-1}]^*$, so there is a maximal ideal $\mathfrak{m}$ of $A[x^{-1}]$ containing x^{-1}. If we let $\Omega = \overline{A[x^{-1}]/\mathfrak{m}}$, then there is a ring homomorphism $f : A[x^{-1}] \to \Omega$, and we can then find a maximal pair (R, g) as before, where R we now know to be a valuation ring of K containing $A[x^{-1}]$, and g is a homomorphism from R to Ω which extends f. I claim that this is the desired R which cannot contain x. For $g(x^{-1}) = 0$, so having $x \in R$ would cause major problems if one tried to define $g(x)$. This proves the theorem.

Note: In the situations that we will be concerned with in this course, we won't really need the axiom of choice, since we'll be given that K is a finite extension of the field of fractions of A.

We conclude with a vague set of remarks. Last time, we found a bijective correspondence:

nontrivial valuation rings of $k(t)$ over $k \longleftrightarrow f \in k[t]$ monic, irreducible $\cup\infty$.

Recall that if $R \leftrightarrow f$, then $R/\mathfrak{m} \cong k[t]/(f)$. If $R \leftrightarrow \infty$, then $R/\mathfrak{m} \cong k$.

Now if $k = \overline{k}$, then f irreducible $\Leftrightarrow f = t - \alpha, \alpha \in k$. Then we have valutation rings of $k(t)$ over $k \longleftrightarrow$ the projective line over k.

For general k, we have that the projective line is in correspondence with the set of R's with residue class field $= k$. For example, if $k = \mathbf{R}$, then irreducibles of degree 1 $\longleftrightarrow$ real projective line. For irreducibles of degree 2, we need to look at the orbit of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ acting on the complex projective line. A general strategy in this course will be that to understand the points on some curve C which maps to the projective line, we will want to understand the set of valuation rings extending $k(t)$.

Next time: e's and f's.

Lecture 6 (September 11, 1995).

Scribe: Diane Maclagan

In this lecture we study a field K, a valuation ring $R \subseteq K$, and an extension field $L \supseteq K$. We are interested in valuation rings $T \subseteq L$ such that $T \cap K = R$.

Definition: The residue class degree, $f(T/R)$, is defined to be $f = [T/m_T : R/m_R]$. We are assuming here that $m_R = m_T \cap K$. This is a consequence of $T \cap K = R$. $f(T/R)$ is sometimes also written $f(L/K)$. We are interested in the case where f is finite.

Definition: The ramification index, $e(T/R)$, is defined to be $e = [\Delta : \Gamma]$, where $\Gamma = K^*/R^*$ and $\Delta = L^*/T^*$. $[\Delta : \Gamma] = |L^*/K^*.T^*|$.

The geometric interpretation of this is as follows: If C is a curve with function field K, and L, a finite extension of K, is the function field of some curve D, then e is a measure of number of points on D above C. If $e = 1$ we say that the point is unramified, while if $e > 1$, it is ramified. We usually expect only finitely many points where ramification occurs.

Note that for algebraically closed base fields, $f = 1$. If the base field is not algebraically closed, we can think of the valuation rings not as points on the curve, but as conjugacy classes of points, so they have size, and if Q is a point over P, then $f = |Q|/|P|$.

We will show that for curves

$$\sum_{Q \text{ over given } P} ef = n = [L : K]$$

This is not true of general valuation rings. We start with the following proposition:

Proposition: If L is finite over K then the product $ef = e(T/R)f(T/R) \leq [L : K]$

Proof: Let $B \subseteq T$ map bijectively to a basis of T/m_T over R/m_R, noting that $B \subseteq T^*$. Let $S \subseteq L^*$ be a set of coset representatives mod $K^*.T^*$. So the cardinality of B is f, and the cardinality of S is e. It suffices to prove that $(b.s)_{b \in B, s \in S)}$ is linearly independent over K.

Suppose $\sum_{b \in B, s \in S)}^{<\infty} k_{bs} bs = 0$ where not all the $k_{bs} = 0$. Choose $b_0 s_0$ with $k_{b_0 s_0} \neq 0$ and $v(k_{b_0 s_0}$ minimal. ($v : L^* \to \Delta$, and we leave out b because it is a unit).

$$\sum_{b \in B} k_{b s_0} b s_0 + \sum_{\substack{b \in B \\ s \in S s \neq s_0}} k_{bs} bs = 0$$

Now divide by $k_{b_0 s_0} s_0$.

$$\sum_{b \in B} \frac{k_{b s_0} b s_0}{k_{b_0 s_0} s_0} + \sum_{\substack{b \in B \\ s \in S s \neq s_0}} \frac{k_{bs} bs}{k_{b_0 s_0} s_0} = 0$$

All the terms have positive valuation, so belong to T. All the terms in the second sum have non-zero valuation because s and s_0 are in different cosets mod $T^* K^*$, and thus are in $\mathbf{m}_T$.

Taking this sum mod $\mathbf{m}_T$ the second sum disappears, so, writing $\lambda_b = \frac{k_{bs_0}s_0}{k_{b_0 s_0}s_0}$,

$$\sum_{b\in B} \lambda_b (b \bmod \mathbf{m}_T) = 0$$

This means that $\lambda_b = 0 \,\forall \lambda_b$ since the b are linearly independent, but $\lambda_{b_0} = 1$. This is a contradiction, so the result follows.

Corollary: If K is a finitely generated field extension of a field k of transcendence degree 1 ($\mathrm{trdeg}_k K = 1$) then every non trivial valuation ring of K/k is discrete and the intersection of all these valuation rings equals $\{\alpha \in K : \alpha \text{ is a algebraic over } k\}$ and this is a finite extension of k.

Proof: Let T be a nontrivial valuation ring of K/k, and let R be its restriction to $k(t)$ ($R = T \cap k(t)$). Then R is nontrival by exercise 4 of the homework, and so R is discrete, as we showed earlier that every valuation ring of $k(t)$ was discrete.

Let Δ be the value group of K with respect to T. Δ is a totally ordered abelian group containing $\mathbf{Z}$, and is of finite index e there, so $\Delta = \mathbf{Z}$. T is thus discrete.

Now

$$\bigcap T = \bigcap_{\substack{T \supset k, \\ T \text{val. ring of } K}} T = \{\text{integral closure of } k \text{ in } K\}$$

Since k is a field, this is the algebraic elements.

We now need to show that $[\cap T : k] < \infty$. Take any T. $T/\mathbf{m}_T$ is of finite degree over $R/\mathbf{m}_R$, which we know from last time is over finite degree over k, so $T/\mathbf{m}_T$ is a finite extension of k. Writing $l = \bigcap T$, $l \subseteq T$, and it injects into $T/\mathbf{m}_T$, so we have embedded l in a finite extension of k, so $[l : k] < \infty$, where $l = \overline{k} \cap K$.

l is the *exact field of constants.* This phrase is usually used when we say "k is the exact field of constants" meaning $k = l$.

Projective curves cannot be adequately defined by rings, as every non constant function has poles and zeroes.

Let R be a discrete valuation ring in a field K with maximal ideal $\mathbf{m}$. Then the completion of R is

$$\hat{R} = \varprojlim R/\mathbf{m}^n = \{\{a_n\} \in \prod_{n=0}^{\infty} R/\mathbf{m}^n : \forall n \geq 0 \ a_n \bmod \mathbf{m}^{n-1} = a_{n-1}\}$$

This is a projective limit. $\hat{R}$ is a ring, and there is a natural injective ring homomorphism $R \to \hat{R}$.

Recommended reading for this section is the relevant chapters of Atiyah-Macdonald.

Example: Let k be a field, $R = k[t]_{(t)}$. Then $R/\mathbf{m}^n = k[t]/(t^n)$ and $\hat{R} = k[[t]]$, the power series ring.

Properties of $\hat{R}$

$\hat{R}$ is a domain. It is a discrete valuation ring in its field of fractions, which is $\hat{K} = K \otimes_R \hat{R}$. $e(\hat{R}/R) = f(\hat{R}/R) = 1$. $\hat{\hat{R}} = \hat{R}$, and R is complete if the natural map $R \to \hat{R}$ is an isomorphism.

Lecture 7 (September 13, 1995).
Scribe: Wayne Whitney

Recall that last time we were discussing extensions of valuation rings: given a valuation R with field of fractions K, and an extension of fields $L \supset K$, we defined a valuation ring $T \subset L$ to be an extension of R if $T \cap K = R$. Then we defined cardinals $e(T/R) = |L^*/T^*K^*|$ and $f(T/R) = [T/m_T : R/m_R]$.

Some Remarks on E and F

From the multiplicativity of the index of subgroups and of the degree of field extensions, we have the following: If $M \supset L$ is an extension field of L and $V \subset M$ is a valuation ring extending T, then V obviously extends R and $e(V/R) = e(V/T)e(T/R)$ and $f(V/R) = f(V/T)f(T/R)$.

Last time we proved that if $[L : K] < \infty$ then $e(T/R)f(T/R) \leq [L : K]$ and in particuluar $e(T/R) < \infty$ and $f(T/R) < \infty$. Later it will arise that in the situations we are interested in,

$$\sum_{T \mapsto R} e(T/R)f(T/R) = [L : K]$$

where the sum is taken over all valuations rings T of L extending R.

Completions

Let R be a ring and $I \subset R$ an ideal of R. Then we define the I-adic completion of R, $\hat{R}$, as $\hat{R} = \varprojlim R/I^n$. In the case that R is a local ring, it is natural to take $I = m_R$ and consider the m_R-adic completion of R. We will be interested in the the case $R \subset K$ is a discrete valuation ring of a field K.

Examples of Completions

$R = k[t]_{(t)}$, then $\hat{R} \cong k[[t]]$.

$R = k[t]_{(t-\alpha)}$ for some $\alpha \in k$, then $\hat{R} \cong k[[t - \alpha]]$.

$R = k[t^{-1}]_{(t^{-1})}$, then $\hat{R} \cong k[[t^{-1}]]$.

If $k \neq \bar{k}$, and f is a separable, irreducible polynomial over k, with $\deg f > 1$, take $R = k[t]_{(f)}$. Then it is an exercise to show that $\hat{R} \cong_k l[[t]]$, where $l = k[t]/(f)$.

Here we have considered the completions of the local rings of the function field $k(t)$. The completions of the local rings of the functions fields of other curves will be similar, as we shall see.

A last example: $R = \mathbf{Z}_{(p)}$. Then $\hat{R} = \varprojlim \mathbf{Z}/p^n\mathbf{Z} = \mathbf{Z}_p$, the ring of p-adic integers. We have $\mathbf{Z}_p \cong \mathbf{Z}[[t]]/(t-p)$.

More Completions

Again, let $R \subset K$ be a discrete valuation ring. Then $\hat{R}$ is a domain, with field of fractions $\hat{K} \cong K \otimes_R \hat{R}$. Two examples: if $\hat{R} = k[[t]]$, then $\hat{K} = k[[t]][t^{-1}] \cong k((t))$. And if $\hat{R} = \mathbf{Z}_p$, then $K = \mathbf{Q}_p$.

Now we give a topological construction of $\hat{K}$. R is a discrete valuation ring, so we have an associated valuation $v : K^* \to \mathbf{Z}$. From v we construct a metric d on K: for x, $y \in K$, define $d(x,y) = 2^{-v(x-y)}$, with the convention that $v(0) = \infty$, so that $d(x,x) = 0$. The choice of 2 is arbitrary; any positive real number will suffice. d gives topology on K, in which $d(x,0)$ is small $\iff$ $x \in m_R^l$ for some large $l \in \mathbf{Z}$. In fact, the powers of m_R form a basis for the open sets containing 0.

Then the topological completion of K with respect to d has a natural field structure which is isomorphic to $\hat{K}$. Furthermore the closure of R in $\hat{K}$ is isomorphic to $\hat{R}$.

Now consider the field extension $K \subset \hat{K}$. Then the valuation ring $\hat{R}$ extends R, and we have $e(\hat{R}/R) = f(\hat{R}/R) = 1$.

A Question Was Asked

A little thought shows that $\hat{K} \cong \varprojlim_{n \in \mathbf{Z}} K/(m_R)^n$, and that $\hat{K}/\hat{R} \cong K/R$. An example: for $R = \mathbf{Z}_{(p)}$, $\mathbf{Q}/\mathbf{Z}_{(p)} \cong \mathbf{Z}[p^{-1}]/\mathbf{Z} \cong \{p\text{-power roots of unity in } \mathbf{C}\}$.

We have the exact sequence:

$$0 \to \mathbf{Z}_p \to \mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p \to 0$$

where $\mathbf{Z}_p$ is compact, $\mathbf{Q}_p$ is locally compact, and $\mathbf{Q}_p/\mathbf{Z}_p$ is discrete.

And now a statement I didn't understand: "$\mathbf{Q}_p$ is self-dual and $\chi(\mathbf{Z}_p) = \mathbf{Q}_p/\mathbf{Z}_p$".

Structure of a Complete DVR

Let $R \subset K$ be a complete discrete valuation ring with valuation v. Then choose a set $B \subset R$ such that $0 \in B$ and the natural map $B \to R/m_R$ is a bijection. Also choose for each $n \in Z$ an element $\pi_n \in K$ with $v(\pi_n) = n$. For example, take $\pi_n = \pi^n$, where π is a uniformizing element of R, that is $m_R = \pi R$.

Then every element of R has a unique expansion as $\sum_{n=0}^{\infty} b_n \pi_n$, where $b_n \in B$, and for any choice of the b_n, that series converges to an element of R. For K we have the analagous statement with $\sum_{n=-l}^{\infty} b_n \pi_n$ for some $l \geq 0$.

The proof of this is straightforward: for example, let $r \in R$. Then $r = x_0\pi_0$ for some $x \in R$, and $x_0 \equiv b_0 \pmod{m_R}$ for some $b_0 \in B$. That is $r = b_0\pi_0 + r_1$ where $r_1 \in m_R$. Again, $r_1 = x_1\pi_1$ for some $x_1 \in R$, and $x_1 \equiv b_1 \pmod{m_R}$ for some $b_1 \in B$. That is, $r = b_0\pi_0 + b_1\pi_1 + r_2$, where $r_2 \in m_R^2$. Proceeding in this fashion, we have $r = \sum_{n=0}^{\infty} b_i\pi_i$.

Finite Extensions of Complete DVR's

Theorem Let $R \subset K$ be a complete discrete valuation ring, let $L \supset K$ be a field extension of K, and let T be a valuation ring of L extending R. Suppose that $e = e(T/R)$ and $f = f(T/R)$ are finite. Then $[L : K] = ef < \infty$, T is complete, T is the unique valuation ring of L extending R, and T is the integral closure of R in L.

Proof Choose a set $B \subset R$ as in the previous section. Also choose a set $A \subset T$ such that the natural map $A \to T/m_T$ is injective and has image a R/m_R-basis of T/m_T. So $|A| = f$.

Let $D = \{\sum_{a\in A} b_a a | b_a \in B\}$. Then $D \subset T$ and the natural map $D \to T/m_T$ is bijective.

As e is finite, T is a discrete valuation ring. So let π_T, π_R be uniformizing elements of T and R, respectively. Let v_T, v_R be the valuations corresponding to T and R respectively. Then $v_T(\pi_R) = e$ by the definition of $e(T/R)$. So for $n = ei + j$, with $0 \leq j < e$, take $\pi_n = \pi_R^i \pi_T^j$; we have $v_T(\pi_n) = n$.

We can apply the discussion from the previous section to $\hat{T}$: any $t \in \hat{T}$ has a unique representation as $t = \sum_{n=0}^{\infty} d_n\pi_n$, where $d_n \in D$. Then write $n = ei + j$ and write $d_n = \sum_{a\in A} b_{aij} a$. So we have

$$t = \sum_{0\leq j<e, a\in A}^{0\leq i<\infty} b_{aij} a \pi_R^i \pi_T^j = \sum_{0\leq j<e, a\in A} (\sum_{i=0}^{\infty} b_{aij}\pi_R^i) a \pi_T^j.$$

For each j and a, the inner sum is an element of R. Therefore we see that $\hat{T}$ is a free R-module with basis $a\pi_T^j$ and rank $e|A| = ef$.

We will complete this proof next time.

Lecture 8 (September 15, 1995).
Scribe: Ben Steinberg

Theorem: Given $K \subset L$ an extension of fields, $R \subset K$ a complete valuation ring, $T \subset L$ a valuation ring of L over R ($T \cap K = R$).

$e < \infty, f < \infty$. Then:

a) $[L : K] = ef$,

b) T is a complete DVR, T is the integral closure of R in L, and the **only** valuation ring of L over R.

Proof: Last time: We showed T is a DVR, $\hat{T}$ is free of rank ef as an R-module with basis taken from T.

So $\hat{T} \subset T \subset \hat{T}$ so $T = \hat{T}$.

So T is free of rank ef. Let π_R be the generator of the maximal ideal of R. Then T_{π_R} is also free of rank ef over R_{π_R}. But $L = T_{\pi_R}, K = R_{\pi_R}$ (since $u\pi_T^n$ for some $n > 0$, u a unit of T).

So $[L : K] = ef$.

Now since T is finite over R as a module, T is integral over R. So the integral closure or R in L equals the integral closure of T in L. But this is T since T is a valuation ring of L and hence integrally closed.

So $T =$ the integral closure of $R \subset$ any non-trivial valuation ring of L extending R. But T is a maximal valuation ring in L since T is discrete.

Corollary: If R is a complete DVR and $L \supset K$ is any algebraic extension, then R has exactly one extension to a valuation ring of L.

Proof: We know from an old result that there is at least one, so let's show there's at most one. It suffices to consider the case $[L : K]$ since two distinct such valuation rings will differ in a finite extension.

Let T_1, T_2 be two such. But $e_i f_i \leq [L : K] \leq \infty$ so by the theorem $T_1 = T_2$.

So in particular we have the following diagrams;

Let L be finite over K. The we get $K^* \to \mathbf{Z}$ and $L^* \to 1/e\mathbf{Z}$ with the obvious maps between these arrows.

Thus we have a surjection $K^{alg*} \to \mathbf{Q}$.

Exercise: Show $L \cong K^n$ where L is given the valuation topology and K^n is given the product topology ($[L : K] = n$). This is also true for T over R.

Hint: Show that the topology on K is independent of the choice of bases, then use the bases from the proof of the theorem.

Theorem: Let R be a DVR of a field K, with completion $\hat{K}(= K \bigotimes_R \hat{R})$ and let $L \supset K$ be any finite field extension. Then there exists bijections between the sets;

$A = \{T | T \text{ is a valuation ring of } L \text{ extending } R\}$

$B = \{\text{field embeddings over } K \text{ of } L \to \hat{K}^{alg}\}/\{\text{Aut }_{\hat{K}}\hat{K}^{alg}\}$

$C = Spec(L \bigotimes_K \hat{K})$

Examples: $L = K[x]/(f)$. Then $B = \{\text{zeroes of f in } \hat{K}^{alg}/\sim R\}$.

But $Spec(L \bigotimes_K \hat{K}) \cong \hat{K}[x]/(f)$

which are the monic irreducible factors of f in $\hat{K}[x]/(f)$.

This theorem is analagous to the fact proved by Kummer that for most primes p in $\mathbf{Z}$ in $\mathbf{Q}[x]/(f)$ primes lying above p correspond to irreducible factors of f mod p in $\mathbf{F_p[x]}$.

Proof: Given $T \in A$, first note T is a DVR. Then $L \subset L\hat{K}$ in $\hat{L} = L \bigotimes_T \hat{T} \hookrightarrow \hat{K}^{alg}$ over K. Note in fact $L\hat{K} = \hat{L}$ since $L\hat{K}$ is finite over K.

Let $\varphi \in B$, then $\varphi : L \hookrightarrow \hat{K}^{alg}$. Also $id : \hat{K} \hookrightarrow \hat{K}$ agree on K. So $\varphi \bigotimes id : L \bigotimes_K \hat{K} \to \hat{K}^{alg}$. The kernel of this map is in C

Let $\wp \in C$. Then since $L \subset L \bigotimes_K \hat{K} \to (L \bigotimes_K \hat{K})/\wp$ a domain finite over $\hat{K}$, a field. So $\wp$ is maximal and hence we can extend this map to an embedding into $\hat{K}^{alg}$.

Finally, if $\varphi \in B$, i.e. $\varphi : L \hookrightarrow \hat{K}^{alg}$ then take φ^{-1} of the unique extension of $\hat{R}$ to $\hat{K}^{alg}$.

Exercise: Show the appropriate maps are inverses.

Note since the second set is finite, all these sets are finite.

Next Time: We'll show $\prod((L \bigotimes \hat{T}) \cong (L \bigotimes_K \hat{K})/\sqrt{0}$ where T runs over the above set and $\sum e(T/R)f(T/R) \leq [L : K]$.

Lecture 9 (September 18, 1995).
Scribe: Emiliano Gómez.

We were proving the following theorem:

Theorem: Let R be a discrete valuation ring of a field K, and L a finite field extension of K. Then we have bijections (see last lecture) between the following three sets:

$\{T \mid T \text{ is a valuation ring of } L \text{ extending } R, \text{ i.e. } T \cap K = R\}$

$\{K\text{-embeddings } L \longrightarrow \hat{K}^{alg}\}/\sim \hat{K}$

$\text{Spec}(L \bigotimes_K \hat{K})$

Also, these sets are finite, and $\prod_T \hat{L}^T \cong_{\hat{K}} (L \bigotimes_K \hat{K})/\sqrt{(0)}$. Also,

$\sum_T e(T/R)f(T/R) \leq [L : K]$, and if $L \supset K$ is separable, then $\sqrt{(0)} = (0)$, and the above inequality becomes an equality.

Proof of the last statements (the bijections are left for us to prove):

The middle set is finite because $[L : K]$ is finite. Another proof of the finiteness is:

$\dim_{\hat{K}} L \bigotimes_K \hat{K} = \dim_K L = [L : K] < \infty$, so $L \bigotimes_K \hat{K}$ satisfies the ascending and descending chain conditions on ideals. It is an Artin ring (see ch.8 of Atiyah & MacDonald). Thus $\mathrm{Spec}(L \bigotimes_K \hat{K})$ is finite. Next, $(L \bigotimes_K \hat{K})/\sqrt{(0)} = (L \bigotimes_K \hat{K})/\bigcap_{\varrho \ prime} \varrho \cong \prod_\varrho (L \bigotimes_K \hat{K})/\varrho = \prod_T \hat{L}^T$.

Here the first isomorphism is a consequence of the Chinese Remainder Theorem, which applies because Artin rings have dimension zero, and so every prime ideal is maximal. Hence any two distinct prime ideals must be coprime.

If L is separable over K, then $L \cong K[X]/(f)$, where f is irreducible and separable. So we have

$L \bigotimes_K \hat{K} \cong \hat{K}[X]/(f) \cong \prod_g \hat{K}[X]/(g)$, the product taken over monic polynomials g of $\hat{K}[X]$ which divide f. We see in this case that $\sqrt{(0)} = (0)$. Next,

$e(T/R)f(T/R) = e(\hat{T}/\hat{R})f(\hat{T}/\hat{R}) = [\hat{L} : \hat{K}]$. So the desired inequality now follows from

$\sum_T [\hat{L} : \hat{K}] \leq [L : K]$. Here we sum over the completions of L with respect to the distinct valuation rings T extending R. This completes the proof.

Remark: In fact, one has $\sum_T e(T/R)f(T/R)g(T/R)$, where $g(T/R)$ = lenght of $(L \bigotimes_K \hat{K})_\varrho$ as a module over itself, if $T \leftrightarrow \varrho$. Here the ϱ's are the prime ideals of $L \bigotimes_K \hat{K}$. The latter, being an Artin ring, is the product of its prime localizations. $g(T/R)$ is a power of p, where $p = \mathrm{char}K$. Note that in the case where $p = 0$, $L : K$ is separable, and so $g(T/R) = 1$ agrees with the theorem. We will study function fields, and it turns out that we will always have $g(T/R) = 1$. So we will not deal with $g(T/R)$ anymore.

Let us consider function fields now: Let K be finitely generated of trascendence degree 1 over k. Then for every $z \in K^*$ one has

$\sum_R v_R(z)[R/\underline{m}_R : k] = 0$, where the sum is taken over the discrete valuation rings R of K over k, where $\underline{m}_R$ is the maximal ideal of R, and where v_R is the valuation $v_R : K^* \longrightarrow K^*/R^* \xrightarrow{\simeq} \mathcal{Z}$.

Let us "almost" prove this, using the inequality of the above theorem. We could prove it if we knew that we actually have an equality. In fact we do, as we will show later. Taking that for granted now, we can prove our assertion:

If z is algebraic over k, then it will be a unit in R (i.e. $z \in R^*$), and so $v_R(z) = 0$ for each R. So let us assume that z is not algebraic over k. Then K is a finite extension of $k(z)$, and each discrete valuation ring R of K over k extends the valuation ring $R_0 = k[z]_{(z)}$ of $k(z)$. We see that $v_R(z) > 0$ iff v_R restricts to the valuation of $k(z)$ corresponding to the prime element z of $k[z]$. So for the positive terms of the above sum we have

$\sum_{v_R(z)>0} v_R(z)[R/\underline{m}_R : k] = \sum_{R over R_0} e(R/R_0)f(R/R_0) = [K : k]$

(again, taking for granted equality in the above theorem, in the case of a function field).

Here the sum is taken over the distinct R's which satisfy $v_R(z) > 0$. We get the negative terms of the sum by considering the inverse of z and doing the same thing we just did. Thus we see that if we add up positive and negative terms, we get zero, and our assertion is proved.

Now we change direction, and review some infinite Galois Theory. We will continue with this in the next lecture, but let us now give an elementary definition:

Definition: Let $L : K$ be a field extension. We say that $L \supset K$ is **Galois** iff any (hence all) of the following equivalent conditions holds:

(a) $L = \bigcup_M M$, where each $M \supset K$ is finite Galois (i.e. separable and normal).

(b) $L \supset K$ is algebraic, separable, and normal.

(c) $K = L^{\mathcal{G}}$ for some compact subgroup $\mathcal{G}$ of $\mathrm{Aut}(L)$.

In condition (c), $L^{\mathcal{G}}$ is, of course, the fixed field of $\mathcal{G}$:
$L^{\mathcal{G}} = \{x \in L : \sigma x = x \ \forall\ \sigma \in \mathcal{G}\}$. We will talk about the topology of $\mathrm{Aut}(L)$ next time.

As an exercise, prove the equivalence of (a), (b) and (c).

Lecture 10 (September 20, 1995).
Scribe: Ezra Miller

Reference: Weil's *Basic Number Theory* gives a full account of infinite Galois theory.

Let L/K be a field extension. Then the following are equivalent:

1. L is a union of finite Galois extensions of K.
2. L/K is algebraic, separable, and normal.
3. $K = L^{\mathcal{G}}$ for some compact $\mathcal{G} \in \mathrm{Aut}\ L$, where $L^{\mathcal{G}}$ =fixed field of $\mathcal{G}$.
4. **Definition:** L/K is Galois.

Notice that topology enters into the picture here, specifically in the automorphism groups G in (3). We define a base for the open sets of Aut L as follows: If $E \subset L$ is a finite subset and $f : E \to L$ is (in the words of Prof. Lenstra) "any stupid map", then we define

$$U_{E,f} = \sigma \in \mathrm{Aut}\ L : \sigma|_E = f$$

to be an open set in Aut L. Aut L becomes a topological group (in fact Hausdorff) with composition and inversion continuous.

Let L/K be Galois. Then the group in (3) is uniquely determined, namely $G = \mathrm{Aut}_K\, L \overset{\text{def}}{=} \mathrm{Gal}(L/K)$. This group is to be thought of as a topological group. If $[L:K] < \infty$, then G is finite. In general, G is **profinite**, i.e. a projective limit of finite groups:

$$\mathrm{Gal}(L/K) \cong \varprojlim_{M \subseteq L} \mathrm{Gal}(M/K) = \left\{ \sigma = (\sigma_M)_M \;\middle|\; \sigma_M|_{M'} = \sigma_{M'} \text{ if } M' \subseteq M \right\}$$

(where the inverse limit is over $M \subseteq L$ such that M/K is finite Galois, so $\mathrm{Gal}(M/K)$ is finite for all M). Every element σ of $\mathrm{Gal}(L/K)$ acts on elements of these M, so $\sigma|_M = \sigma_M$, and if $M \subseteq M'$, then we must have $\sigma|_{M'} = \sigma_M|_{M'}$. The isomorphism above is as topological groups, the topology on the inverse limit being induced by $\varprojlim_M \mathrm{Gal}(M/K) \subseteq \prod_M \mathrm{Gal}(M/K)$. The product on the right is a product of finite (hence compact) spaces, so is itself compact (by Tychonoff's Theorem), and it is relatively easy to show that the projective limit is closed in the product (with the product topology).

Here are a couple of entertaining facts: Any bijective continuous map from a compact space to a Hausdorff space is a homeomorphism. (Proof: The continuous image of a compact set is compact, so the inverse map is continuous.) One can show that a topological group is profinite if and only if it is Hausdorff, compact, and totally disconnected.

Examples: 1. $\varprojlim_n \mathbf{Z}/p^n\mathbf{Z} = \mathbf{Z}_p = p$-adic integers.

2. $\varprojlim_n \mathbf{Z}/n\mathbf{Z} = \hat{\mathbf{Z}}$.

3. $\varprojlim_n \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) = \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$.

In fact, Examples 2 and 3 are isomorphic, in a canonical way. If we let $\mathbf{1} = (1)_n \in \hat{\mathbf{Z}}$, where the operation is addition, then $\mathbf{1}$ corresponds to the Frobenius element $\mathrm{Frob} = (\sigma_n)_n \in \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$, where the operation is composition and $\sigma_n \colon \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ via $x \mapsto x^q$. Note that $\mathrm{Frob}(x) = x \iff x^q = x \iff x \in \mathbf{F}_q$.

"Main Theorem of Infinite Galois Theory"

Let L/K be Galois with group G. Then the maps

$$\left\{ E \;\middle|\; K \subseteq E \subseteq L \right\} \longleftrightarrow \left\{ H \subseteq \mathcal{G} \;\middle|\; H \text{ is a closed subgroup} \right\}$$

(with the forwards map defined by $E \mapsto \mathrm{Gal}(L/E)$ and the reverse map defined by $H \mapsto L^E$) are inclusion-reversing inverse maps. If $E \leftrightarrow H$, then (E/K is Galois) $\iff$ (H is normal in $\mathcal{G}$), and in that case $\mathrm{Gal}(E/K) \cong \mathcal{G}/H$. [N.B. Check continuity of reduction with respect to the topologies involved.] Furthermore, (E is finite over K) $\iff$ (H is open in $\mathcal{G}$) $\iff$ (H is closed and $[\mathcal{G} : H] < \infty$). To prove the last equivalence, we note that (H is open) implies (i) each coset of H is open, so that H is the complement of the open set $\bigcup_{\sigma H \neq H} \sigma H$ and hence H is closed; (ii) the cosets of H constitute an open cover (which is actually a partition) of the compact set $\mathcal{G}$, so that there can be only a finite number of them (since any proper subset is not a cover). The reverse implication is proved the same way (using the fact that a finite union of closed sets is closed). Any statements above that have not been proven here can be taken as exercises, as can the following standard generalization of finite Galois theory: Suppose that the fields $E_1 \supseteq E_2$ correspond to $H_1 \subseteq H_2$; then $[E_1 : E_2] < \infty \iff [H_2 : H_1] < \infty$. We can try to generalize in other ways, e.g. try the statement: Suppose $K \subseteq E, F \subseteq L$ with E Galois over K; then $E/E \cap F$ and EF/F are Galois, with isomorphic Galois groups (isomorphism as topological groups).

It turns out that the main interest is in finite algebraic extensions. So why should we introduce infinite Galois theory just to do finite things? Because it may be necessary (or convenient) to choose a field before you start that is large enough to encompass all of the fields you are interested in, instead of enlarging your finite extension every time it becomes necessary. Therefore, we make the following definition:

Definition: $K^{sep} = K_s = \{\alpha \in \bar{K} \mid \alpha \text{ separable over } K\}$.

Note that this construction depends on first choosing an algebraic closure $\bar{K}$ for K. If a different algebraic closure were chosen, there would be no canonical isomorphism sending one separable closure to the other.

Definition: $\mathcal{G}_K = \mathrm{Gal}(K^{sep}/K)$ is called the **absolute Galois group** of K.

Remark: Sending $K_1^{sep} \to K_2^{sep}$ results in an inner automorphism of $\mathcal{G}_K$.

Topological Remark: If X is a topological space with decent conncectedness properties (i.e. locally path-connected, path connected, and semilocally simply-connected), then the category of coverings of X can be described by means of the fundamental group. We will go into this construction (as well as its relations to the description of Galois theory above) next time.

Lecture 11 (September 22, 1995).
Scribe: Ebrahim Jahangard Mahboob

Useful references for infinite Galois theory:
1. Artin, Algebraic Numbers and Algebraic Functions (Chapter 6, Section 1).
2. Cassels-Fröhlich, Algebraic Number Theory (Chapter 5).

We want to reformulate the main Galois theorem. Analogy with algebraic topology:

Let X be a connected topological space. Assume that every $x \in X$ has a pathwise connected, simply connected open neighborhood, U_x. A covering of X (at x_0) is a pair of a topological space Y and a continuous map $f : Y \to X$ such that there exists an isomorphism between $f^{-1}U_{x_0}$ and $U_{x_0} \times E$, where E is some discrete topological space, and so we have the following commutative diagram:

$$\begin{tikzcd} Y \arrow[d, "f"'] & \supset & f^{-1}U_{x_0} \arrow[d, "f"'] & \cong & U_{x_0} \times E \arrow[dll, "\pi"] \\ X & \ni x_0 \in & U_{x_0} & & \end{tikzcd}$$

Where π is the natural projection map.

Let $\mathcal{C}_1$ be the category whose objects are coverings of X and whose morphisms are defined as follows:
If $f_1 : Y_1 \to X$ and $f_2 : Y_2 \to X$ are two coverings of X, then morphisms between them are the continuous maps from Y_1 to Y_2 such that the following diagram is commutative:

$$\begin{tikzcd} Y_1 \arrow[rr, "g"] \arrow[dr, "f_1"'] & & Y_2 \arrow[dl, "f_2"] \\ & X & \end{tikzcd}$$

Now, for $x_0 \in X$, let $\pi_1(X, x_0)$ be the fundamental group of X (at base x_0). Each covering $f : Y \to X$ (at x_0) gives rise to a set, namely the fiber $f^{-1}x_0$, provided with an action of $\pi_1(X, x_0)$. (If a set equipped with a group action $\pi_1(X, x_0)$ is given, then one could uniquely determine the covering.)

Let $\mathcal{C}_2$ denote the category whose objects are sets provided with a $\pi_1(X, x_0)$-action and whose morphisms are set theoretic maps respecting the group action. I.e. if E_1 and E_2 are two sets with $\pi_1(X, x_0)$ acting on them and $f : E_1 \to E_2$ is a morphism (a set map) then $\forall \sigma \in \pi_1(X, x_0)$ & $\forall x \in E_1$ we have $f(\sigma x) = \sigma f(x)$.

Theorem: The above association gives an equivalence of categories, $F : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$.

So, we have

$$Hom(Y_1, Y_2) \xrightarrow{\overset{F}{\sim}} Hom(FY_1, FY_2)$$

for coverings (Y_1, f_1) and (Y_2, f_2) of X.

Note: The degree of a covering in $\mathcal{C}_1$ (i.e. number of originals of a point, x_0) corresponds to cardinality of the set with $\pi_1(X, x_0)$-action in $\mathcal{C}_2$. Also, connectedness of a covering corresponds to transitivity of the $\pi_1(X, x_0)$-action.

Reformulation of the main theorem of Galois theory:

Let K be a field and choose a separable closure, K^{sep} of K. (Choice of this field $K^{sep} \supset K$ corresponds to a choice of an embedding $\{x_0\} \longrightarrow X$.) Write $\mathcal{G}_K = Gal(K^{sep}/K)$. Then there are anti-equivalences of categories:

Theorem:

$$\left(\begin{array}{c}\text{finite separable field}\\ \text{extensions of } K \text{ with}\\ K\text{−morphisms}\end{array}\right) \underset{G}{\overset{F}{\rightleftarrows}} \left(\begin{array}{c}\text{finite sets provided with continuous}\\ \text{transitive } \mathcal{G}_K\text{−action with set theoretic}\\ \text{maps compatible with the } \mathcal{G}_K\text{−action}\end{array}\right)$$

The category on the right side is called "Algebraic fundamental group of K". Let's denote this category by $\mathcal{AFG}_K$ and the one on the right side by $\mathcal{FSF}_K$.

Note: Since Galois groups have in general more properties than the fundamental groups, our objects in $\mathcal{AFG}_K$ have more properties: finiteness of sets and continuity and transitivity of the actions.

What are the functors F and G?

$$F : E \longmapsto \{K\text{−maps } : E \to K^{sep}\}$$

And

$$\{\mathcal{G}_K\text{−maps } : S \to K^{sep}\} \longleftarrow\!\shortmid S : G.$$

Note: $\{\mathcal{G}_K\text{−maps } : S \to K^{sep}\}$ is a field.

One can check that

$$\mathrm{id}_{\mathcal{FSF}_K} \longrightarrow GF$$

is an isomorphism of functors. (If this were an equality then F would give an isomorphism of categories instead of equivalence of them!) I.e. $\forall E, E^{'} \in \mathrm{Ob}(\mathcal{FSF}_K)$ & $\forall \varphi \in \mathrm{Mor}(E, E^{'})$ the following diagram is commutative:

$$\begin{array}{ccccc} E & \xrightarrow{\sim} & GF(E) & = & \{\mathcal{G}_K\text{−maps } : \{K\text{−maps } : E \to K^{sep}\} \to K^{sep}\} \\ \varphi \big\downarrow & & \big\downarrow GF(\varphi) & & \\ E^{'} & \xrightarrow{\sim} & GF(E^{'}) & & \end{array}$$

Little exercise: assume the above theorem and try to get the main theorem for "traditional" finite Galois theory.

Definition: Let A be a ring (commutative with unity as usual) and B be an A-algebra such that $B \cong A^n$ as an A-module for some positive integer n. Then B is called finite etale if for a basis $\omega_1, \omega_2, ..., \omega_n$ of B over A we have

$$\det\big(\mathrm{Tr}(\omega_i\omega_j)\big)_{i,j} \in A^*.$$

I.e. the discriminant is a unit in A. (In general, we call something finite etale if it is locally like the above.)

If $A = K$ is a field, then a finite K-algebra is finite etale if and only if it is isomorphic as K-algebra to a finite product of finite separable field extension of K.

Now, if we cross out the words separable field extension of K and replace it by finite etale K-algebra in $\mathcal{FSF}_K$ then we can get rid of the transitivity condition in $\mathcal{AFG}_K$ in the above correspondence.

Note: if B is finite etale then $L \otimes_K B$ is also finite etale.

$$\begin{array}{ccc} L \otimes_K B & \supset & B \\ \uparrow & & \uparrow \\ L & \supset & K \end{array}$$

This is how Galois theory will look in the 21st century!

Lecture 12 (September 25, 1995).
Scribe: Wayne Whitney

Recall that last time we discussed a reformulation of the fundamental theorem of Galois Theory: Let K be a field, and let K^{sep} be a separable closure of K. Let $G_K = Gal(K^{sep}/K)$, G_K is called the absolute Galois group of K. A G_K-set is just a set with a continuous action of the group G_K on it. Then we have a contravariant equivalence of categories $(*)_K$:

$$\{\text{finite separable extensions } L \supset K\} \leftrightarrow \{\text{finite transitive } G_K\text{-sets}\}$$

given by:

$$L \mapsto \{K\text{-embeddings } L \subset K^{sep}\}$$

So now let $R \subset K$ be a discrete valuation ring and let $\hat{R} \subset \hat{K}$ be the completion of R. Choose a separable closure $\hat{K}^{sep}$ of $\hat{K}$; then the embedding $K \subset \hat{K}$ determines a subfield K^{sep} of $\hat{K}^{sep}$ which is a separable closure of K. We have the commutative diagram:

$$\hat{K}^{sep}$$

$$
\begin{array}{ccc}
 & | & \\
 & K^{sep}\hat{K} & \\
 / & & \backslash \\
K^{sep} & & \hat{K} \\
 \backslash & & / \\
 & K^{sep}\cap\hat{K} & \\
 & | & \\
 & K &
\end{array}
$$

Thus we get a restriction map from $G_{\hat{K}}$ to G_K. Eventually we will study extensions of $\hat{K}$ and shall see that $K^{sep}\hat{K} = \hat{K}^{sep}$, so the map $G_{\hat{K}} \to G_K$ is injective. Its image is a closed subgroup of G_K, since $G_{\hat{K}}$ is compact, which is called "the" decomposition group D of R in G_K. "The" because the decomposition group D is only defined up to conjugacy in G_K due to the choice of $\hat{K}^{sep}$.

Theorem Let $L \supset K$ be a finite separable field extension, which corresponds to a G_K set S under the equivalence $(*)_K$. Then the decomposition group D acts on S since $D \subset G_K$. There is a bijection:

$$\{\text{valuation rings } T \text{ of } L \text{ extending } R\} \leftrightarrow S/D, \text{ the } D\text{-orbit space of } S$$

and if $T \leftrightarrow S' \subset S$, then $e(T/R)f(T/R) = |S'|$ and $(*)_{\hat{K}}$ sends $\hat{L}_T$ to S'. Here $\hat{L}_T$ refers to the completion of L with respect to the valuation defined by T.

Remark

Assume $k = R/m_R$ is perfect. Then D has a closed normal subgroup I, the inertia group of R, such that $D/I \cong G_k$ and for a valuation ring T of L extending R, which corresponds as in the theorem to a G_K-set S', then:

1) $e(T/R) = 1$ (T is unramified over R) $\iff$ I acts trivially on S'.

2) S' is the union of $f(T/R)$ I-orbits of S, each of size $e(T/R)$.

3) $(*)_k$ sends T/m_T to S'/I a D/I-set.

Definition of I

The valuation ring $\hat{R}$ of $\hat{K}$ extends uniquely to a valuation ring U of $\hat{K}^{sep}$. Furthermore, U/m_U is a separable closure of k. The absolute Galois group $G_{\hat{K}}$ fixes U and m_U as sets. So $G_{\hat{K}}$ acts as field automorphisms on $k^{sep} = U/m_U$, fixing $k = R/m_R$. Thus we get a map $\phi : G_{\hat{K}} \to G_k$. That is, we have the following diagram:

$$\begin{array}{ccc} \hat{K}^{sep} \supset & U \to & k^{sep} \\ G_{\hat{K}} \mid & \mid & \mid G_k \\ \hat{K} \supset & \hat{R} \to & k \end{array}$$

One proves that the map ϕ is surjective, and then defines $I = \ker\phi$. If $\mathrm{char}k = 0$, $I \cong \hat{\mathbf{Z}}$; if k is finite, $G_k \cong \hat{\mathbf{Z}}$. These topics are the beginning of the study of local fields.

Back to Curves

So now we consider a field k and a field extension $K \supset k$ which is finitely generated of transcendence degree 1. Such a field extension we will call a "function field of a curve over k".

We then define the "abstract curve associated to $K \supset k$", denoted by C or C_K, as $C = \{\text{valuation rings of } K \supset k\}$. We think of the elements of C as points, denoted by P. If we are faced with the reality that P is a ring, then we usually denote it by O_P (or $O_{C,P}$ or $O_{K,P}$).

C contains the "generic point" $\xi = K$ with $O_\xi = K$, and all the other points of C are called "closed points". We know that for P closed, O_P is a discrete valuation ring with $[O_P/m_P : k] = \deg P < \infty$

Connection with Schemes (Informal)

We define a topology on C: let $X \subset C$ be closed $\iff$ X is finite with $\xi \notin X$, or $X = C$. Then if $U \subset C$ is open, let $O(U) = \cap_{P\in U} O_P$. $O(U) \subset K$, and O is a sheaf of rings on C, so (C, O) is a ringed space.

In fact (C, O) is a scheme. To be precise, (C, O) is an integral, 1-dimensional scheme over k which is proper and regular. Regular means the local rings O_P are regular local rings; proper is a property of schemes corresponding to the property of compactness in topology.

Furthermore, the category of such schemes over k is anti-equivalent to the category of functions fields of curves. This is the reason that we approach the study of curves by considering their functions fields, and thereby avoid most algebraic geometric detail.

Lecture 13 (September 27, 1995).
Scribe: Lawren Smitline

Let $K \supset k$ be a finitely generated extension of transcendence degree 1. We define $C = C_K = \{\text{valuation rings of } K \text{ over } k\} \ni p = \mathcal{O}_p$. Note that C is an integral one dimensional proper regular scheme over k. Proper means separated, of finite type, and universally closed.

If your C satisfies these properties, in fact, C is a curve. If you look at more general curves, there may be more than one with the same function field K. The conditions regular and universally closed correspond to nonsingular and projective.

To get curves without the universal closure property, include as new curves nonempty open subsets of C. To get curves without the regularity property, look at sets C' consisting of local rings between k and K with field of fractions K such that $C' \cap C_K$ is open, nonempty in C_K and such that any two rings in C' generate K as a ring.

To desingularize, replace all reduced fat local rings in C' by the valuation rings which dominate them.

The term regular means that all $\mathcal{O}_p$ are regular. The term nonsingular means all $\Omega_{\mathcal{O}_p/k}$ are free of rank 1 over $\mathcal{O}_p$. If k is perfect, regular implies nonsingular.

Example: Hyperelliptic curves.

Let $g \geq 0, g \in \mathbf{Z}$. Let $a, b \in k[X]$ such that $\deg a \leq g,\ \deg b = 2g+1$. Let the curve be $Y^2 + a(X)Y + b(X) = 0$. Consider the ring $k[X,Y]/(Y^2 + aY + b) = k[x,y]$.

We show $Y^2 + aY + b$ is irreducible over $k(X)$. If char $k \neq 2$, irreducibility is clear, since $k[X]$ is integrally closed. If there are roots, they have degrees summing to $2g+1$, so one root has degree at least $g+1$, so $\deg a \geq g+1$. $\Rightarrow\Leftarrow$

If $g = 1$, we have an elliptic curve. For $g > 1$, ∞ is a singular point.

So $K = Q(k[x,y])$ is a field.

The equation defines an affine curve Spec $k[x,y]$, which corresponds to the set $C' = \{k[x,y]_{\mathfrak{p}} : \mathfrak{p} \in \text{Spec } k[x,y]\}$. This affine curve is regular if and only if $k[x,y]$ is Dedekind, or $k[x,y]$ is the integral closure of $k[x]$ in K. If char $k \neq 2$, this holds iff $a^2 - 4b$ is square free in $k[x]$. It is nonsingular if $\Delta = a^2 - 4b \neq 0$.

If k is not perfect, then there is $a \in k$ such that a is not α^p for $\alpha \in k$ and char $k = p$. So $x^p - a$ is irreducible and square free; e.g. $y^2 = x^p - a$ has genus $\frac{p-1}{2}$.

If char $k = p$, C is nonsingular iff $\gcd(a, (a^2)'b - (b')^2) = 1$.

What are morphisms between these (actual) curves? Suppose L/k and $D = C_L$, where L is a finitely generated field extension of transcendence degree 1. Translating the scheme theoretic notion of a morphism $D \to C$ to fields, we find $\text{Hom}_{\text{schemes}}(D, C)$ is equivalent to $\text{Hom}_{\text{fields over } k}(K, L)$, where $K \subset L$. In fact, it is $\bigcup\{$pairs consisting of a closed point $P \in C$ plus a k-algebra embedding $k \subset k(P) \subset L\}$.

$C(k) = \{P \in C : k(P) = k\}$.

Next time: line bundles and adeles.

Lecture 14. (September 29, 1995).
Scribe: Dylan Thurston

Coming next: The Riemann-Roch Theorem!

But first, some notation from our sponsor.

Recall that for any base field k contained in a function field K, we have defined the curve C, whose points P are the valuation rings of K lying over k. As a matter of notation, the ring corresponding to a point P is denoted $\mathcal{O}_P$, with maximal ideal $\mathfrak{m}_P$. (So in some sense $\mathcal{O}_P = P$.) We are usually interested in the closed points, which correspond to discrete valuation rings (that is, all valuation rings besides the trivial one with $\mathcal{O}_P = K$ and $\mathfrak{m}_P = (0)$).

The divisor class field $\mathcal{O}_P/\mathfrak{m}_P$ will be denoted $K(P)$. The degree of $k(P)$ over k, $[k(P) : k]$, is called the degree of P, $\deg P$; it is a positive integer. $C(K)$ is the set of "rational points" of C; it is the set

$$C(K) = \{P | P \text{ a closed point}, \ \deg P = 1\}.$$

The valuation $K \Rightarrow \mathbf{Z} \cup \{\infty\}$ corresponding to P is denoted ord_P (or, occassionally, v_P). The completion of K with respect to P, which was formerly $\hat{K}$ (in an abuse of notation) will now be denoted K_P. Note that this is *not* a localization.

Suppose L/K is a finite extension. Then there is a natural map between the corresponding curves D and C, defined by $Q \in D \mapsto P \in C$ if $\mathcal{O}_Q \cap K = \mathcal{O}_P$. Note that each point in D maps to a unique point in C, but there may be several points mapping to a given point in C. Each inverse image of a point $P \in C$ corresponds to an extension of the valuation ring $\mathcal{O}_P$, so we can use the numbers defined earlier: $e(\mathcal{O}_Q/\mathcal{O}_P)$ and $f(\mathcal{O}_Q/\mathcal{O}_P)$, usually denoted $e(Q/P)$ and $f(Q/P)$. In particular,

$$f(Q/P) = [k(Q) : k(P)] = \frac{\deg Q}{\deg P}.$$

By an earlier result (reference!), $\bigcap_{P \in C} \mathcal{O}_P = \bar{k} \cap K$ is a finite algebraic extension of k, which we can assume to be equal to k (redefining k if necessary). In other language, this says that the only functions on the curve with no poles are the constants, the elements of k.

A *divisor* D of C is a formal finite sum

$$D = \sum_{\substack{P \in C \\ P \text{ closed}}} n(P) \cdot P.$$

Saying the sum is finite means that $n(P) = 0$ for all but finitely many points P. The divisors form a partially order abelian group Div (or Div_K if the field is not clear from context), ordered by the relation

$$\sum n(P) \cdot P \geq \sum m(P) \cdot P \quad \text{iff} \quad \forall P : n(P) \geq m(P).$$

A divisor D is *effective* if $D \geq 0 \equiv \sum 0\dot{P}$, and is *prime* if there is a point P so that $D = P$.

The degree, defined above for points, has a natural extension to divisors:

$$\deg(\sum n(P) \cdot P) = \sum n(P) \deg P.$$

The image of the degree map is a subgroup of $\mathbf{Z}$, of finite index since it contains $\deg P \neq 0$ for any point p. It is an interesting question when this map is surjective. For instance, it is a non-trivial fact (to be proved later [ref]) that when k is a finite field, *deg* is surjective. On the other hand, it is easy to see that when k is algebraically closed, deg is surjective, as $\deg P = 1$ for any point p.

There is a natural group homomorphism

$$\begin{aligned} K^* &\to \mathrm{Div}_K \\ f &\mapsto (f) \equiv \sum_P \mathrm{ord}_P(f) P \end{aligned}$$

(This is a finite sum by earlier results (ref!).) The image of this map is called the set of *principal divisors*. By our assumption above, the kernel is k^*. The cokernel is new; it is called the *Picard group* Pic_K of C (or the *divisor class group* of C); it is an infinite group. Later we will see an alternative definition of the Picard group as the group of equivalence classes of line bundles, with sum corresponding to the tensor product.

To see that Pic_K is infinite, consider the sequence of maps

$$K^* \to \mathrm{Div}_K \stackrel{\deg}{\to} \mathbf{Z}$$

The composition is 0. (This has already been stated, but not yet completely proved; it depends on the fact that $\sum ef = n$ for the relevent finite extensions of degree n.) Hence the degree map descends to a map $\mathrm{Pic}_K \to \mathbf{Z}$ (in other language, the degree of a line bundle is well-defined) and Pic_K is infinite, as any divisor class with non-zero valuation will have infinite order.

For $D \in \mathrm{Div}_K$, define a vector space

$$\begin{aligned} L(D) &= \{0\} \cup \{f \in K^* : (f) \geq -D \\ &= \{0\} \cup \{f \in K^* : \forall P : \mathrm{ord}_P\, f \geq -n(P)\}. \end{aligned}$$

Why is there a minus sign? This definition is primarily of interest when D is effective. But it is immediate that $L(0) = k$ and hence $L(-D) = \{0\}$ for any $D > 0$. Without the minus sign in the definition, we would have $L(D) = 0$ instead. Another reason for the minus sign is the connection with line bundles. We'll associate a bundle to each D, and $L(D)$ will be identified with the space of sections of D.

$L(D) \subset K$ is a k vector space, so we can use its dimension

$$l(D) \overset{\text{def}}{\cong} \dim_K L(D).$$

We immediately have that $l(0) = 1$. It's not obvious yet, but $l(D)$ turns out to be finite.

Adèles.

The Adéle ring $\mathbf{A}_K$ of K is, by definition,

$$\mathbf{A}_K = \prod_{\substack{P \in C \\ \text{closed}}}' K_P$$

The notation $\prod'$ means the *restricted* direct product. It needs additional information to be well-defined; in this case it means

$$\mathbf{A}_K = \{\, (x_P) \in \prod K_P : x_P \in \hat{\mathcal{O}}_P \text{ for almost all } P\}.$$

(As usual, 'almost all' means 'all but finitely many.')

$\mathbf{A}_K$ has a natural topology. We have

$$\prod_P \hat{\mathcal{O}}_P \subset \mathbf{A}_K.$$

Give $\prod \hat{\mathcal{O}}_P$ the product topology. Then, in $\mathbf{A}_K$, define it and its translates to be open. (Note that this is different from the topology induced from $\prod K_P$.) There is a natural inclusion $K \subseteq \mathbf{A}_K$ (K is in $\prod K_P$ and lands in the restricted product). What is the induced topology on K? For an arbitrary $P_0 \in C$, consider the open set

$$\hat{\mathfrak{m}}_{P_0} \times \prod_{P \neq P_0} \mathcal{O}_P.$$

The intersection of this set with K is just $L(-P_0) = \{\, 0\,\}$, so the induced topology on K is the discrete topology.

Any divisor D gives a fractional ideal

$$\mathfrak{d} = \prod_{P \text{closed}} (\hat{\mathfrak{m}}_P)^{n(P)} \subseteq \mathbf{A}_K.$$

By definition,

$$L(D) = K \cap \mathfrak{d}^{-1}.$$

(To get $\mathfrak{d}^{-1}$, put a $-$ in front of $n(P)$ in the definition of $\mathfrak{d}$.) A subset $\mathfrak{h}$ of $\mathbf{A}_K$ is a *fractional ideal* if there is a $c \in \mathbf{A}_K$ so that $c\mathfrak{h}$ is an open ideal of $\prod \hat{\mathcal{O}}_P$.
Exercise: each fractional ideal comes from a unique divisor in this way.

If D is effective, then $\mathfrak{d}$ is a true ideal. If D is prime, then $\mathfrak{d} = \hat{\mathfrak{m}}_{P_0} \times \prod_{P \neq P_0} \hat{\mathcal{O}}_P$, which is a prime ideal. If $D \geq D'$, then $\mathfrak{d} \leq \mathfrak{d}'$ and $\dim_K \mathfrak{d}'/\mathfrak{d} = \deg D - \deg D'$ by a local computation.

Finally we are in a position to state
Riemann's Theorem. For every divisor D, the numbers $l(D)$ and $c(D) = \dim_k \mathbf{A}_K/(K + \mathfrak{d}^{-1})$ are finite (and ≥ 0), and if we write $g = c(0)$ (the *genus* of K over k), then

$$\deg D - l(D) + c(D) = g - 1.$$

(Assuming still that $\bar{k} \cap K = k$; if not, replace 1 in the equation above by $[\bar{k} \cap K : k]$.

The Roch half of the theorem involves "identifying l(D) with c(D)." You can see a formal analogy already: in the definition of $l(D)$, replace intersection with sum and dimension with codimension to get the definition of $c(D)$.

Lecture 15 (October 2, 1995).
Scribe: Nghi Nguyen

We recall the notations: $k \subset K$ is a finitely generated field extension of transcendence degree 1. We assume $K \cap \bar{k} = k$. $\mathbf{A}_K = \prod'_{P \text{ (closed point) } \in C_K} K_P$ (restricted product).

$\mathbf{A}_K \supset \prod_P \hat{m}_P^{n(P)} = \underline{d} \longleftrightarrow D = \sum_P n(P)P \quad (n(P) \in \mathbf{Z} \ = 0$ for almost all P)
$L(D) = \{0\} \cup \{f \in K^*\colon (f) \geq -D\} = K \cap \underline{d}^{-1}$ where $\underline{d}^{-1} = \prod_P \hat{m}_P^{n(P)}$
$l(D) = \dim_k L(D) \qquad c(D) = dim_k \mathbf{A}_K/(K + \underline{d}^{-1})$
Remark: If $D = 0$, then $c(0) = \dim_k coker(K \longrightarrow \mathbf{A}_K/\hat{\mathcal{O}} = \bigoplus_P K_P/\hat{\mathcal{O}}_P)$
Also, $K_P/\hat{\mathcal{O}}_P \cong K/\mathcal{O}_P$

Riemann's Theorem: For all divisors D, the numbers $l(D)$ and $c(D)$ are finite, and if we put $c(D) = g$ (the *genus* of K over k) then for all D one has

$$degD - l(D) + c(D) = g - 1$$

.

Proof: There is an exact sequence (for every two divisors $D \geq E$):

$$0 \longrightarrow L(D)/L(E) \longrightarrow \underline{d}^{-1}/\underline{e}^{-1} \longrightarrow (K + \underline{d}^{-1})/(K + \underline{e}^{-1}) \longrightarrow 0$$

We know from last time: $\dim_k \underline{d}^{-1}/\underline{e}^{-1} = degD - degE$. Consequently, if $D \geq 0$ then, by letting $E = 0$ on the left arrow, we have $l(D) - l(0) \leq degD - deg(0)$. Since

$l(0) = 1$ and $deg(0) = 0$, it follows that $l(D) \leq 1 + degD < \infty$. For any D not neccessarily$>$ 0 one can choose D' with $D' \geq 0$, $D' \geq D$. Then $L(D) \subset L(D')$ and $l(D) < l(D') < \infty$.

Now take an arbitrary $z \in K \backslash k$. We write $(z) = N - D$, where N and D are effective and coprime. Note that $k(z)$ is a purely transcendental field extension. If we denote ∞ for the infinity point of the curve $\mathbf{P}^1$ having this function field, then $D = \sum_{Q \mapsto \infty} e(Q/\infty).Q$. We shall study $l(nD)$ when $n \to \infty$.

<u>Upper bound</u> : (for large n) $l(nD) \leq 1 + n.degD = 1 + \ n\ .\ \sum_{Q|\infty} e(Q/\infty) f(Q/\infty)$

<u>Lower bound</u> : Choose a basis $\{u_i\}$ of K over $k(z)$. Multiplying each u_i by a suitable $f_i \in k[z] \backslash \{0\}$ we can achieve $ord_P u_i \geq 0$ for all P not dividing D. Hence $(u_i) \geq -(a_i + 1)D$ for some integers a_i's. Now $L(nD) \ni z^j \cdot u_i$, $0 \leq j \leq n - a_i - 1$. All u_i are $k(z)$-linearly independent, so all $z^i u_i$ are k-linearly independent. Therefore,

$l(nD) \geq \sum_i (n - a_i) = -\sum_i a_i + n[K{:}k(z)]$

Letting $n \mapsto \infty$ lower and upper bounds imply:

$\sum e(Q/\infty) f(Q/\infty) \geq [K{:}k(z)]$

We also know from previous lectures that $\leq$ is true. So we have equality, and the following important equation:

$$degD = [K{:}k(z)]$$

It follows that $deg((z)) = 0$.

Next, for two divisors D and D', $D = (f) + D' \iff \underline{d} = f \cdot \underline{d'} \iff f \cdot \underline{d}^{-1} = \underline{d'}^{-1} \Longrightarrow f \cdot L(D) = L(D') \Longrightarrow l(D) = l(D')$. Likewise: $D = (f) + D' \Longrightarrow c(D) = c(D')$ (we say $l(D)$ and $c(D)$ are defined up to linear equivalence.)

For the divisor D above we have: $l(nD) \geq deg(nD) - \sum a_i$.

<u>*Claim*</u>: $\quad l(E) \geq degE - \sum a_i$ for every divisor E.

Proof: The statement is true if $E = nD$ for some $n \geq 0$. It is also true if $E \leq nD$ (same n) because: From the exact sequence above we had $l(D) - l(E) \leq degD - degE$ if $D \geq E$. So $l(E) - degE \geq l(D) - degD$. For general E: find $f \in k[z] \backslash \{0\}$ such that $E - (f) = E'$ has coefficients ≤ 0 for all P not dividing D. Then the statement is true for E' (since $\exists n$ such that $nD \geq E'$) and hence for E because E is linearly equivalent to E'.

Lecture 16 (October, 4, 1995).
Scribe: Saul Schleimer

Today we finish the proof of Riemann's theorem.

Theorem: Let k be any field, and let K be a function field over k. (i.e. k has transcendence degree 1 over k and $\bar{k} \cap K = k$.) Let D be a divisor. Let $c(D) = dim_k(\mathbf{A}_k/(K + \underline{d}^{-1}))$, $l(D) = dim_k L(D)$. Then $c(D) \leq \infty$ and $degD - l(D) + c(D) = g - 1$ where $g = c(0)$.

Proof: (cont) Let $D \geq E$. Last time we used the short exact sequence

$$0 \to L(D)/L(E) \to d^{-1}/e^{-1} \to (K + d^{-1})/(K + e^{-1}) \to 0$$

to show that $l(D) - l(E) \leq deg(D) - deg(E)$; and, if $z \in K - k$ then we have the equality

$$\sum e(Q/\infty)f(Q/\infty) = [K : k(z)]$$

where the sum runs over all $Q \in C_K$ such that $Q \mapsto \infty$ under z. Also, $\forall z \in K^*$ the $deg((z)) = 0$. And finally, we showed that $\forall E$, $l(E) \geq deg(E) - \sum a_1$ $(a_i \geq -1)$.

It is now easy to show that $c(D) \leq \infty$ by varying D. $\forall D \geq E$ we have the string of inequalities:

$$\begin{aligned} dim_k(K + d^{-1})/(K + e^{-1}) &= dim(d^{-1}) - dim(e^{-1}) \\ &\leq deg(D) - deg(E) - l(D) + l(E) \\ &\leq \sum a_i - deg(E) + l(E) \end{aligned}$$

Now, $\sum a_i - deg(E) + l(E)$ is finite, and so every k-vector space $(K + d^{-1})/(K + e^{-1})$ is finite dimensional. Thus $(\bigcup(K + d^{-1}))/(K + e^{-1})$ is as well. Note however, $\bigcup(d^{-1}) = \mathbf{A}_k$ and thus $(\bigcup(K + d^{-1}))/(K + e^{-1}) = \mathbf{A}_k/(K + e^{-1})$.

$\Longrightarrow c(E)$ is finite.

Then we have the equality,

$$deg(D) - deg(E) = l(D) - l(E) + c(E) - c(D).$$

So for any $D \geq E$, $deg - l + c$ is the same for D and E, i.e. constant. Thus $deg - l + c$ is constant for all D. Letting $D = 0$ we find that $deg(0) - l(0) + c(0) = 0 - 1 + c(0) = g - 1$ and this completes the proof.

(Notice that we did not really use the assumption $\bar{k} \cap K = k$. Indeed, if we assume that $[\bar{k} \cap K : k] < \infty$ then the theorem becomes simply $degD - l(D) + c(D) = g - [\bar{k} \cap K : k]$)

Another statement of the theorem is: For every $D \geq E$ one has $\exists D$ such that $K + d^{-1} = \mathbf{A}_K$ and this is equivalent to saying $c(D) = 0$.

Example: We will find g for the function field $K = k(z)$. Let $u_i = 1$. (Recall that the u_i's were to be a basis for K over $k(z)$, where z was any sufficiently interesting element of $K - k$.) Note that u_i has no poles. We have $a_i \in \mathbf{Z}$ such that the divisor $(u_i) \geq -(a_i + 1)D$, where D is the denominator of z. The smallest possible choice for a_i is -1, and so we find that $0 \leq g \leq 0$, i.e. $g = 0$.

Note that it is also possible to compute g using $c(0) = g$. Let L be a finite extension of K. Then for any closed point $P \in C_K$ there are points $Q_i \in C_L$ lying over p.

Claim: $\sum_{Q_i} e(Q_i/P)f(Q_i/P) = [L : K]$

Proof: Pick $z \in K$, $ord_P(z) < 0$ i.e. z has a pole at P. By our proof of Riemann's Theorem we know that

$$\sum_{Q \mapsto \infty \in C_{k(z)}} e(Q/\infty)f(Q/\infty) = [L : k(z)]$$

for $Q \in C_L$. (Actually, this equality does not directly follow when $L \cap \bar{k} \neq k$. This case is left as an exercise.) Now, since $\sum = (\sum_{P' \mapsto \infty} ef(P'/\infty))(\sum_{Q \mapsto P'} ef(Q/P'))$ and the first sum on the right hand side is equal to $[K : k(z)]$, the desired equality holds.

Remark: From algebraic geometry we have another way to define g, the genus of a curve. We set $g = dim_k(H^1(C, O_C))$. To show that this is equivalent to our previous definition of g consider the short exact sequence,

$$0 \to \mathcal{O}_C \to \mathcal{K} \to \mathcal{K}/\mathcal{O}_{\mathcal{C}} \to \prime$$

where $\mathcal{K}$ is the constant sheaf K on C. Taking global sections, we have that $H^1(C, \mathcal{O}_C) = coker(K \mapsto H^0(\mathcal{K}/\mathcal{O}_{\mathcal{C}}))$. But $H^0\mathcal{K}/\mathcal{O}_{\mathcal{C}} = \sum \mathcal{K}/\mathcal{O}_{\mathcal{P}} = \mathbf{A}_{\mathcal{K}}/\hat{\mathcal{O}}$. Thus $g = dim_k(\mathbf{A}_K/K + \hat{\mathcal{O}}) = c(0)$.

Scribe's note - At this point a homework problem (5B) was discussed at some length. As I was not enrolled - i.e. not doing the homework - I can't do justice to the this part of the lecture. Please contact Professor Lenstra for a copy of the relevant homework set or Howard Thompson for solutions.

Lecture 17 (October, 6, 1995).
Scribe: Saul Schleimer

Today we will begin to derive the Riemann-Roch Theorem from Riemann's Theorem proved in lecture 16. As usual let k be a field (assumed algebraically closed as necessary) with K a function field over k.

Recall the statement of Riemann's Theorem - If D is a divisor, then letting $c(D) = dim_k(\mathbf{A}_k/(K + d^{-1}))$, $L(D) = K \cap (d^{-1})$, and $l(D) = dim_k L(D)$ we have that $c(D) \leq \infty$ and $degD - l(D) + c(D) = g - 1$ where $g = c(0)$.

We will need the following useful facts:

• If $degD < 0$ then $l(D) = 0$. (To see this: suppose that $f \in L(D)$ and $f \neq 0$. Then $(f) \geq -D$. Taking degrees we have that $0 \geq -deg(D)$, i.e. $deg(D) \geq 0$.)

• If $deg(D) \geq 0$ then $l(D) \leq deg(D) + 1$. (We have already dealt with the case $D \geq 0$ (see lecture 15.) In general, if $l(D) \geq 0$ then $\exists f \in L(D)$ such that $f \neq 0$. Now replace D by the equivalent divisor $D + (f) \geq 0$ and we are done.)

- $c(D) \geq 0$

Definition: A *Weil differential* is a continuous, k-linear function $\lambda : \mathbf{A}_K \to k$ that vanishes on K (k is given the discrete topology here.) Note that the kernal of λ is open and thus contains some d $(= \prod_P \hat{m}_P^{n(P)})$ since these d's are basic open sets.

Notation: $Diff = Diff_K = \{$ all Weil differentials $\}$. This is a K-vector space with scaler multiplication given by $c\lambda(x) = \lambda(cx)$ and vector addition given by the standard point-wise addition of functions.

The rest of this lecture will be devoted to showing that $dim_K Diff = 1$:

We note that $c(D) = dim_k(\mathbf{A}_K/(K + d^{-1})) = dim_k\{f : \mathbf{A}_K \to k \mid f$ is k-linear, $f\mid_K = 0$, and $d^{-1} \subset ker(f).\} = dim_k Diff_D$ where $Diff_D$ is defined to be the set $\{\lambda \in Diff \mid d^{-1} \subset ker(\lambda)\}$. Of course $Diff_D$ is a sub k-vector space of $Diff$.

Now, if $deg(D) < g-1$ then Riemann's Theorem implies that $c(D) > 0$. Thus $Diff \neq 0$ (i.e. $dim_K Diff \geq 1$.) Let D,E be divisors. We

Claim: $L(D-E) \cdot Diff_D \subset Diff_E$. To prove this let $f \in L(D-E)$ and $\lambda \in Diff_D$. Then $\lambda\mid_d^{-1}$ is zero and $f \in e \cdot d^{-1}$. Fix $x \in e^{-1}$. Then $f\lambda(x) = \lambda(fx) = 0$ since $f \cdot x \in d^{-1}$. Since we may chose $f \neq 0$ we are done.

Claim: If $deg(D) > 2g-2$ then $c(D) = 0$.

Let E be any divisor with $l(E) = 0$. Suppose that $c(D) > 0$ Then $c(D) = dim Diff_D > 0$ implies that

$$dim_k Diff_E = c(E) = g - 1 - deg(E) + l(E) = g - 1 - deg(E)$$

while

$$dim_k Diff_E \geq dim_k L(D-E) = l(D-E) =$$

$$= deg(D) - deg(E) + c(D-E) \geq deg(D) - deg(E) - g + 1$$

Moving things around a bit we see that $deg(D) \leq 2(g-1)$.

This shows that there exist an upper bound on the possible degrees of divisor D for which d^{-1} sits inside the kernal of a nonzero Weil differential λ. This will allow us to associate a "special" divisor to a differential.

Let λ be any Weil differential not equal to zero. Then there exists a divisor D such that $d^{-1} \in ker(\lambda)$. We examine the set of all such D. (For example, if $E < D$ then E lies in this set. Also, if D_1 and D_2 are two such divisors then $sup(D_1, D_2) = \sum \max(n_1(P), n_2(P)) \cdot P$ is in the set as well, where $D_i = \sum n_i(P) \cdot P$ and the sum ranges over $P \in C_K$.) Hence, if D is such a divisor of largest possible degree (it exists due to the upper bound) then $D \geq$ any other such divisor.

Conclusion: $\forall \lambda \in Diff_K - \{0\}$ there is a unique largest divisor D with $d^{-1} \subset ker(\lambda)$.

Notation: This D is denoted by K_λ or W_λ, and is called the *canonical divisor*.) (Here Professor Lenstra points out that both of these terrible notations are used in the literature and neither of them are his fault.)

Claim: $W_{f\lambda} = (f) + W_\lambda$ ($f \in K^*, \lambda \in Diff_K - \{0\}$).

Using the fact that $L(f) \cdot Diff_{W_\lambda} \subset Diff_{W_\lambda + (f)}$ (which follows from the first claim above with $D = W_\lambda$ and $E = W_\lambda + (f)$) we see that $f \cdot \lambda \in Diff_{W_\lambda + (f)}$ (since $f \in L(f)$ and $\lambda \in Diff_{W_\lambda}$.) It follows that $(W_\lambda + (f))^{-1} \subset ker(f\lambda)$ and thus $(f) + W_\lambda \leq W_{f\lambda}$ by the definition of $W_{f\lambda}$. The $\geq$ case follows by symmetry.

Now suppose that λ, μ are linearly independent in $Diff_K$. We look for a contradiction: As above we have

$$L(W_\lambda - E) \cdot \lambda \subset Diff_E$$

Thus,

$$L(W_\lambda - E) \cdot \lambda + L(W_\mu - E) \cdot \mu \subset Diff_E$$

Since λ and μ are independent we have the inequality of dimensions

$$l(W_\lambda - E) + l((W_\mu - E) \leq c(E)$$

Now let $deg(E) \to -\infty$. Using Riemann's Theorem and the fact that $deg(D) > 2g - 2$ implies $c(D) = 0$ we have that

$$deg(W_\lambda - E) - l(W_\lambda - E) = g - 1$$

i.e. $deg(-E) = l(W_\lambda - E)$ plus some constant. Similarly $deg(-E) = l(W_\mu - E)$ plus some constant. But Riemann's Theorem applied to the divisor E alone implies that $c(E) = -deg(E) +$ constant. We are forced to conclude that

$$2 \cdot deg(-E) \leq -deg(E) + (\text{constant})$$

as $deg(E)$ goes to negative infinity. This is a contradiction.

$\Longrightarrow \lambda$ and μ are dependent.

$\Longrightarrow dim_K Diff_K = 1$.

Lecture 18 (October 9, 1995).
Scribe: Nghi Nguyen

We recall the notations: $k \subset K$ is a function field, D is an arbitrary divisor on the curve C_K, $\underline{d} = \prod \hat{m}_p^{n(P)}$, $l(D) = \dim_k L(D)$, $L(D) = K \cap \underline{d}^{-1}$ inside $\mathbf{A}_K$, $c(D) = \dim_k \mathbf{A}_k/(K + \underline{d}^{-1})$,

$$Diff_K = \{\text{Weil differentials}\}$$
$$= \{k - \text{linear maps } \lambda : \mathbf{A}_K \longrightarrow k \text{ which are zero on K and on some } \underline{d}^{-1}\}$$
$$= \bigcup_D (Diff_D) \text{ where } Diff_D = \{\lambda \in \ Diff_K \text{ with } \underline{d}^{-1} \subset ker\lambda\}$$

, so $c(D) = \dim_k Diff_D$. For each $0 \neq \lambda \in Diff_K$ there is a unique largest D with $\lambda \in Diff_K$; this D is denoted by K_D or W_λ ("canonical divisor"). Last time we proved: $\dim_K Diff_K = 1$. Also, $W_{f\lambda} = (f) + W_\lambda$ for $f \in K^*$. So the divisor class of K_λ is independent of λ.

Now pick $\lambda \in Diff_K, \neq 0$. Then $Diff_K = K.\lambda$. If $f \in K^*$, then $f\lambda \in Diff_D \iff W_{f\lambda} \geq D \iff (f) + W_\lambda \geq D \iff f \in L(W_\lambda - D)$. This argument gives

Riemann-Roch Theorem:

$$l(D) - l(W_\lambda - D) = degD + 1 - g$$

Remarks:
$l(D) = 0$ if $degD < 0$,
$l(W_\lambda) = g$,
$deg(W_\lambda) = 2g - 2$,
and $l(D) = degD + 1 - g$ if $degD > 2g - 2$.

Lecture 19 (October 11, 1995).
Scribe: David M. Jones

Recall: $\ell(D) - \ell(W_\lambda - D) = \deg D + 1 - g$
$\ell(D) = 0$ if $\deg D < 0$.
$\ell(D) = \deg D + 1 - g$ if $\deg D > 2g - 2$.
$K = k(t)$ has $g = 0$.

Recall from the proof of the Riemann-Roch Theorem:
$k(t) \overset{m}{\subset} K$, $(t) = N - D$ where N, D are effective, coprime divisors.
If $K = \bigoplus_{i=1}^m k(t) \cdot u_i$ and $(u_i) \geq -(a_i + 1) \cdot D$, then $g \leq 1 + \sum_{i=1}^m a_i$.
In the case $K = k(t)$, $m = 1, u_1 = 1, a_1 = -1$ so $g \leq 0 \Rightarrow g = 0$.

Another proof that $g = 0$ for $K = k(t)$: $g = \dim_k \mathbf{A}_K/(K + \hat{\mathcal{O}})$. But $\hat{\mathcal{O}} = \prod_P \hat{\mathcal{O}}_P$ and $K + \hat{\mathcal{O}} = \mathbf{A}_K$ so $g = \dim_k\{0\} = 0$.

Since $g = 0$, we have: $\ell(D) = 0$ if $\deg D < 0$ and
$$\ell(D) = \deg D + 1 \text{ if } \deg D > -2.$$

We have $K \xrightarrow{\varphi} \mathbf{A}_K/(\prod_P \underline{\hat{m}}_P^{n(P)})$, where $\begin{cases} n(P) = 0 & \forall P \neq \infty \\ n(\infty) = 0, 1, 2 \end{cases}$

∞ is the point in $\hat{\mathcal{O}}$ for which $\mathcal{O}_\infty = k[t^{-1}]_{(t^{-1})} = \{\frac{f}{g} \in K : f, g \in k[t], g \neq 0, \deg g \geq \deg f\}$. As $n(\infty) = 0, 1, 2$, we get $\dim(\mathrm{coker}(\varphi)) = 0, 0, 1$.

Question: How does this relate to Riemann-Roch?

Answer: $c(D) = \ell(W_\lambda - D) = \dim_k \mathbf{A}_K/(K + \underline{d}^{-1})$. Take $D = 0, -\infty, -2 \cdot \infty$.

Now we would like to find a basis for $K = k(t)$ over k:

"partial fraction expansion":

$$\begin{cases} t^i & \text{s.t. } i \in \mathbf{Z}_{\geq 0} \\ \frac{t^i}{f^n}, & f \in k[t] \text{ monic, irred.; } n \in \mathbf{Z}_{>0}, 0 \leq i \leq \deg f, i \in \mathbf{Z} \end{cases}$$

For now, assume that $k = \bar{k}$: $\begin{cases} t^i & i \in \mathbf{Z}_{\geq 0} \\ \frac{1}{(t-\alpha)^n} & \alpha \in k, n \in \mathbf{Z}_{>0} \end{cases}$

$K \xrightarrow{\varphi} \mathbf{A}_K/\prod_P \underline{\hat{m}}_P^{n(P)} = \bigoplus_P (K_P/\underline{\hat{m}}_P^{n(P)})$.

Now, $\mathbf{A}_K/\prod_P \underline{\hat{m}}_P^{n(P)} = \hat{\mathcal{O}}$ if all $n(P) = 0$.

$\{$ closed points $P\} \leftrightarrow k \cup \{\infty\}$ via $k[t]_{(t-\alpha)} \leftrightarrow \alpha$

1. If $K_P = k((t - \alpha))$ and $\hat{\mathcal{O}}_P = k[[t - \alpha]]$, then a basis for $K_P/\hat{\mathcal{O}}_P$ over k is: $\frac{1}{(t-\alpha)^n}, n \in \mathbf{Z}_{>0}$.

2. If $P = \infty$, then $K_\infty = k((t^{-1})) \supset \hat{\mathcal{O}}_\infty = k[[t^{-1}]]$. Then a basis for $K_\infty/\hat{\mathcal{O}}_\infty$ over k is: $t^i, i \in \mathbf{Z}_{>0}$. A basis for $K_\infty/\underline{\hat{m}}_\infty^n$ over k is: $t^i, i \in \mathbf{Z}_{\geq 1-n}$ (esp. $n = 1, 2$).

Suppose $n(\infty) = 0$. Then φ is onto with kernel $= k$. (Every basis element of $k(t)/k$ is sent to itself in $\bigoplus_P K_P/\underline{\hat{m}}_P^{n(P)}$ except 1 which is sent to 0.)

Suppose $n(\infty) = 1$. Then φ is bijective, $\mathbf{A}_K = K \oplus (\underline{\hat{m}}_\infty \oplus \prod_{P \neq \infty} \hat{\mathcal{O}}_P)$ so $D = -\infty$ has $\ell(D) = 0, c(D) = 0 = \ell(W_\lambda - D)$.

Suppose $n(\infty) = 2$. Then φ is injective and has cokernel of dimension 1. $D = -2 \cdot \infty$ has $\ell(D) = 0, c(D) = 1 = \ell(W_\lambda - D)$. Also, $c(D) = 1 = \dim_k \mathrm{Diff}_D$. $\mathrm{Diff}_D =$ the set of k-linear functions $\mathbf{A}_K/(\underline{\hat{m}}_\infty^2 \oplus \bigoplus_{P \neq \infty} \hat{\mathcal{O}}_P) \to k$ that are 0 on the image of K.

(An example of such a function $\lambda \neq 0$ is given as follows: Take $x \in \mathbf{A}_K$ and write $x = y + z$ where $y \in K$ and $z \in (\underline{\hat{m}}_\infty \oplus \prod_{P \neq \infty} \hat{\mathcal{O}}_P)$, where $z_\infty =$ (component of z at ∞) $\equiv c \cdot t^{-1} \bmod \underline{\hat{m}}_\infty^2$ and $c \in k^*$.)

That's it for the case $k = \bar{k}$. As an exercise, work out this basis in the non-algebraically closed case.

Above, λ is 0 on $\underline{d}^{-1}$ where $\underline{d} \leftrightarrow D = -2 \cdot \infty$. Actually, D is the largest D' for which $\lambda \in \mathrm{Diff}_{D'}$. So $W_\lambda = -2 \cdot \infty$.

$\underline{d}^{-1} = \{z \in \mathbf{A}_K : \lambda(\hat{\mathcal{O}} \cdot z) = 0\}$.

Remark: One could carry out these calculations replacing $\mathbf{A}_K$ with the "non-complete" analogue $\prod'_P K$, restricted with respect to $\prod_P \hat{\mathcal{O}}_P$. However, adele rings have very nice "structural" properties. For example, if L/K is complete then $\mathbf{A}_K \otimes_K L \to \mathbf{A}_L$ is an isomorphism. This is not true if you are not using complete fields.

FACT: If $g = 0$, then $K \cong_k k(t) \Leftrightarrow \exists$ closed $P : \deg P = 1$.

Proof: $\Rightarrow P = \infty$ has degree 1.

$\Leftarrow \deg P = 1$. Then $\ell(P) = 2$. So $L(P) \supset k$ but $L(P) \neq k$ so $\exists x \in L(P)$ with $x \notin k$. Then the pole divisor of x is P. Then $[K : k(x)] = \deg$ (pole divisor of x) $= 1$.

Lecture 20. (October 13, 1995).

Scribe: Dylan Thurston

Plan for the remainder of the course:

- fields of low genus (to see Riemann-Roch at work)
- line bundles / linear systems / maps to projective space (in particular, embeddings of a curve in $\mathbf{R}^n$). (In some sense, the coming computations are special cases of line bundles.)
- connection between Kähler and Weil differentials (with proofs omitted at times)
- genus formula of Hurewicz / extensions of local fields
- ζ-functions of curves over finite fields
- Riemann hypothesis for curves over finite fields
- and finally, the relation of the last two items to coding theory.

Fields of genus 0.

For this lecture, assume $k \subset K$ and $\bar{k} \cap K = k$.

If $K = k(t)$, then K has genus 0. Conversely, if K has genus 0 and there exists $P \in C$ with $\deg P = 1$ (or, equivalently, $C(k) \neq \emptyset$) then $K \cong k(t)$. So the interesting case will be when $C(k) = \emptyset$.

Function fields of conics.

Now pick a non-zero (and usually irreducible over k) quadratic polynomial

$$f = \sum 0 \leq i \leq j \leq 2 a_{ij} X_i X_j \in k[X_0, X_1, X_2].$$

If f is reducible, the zero-set of each factor is a line; the two lines are either degenerate or intersect in a point. If they intersect in a point, then the variety is singular. f is irreducible iff the zero-set is non-singular, i.e., f, f_0, f_1, f_2 have no common root; or $\mathrm{char}\, k = 2$ and

$$f = aX_0^2 + bX_1^2 + cX_2^2$$

with a, b, c satisfying

$$(a : b : c) \in \mathbf{P}^2(k) - \mathbf{P}^2(k^2)$$

(which is to say, the ratios between a, b, and c are not all squares). The function field K of f is the field generated by $x = \frac{X_1}{X_0}$ and $y = \frac{X_2}{X_0}$ in $Q(k[x_0, X_1, X_2]/(f))$.

Remark. As a function on $k \times k \times k$, f is not identically 0. (Explicit argument: Suppose f were 0 as a function. Then plugging in $1, 0, 0 \Rightarrow a_{00} = 0$, similarly for a_{11} and a_{22}; then plugging in $1, 1, 0 \Rightarrow a_{01} = 0$, similarly for a_{12} and a_{02}.) So by a linear change of variables we may assum $f(0, 0, 1) \neq 0$, i.e., $a_{22} \neq 0$. Then replace f by $\frac{f}{a_{22}}$ to make $a_{22} = 1$. Then K is an extension of $k(x)$ of the form $k(x)[y]$ where y satisfies

$$y^2 + (\text{poly. in } x \text{ of deg} \leq 1) \cdot y + (\text{poly. in } x \text{ of deg} \leq 2) = 0. \tag{$*$}$$

Since this is a monic and irreducible polynomial, K is a degree 2 extension of $k(x)$.

Now we'll show the genus of K is 0. By one of the exercises,

$$K \supseteq \text{int. closure of } k[x] = \bigcup_{n \geq 0} L(nD) \supseteq k[x, y].$$

(Here D is the divisor so that $x = N - D$ with N and D effective.) Also, $k[x, y] = k[x] + yk[x]$ is a free module of rank 2 over $k[x]$.

The basic technique will be to use Riemann-Roch, which in this case says that, for $n >> 0$,

$$\dim_k L(nD) = \underbrace{\deg(nD)}_{2n} + 1 - g. \tag{$**$}$$

Claim. If $\mathrm{ord}_P\, x < 0$ (x has a pole at P, so $D \geq P$) then $\mathrm{ord}_P\, y \geq \mathrm{ord}_P\, x$.

Proof. Look at the relation $(*)$. If y has a large pole, then the first term dominates when you take the order at p, a contradiction.

From the claim, we immediately have $y \in L(D)$ and therefor

$$L(nD) \supseteq k[x]_{\deg \leq n} + y \cdot k[x]_{\deg \leq n-1}.$$

The dimension over k of the right hand side is $(n + 1) + n = 2n + 1$. Thus, by $(**)$, $g = 0$,

$$L(nD) = k[x]_{\deg \leq n} + y \cdot k[x]_{\deg \leq n-1},$$

and the integral closure of $k[x]$ is $\bigcup L(nD) = k[x, y]$. (Notice that only the trivial part of the exercise was needed.)

We have proved that **function fields of conics have genus 0**.

Question: Do we get any function fields besides the one we found earlier?

Remember that we showed that if k has genus $g = 0$, then $C(k) \neq \emptyset \Leftrightarrow \exists t : K = k(t)$. You should think

$$C(k) \text{“}=\text{”} \{P \in \mathbf{P}^2(k) : f(P) = 0\}.$$

In particular, the two sets have the same size. (*Exercise:* Check this.) Thus $K \simeq k(t) \Leftrightarrow f$ has a non-trivial zero over k.

Example: The curve with $k = \mathbf{R}$, $f = X_0^2 + X_1^2 + X_2^2$ has function field $K = \mathbf{R}(x, y), x^2 + y^2 = -1$ which has genus 0 but not isomorphic to $\mathbf{R}(x)$.

There are many more examples of non-isomorphic conics over $\mathbf{Q}$: f may fail to have a root p-adically for different p.

In particular, if $k = \bar{k}$, then $C(k) \neq \emptyset$ (since for all $P \in C$, $\deg P = 1$) and all conics are rational. There is a direct geometric proof of this: given any point P on the conic, parametrize all other points Q by the slope of the (unique) line passing through P and Q. If we choose coordinates so that P is at $(1 : 0 : 0)$ and set $x = \frac{X_1}{X_0}$ and $y = \frac{X_2}{X_0}$, then the slope $t = \frac{y}{x}$ generates the function field K.

It is a non-trivial fact that if k is *finite* all conics are rational.

Theorem. If $K \supset k$ is a function field of genus 0, then it is isomorphic to $k(t)$ or the function field of a conic.

Proof. Let at $\deg : \mathrm{Div}_K \to \mathbf{Z}$. The image is a non-zero subgroup of $\mathbf{Z}$ containing $2g - 2$, the degree of the canonical divisor. So $\deg(\mathrm{Div}_K) = d\mathbf{Z}$ for some $d \in \{1, 2\}$. (In general, $d \,|\, 2g - 2$. This is useful except when $g = 1$.)

Choose any D with $\deg D = d$. Then, by Riemann-Roch, $L(D)$ has dimension $\deg D + 1ge2 > 1$. So there is a $f \neq 0 \in L(D)$ and $(f) + D \geq 0$. So assume that D is effective and therefore $L(D) \supset k = L(0)$.

Case $d = 1$: D is *prime*, of degree 1, so $K = k(x)$ (for any $x \in L(D) - k$).

Case $d = 2$: We may assume D is prime. (Otherwise $D = P + Q$ with P and Q prime, contradicting the assumption that $d = 1$.) Then $L(D)$ is 3-dimensional:

$$L(D) = k + k \cdot x + k \cdot y.$$

x has D as a denominator divisor of degree 2, so $[K : k(x)] = 2$. Since y also has D as a denominator divisor of degree 2, $y \notin k(x)$ (as all powers of x have a larger multiple of D as denominator divisor) and $K = k(x, y)$. We must show that y satisfies a quadratic. Consider the k-vector spaces

$$L(0) \subset L(D) \subset L(2D).$$

These have dimensions, respectively, 1, 3, and 5, with new elements of a basis given by, respectively, 1; x and y; and x^2 and xy. Since $y^2 \in L(2D)$, it can be expressed in terms of this basis and satisfies a quadratic equation over $k(x)$.

[This proof will be seen in a better perspective with line bundles.]

Reference: Miranda, *Algebraic Curves and Riemann Surfaces.*

Lecture 21 (October 16, 1995).
Scribe: Matt Baker

Recall that in the last lecture, we showed that if $K \supset k$ is a function field of genus zero, then it is isomorphic to either $k(t)$ or the function field of a conic.

Here is the last detail in that argument:

We had $L(0) \subset L(D) \subset L(2D)$, and we claimed that x^2 and xy were linearly independent elements of $L(2D)$, where $1, x, y$ span $L(D)$. To see this: if we had a dependence relation, i.e. if $ax^2 + bxy \in L(D), a, b \in k$, then $ax + by \in L(0)$, so a=b=0.

There is a similar story for fields of genus one.

In general, what we do is look at the map

$$\deg : Div_K \to \mathbf{Z},$$

which contains $2g-2$ in its image because of the existence of the canonical divisor.

In the case $g = 0$, we know the degree map is either onto or has cokernel of order 2. But a priori, for $g > 0$, we don't know much else about the image of this map. An interesting question to think about (but about which we won't say a whole lot more) is the folowing.

Problem: Given $n \in \mathbf{Z}_{>0}$, construct a field k plus a function field of genus 1 over k such that image(deg) $= n\mathbf{Z}$.

Now, let K/k have genus 1, and suppose that the degree map is **surjective**. Recall: Riemann-Roch says that (if we let D be a divisor of degree m)

$$l(D) = m, (m > 0)$$

$$l(D) = 0, (m < 0)$$

In general, $l(D) \leq 1+$ deg(D), and if deg(D)=0,

$$l(D) = 1, (D = (f))$$

$$l(D) = 0, (D \neq (f)).$$

So the canonical divisor, which has degree $2g-2 = 0$, must be equivalent to 0 as an element of the divisor class group.

Now choose a divisor D with deg(D)=1. [Which we can do by the assumption that deg is surjective].

Then $L(D)$ has dimension $l(D) = 1$, so $(f) + D \geq 0$ for some nonzero element $f \in K^*$. Hence there is an effective divisor of degree 1, i.e., a prime divisor P_0 with $\deg P_0 = 1$. This means that $P_0 \in C(k)$.

We will now keep this point P_0 fixed for a while [some people who work with elliptic curves call this point 0, because it acts as the identity element in the group law on such curves].

An **elliptic curve** can be defined as a function field of genus one plus a point of degree 1 in $C(k)$. As was the case for fields of genus zero, we can extract some useful information by writing out a chain of vector spaces

$$L_0 \subset L_1 \subset L_2 \ldots \subset L_6,$$

where $L_n = L(nP_0)$ has dimension 1 for $n = 0$ and dimension n for $n = 1, 2, \ldots, 6$ (Riemann-Roch). A search for explicit elements of these vector spaces yields the following members:

$$1 \in L(0)$$

$$x \in L(2P_0)$$

$$y \in L(3P_0)$$

$$x^2 \in L(4P_0)$$

$$xy \in L(5P_0)$$

$$y^2, x^3 \in L(6P_0).$$

Note that here x has a pole of order exactly 2 at P_0, and no pole anywhere else. x is also unique, up to a linear transformation.

By 6-dimensionality of $L(6P_0)$, there is a linear relation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where we have normalized the coefficients of y^2, x^3 to make them both equal to 1 [see Knapp's 'Elliptic Curves' for a detailed description of this normalization, as well as an explanation of the terminology for the coefficients].

Notice that $[K : k(x)] = 2$, and as in one of the homework problems, one sees that $e(P_0/\infty) = 2$, since $v_{P_0}(x) = -2$ and $v_\infty(x) = -1$. Also, since $v_{P_0}(y) = -3$, we have $y \notin k(x)$, so $K = k(x, y)$.

It is also easy to use a ramification argument to establish the irreducibility of the linear relation between x and y.

Notice that if we write down a_1, a_3, a_2, a_4, a_6, then we can determine if we get an elliptic curve or not by looking at whether $k[x, y]$ is the integral closure of $k[x]$ in K. This is, by the homework, some sort of polynomial condition that can be easily verified.

To elaborate on this slightly, note that if A (= integral closure of $k[x]$ in K), which is equal to $\cup_{n\geq 0} L(nP_0)$, is strictly bigger than $k[x, y]$, then there exists $z \in L(nP_0) - k[x, y]$ for some n, and by subtracting appropriate combinations of x, y, we may assume that $z \in L(P_0)$. Then z generates the whole function field, so the genus is zero.

We now move on to a different topic: line bundles, linear systems, and maps to projective space.

Notice the following pattern in our classification of low-genus function fields:

$g = 0 : L(0) \subset L(P)$, deg=1,$l = 2$, $C \cong \mathbf{P^1}$

$g = 0 : L(0) \subset L(P)$, deg=2,$l = 3$, $C \cong$ conic in $\mathbf{P^2}$

$g = 1 : L(0) \subset L(3P)$, deg=3,$l = 3$, $C \cong$ cubic in $\mathbf{P^2}$.

In each case, the degree is the degree of the corresponding curve, and l is one more than the dimension of the corresponding projective space. To help explain what's going on with the geometry here, it is useful to introduce the notion of a line bundle. So given k, K, C as above:

Def: A **line bundle** on C is a one-dimensional vector space $\mathcal{L}$ over K together with, for every closed point $P \in C$, a free O_P-module $\mathcal{L}_P \subset \mathcal{L}$ of rank 1, such that for every $x \in \mathcal{L} - 0$, one has $O_P x = \mathcal{L}_P$ for almost all P.

Example: $\mathcal{L} = K, \mathcal{L}_P = O_P$. If we have just one point, this is the only example of a line bundle, up to isomorphism.

Def: An **isomorphism** of line bundles $\mathcal{L}, \mathcal{M}$ is a K-linear isomorphism from $\mathcal{L}$ to $\mathcal{M}$ mapping $\mathcal{L}_P$ isomorphically onto $\mathcal{M}_P$ for all P.

The set of isomorphism classes of line bundles forms a group with the tensor product as multiplication [note the analogy with number theory]. The unit element is given by the trivial line bundle from the above example, and inverses are given by the K (resp. O_P)-linear duals. This group is defined to be the **Picard group** Pic C = Pic K.

Next time, we will relate this definition to divisors and give some geometric intuition of what this all means.

Lecture 22 (October 18, 1995).
Scribe: Diane Maclagan

Recall in the last lecture we studied fields of low genus.

Take a divisor D with $L(D) \neq \{0\}$. This gives rise to a map $\phi : C \to \mathbf{P}^{l(D)-1}$. This is not an embedding in general. The degree in the table in the previous lecture comes from the degree of the curve in projective space, which is well defined (for more information on this see Hartshorne).

In Number Theory, we deal with a number field K and its ring of integers $\mathcal{O}$, and consider the class group $cl(\mathcal{O})$ whose elements are the classes of fractional ideals factored by the group of principal fractional ideals.

In our context we take the collection of projective $\mathcal{O}$ modules of rank 1.

Definition: If A is a non-zero Noetherian ring, a projective A module of rank 1 is a finitely generated A module M such that $\forall p\, M_p \cong_{A_p} A_p$.

A one dimensional object is obtained when a projective A module is localized.

Definition: A Line Bundle on C is a one dimensional K vector space $\mathcal{L}$ together with, for each $P \in C$ a free $\mathcal{O}_P$ module $\mathcal{L}_P \subseteq \mathcal{L}$ of rank 1 such that $\forall x \in \mathcal{L} - \{0\}$ $\forall P$ with finely many exceptions $\mathcal{O}_P x = \mathcal{L}_P$

The trivial example of a line bundle is $\mathcal{L} = K$, and $\mathcal{L}_P = \mathcal{O}_P$ $\forall P$.

If the curve has only one point then the trivial line bundle is the only one up to isomorphism.

Another example of a line bundle is got by starting with a divisor $D = \sum n(P)P$, and taking $\mathcal{L} = \mathcal{L}(D) = K$ and $\mathcal{L}_P = \mathcal{L}_P(D) = \mathbf{m}_P^{-n(P)}$

Recall that two line bundles are isomorphic if there is an isomorphism between the vector spaces taking one $\mathcal{L}_P$ to the other. It is not hard to show that every line bundle is isomorphic to $\mathcal{L}(D)$ for some D. This D is uniquely determined up to a principal divisor. So we have a bijection:
Pic(C)={group of line bundles on C} $\rightleftharpoons$ { divisor class group of K}

where $[D] \mapsto \mathcal{L}(D)$ and $\mathcal{L} \mapsto \sum n(P)P$ where the $n(P)$ are calculated as follows: Choose a basis vector $x \in \mathcal{L} - \{0\}$ and look at the submodule $)_P x = \mathbf{m}_P^{-n(P)} \mathcal{L}_P$. We need to to show that $\mathcal{L}(D_1 + D_2) \cong \mathcal{L}(D_1) \otimes \mathcal{L}(D_2)$. Note that by abuse of notation this also means showing this for the $\mathcal{L}_P$ as well.

We define deg $\mathcal{L} = \sum n(P)\text{deg}P$. This does not depend on the basis because $\text{deg}(f) = 0$.

If $U \subseteq C$ is open (i.e. empty or cofinite) we define

$$\mathcal{L}(U) = \bigcap_{P \in U} \mathcal{L}_P$$

$$\mathcal{L}(C) = \bigcap_{P} \mathcal{L}_P$$

The connection with Riemann-Roch is that if $\mathcal{L} = \mathcal{L}(D)$ then $\mathcal{L}(D)(C) = L(D)$.

Lecture 23 (October 20, 1995).
Scribe: Emiliano Gómez

Today we will see some examples of line bundles. We will also define linear systems on a curve C. This will lead us to find a connection between rational maps of curves into projective space $\mathbf{P}^n(k)$ and line bundles (with an additional vector spa ce structure).

As usual, let K/k be a finitely generated field extension of trascendence degree 1, and let C be the "abstract curve" thus defined: C is the set of valuation rings of K over k.

Recall the definition of a line bundle on C:

Definition: a **line bundle** on C is a one-dimensional K-vector space $\mathcal{L}$ together with, for each $P \in C$, a free $\mathcal{O}_P$-module $\mathcal{L}_P \subset \mathcal{L}$ of rank 1, such that for all $x \in \mathcal{L} - \{0\}$, we have $\mathcal{O}_P \cdot x = \mathcal{L}_P$ for almost all P.

Also, recall that we defined the set of **global sections** of C as the set $\mathcal{L}(C) = \bigcap_{P \in C} \mathcal{L}_P$

We also defined, given a divisor D, a line bundle $\mathcal{L}(D)$, for which the set of global sections is $L(D)$ (see last lecture).

For the rest of this lecture, we will assume that $\overline{k} = k$ (i.e. that k is algebraically closed), and we will write $\mathbf{P}^n$ for the nth-dimensional projective space over k.

Now we will see some examples of line bundles on $\mathbf{P}^n$:

The **tautological** line bundle on $\mathbf{P}^n$ is defined as

$$\mathcal{L} = \{(x, y) \in k^{n+1} \times \mathbf{P}^n | x \in y\}$$

Here we are thinking of $\mathbf{P}^n$ as the curve of a function field.

Note that we have a natural map $\mathcal{L} \longrightarrow \mathbf{P}^n$, given by $(x, y) \longmapsto y$

This line bundle has only one section, namely the zero section. For this reason, it is not useful to us.

However, things change drastically when we look at its inverse (recall that the isomorphism classes of line bundles on a curve C form a group Pic C).

The inverse of $\mathcal{L}$ is obtained by dualizing (see last lecture). So we look at the fiber of every $y \in \mathbf{P}^n$. This is a "line", whose inverse (dual) gives us the fiber over y in $\mathcal{L}^{-1}$. Therefore, the inverse of the tautological line bundle is

$$\mathcal{L}^{-1} = \{(x, y) | y \in \mathbf{P}^n, x \in k^{n+1}/y^{\perp}\}$$

Here $k^{n+1}/y^{\perp} = \mathrm{Hom}_k(y, k)$. We have an inner product $k^{n+1} \times k^{n+1} \longrightarrow k$, sending $(x, y) \longmapsto \langle x, y\rangle$, and $y^{\perp} = \{x | \langle x, y\rangle = 0\}$

Note again that there is a natural map $\mathcal{L}^{-1} \longrightarrow \mathbf{P}^n$.

It turns out that Pic $\mathbf{P}^n$ is infinite cyclic, with generators $\mathcal{L}$ and $\mathcal{L}^{-1}$. The latter is the "better" generator, because it has lots of sections, as opposed to the tautological line bundle.

Next let us consider line bundles on $\mathbf{P}^1$:

Recall that Pic C is isomorphic to the divisor class group. If the genus of the function field is zero, then the degree map Pic $C \longrightarrow \mathbf{Z}$ is injective (exercise 19 on the homework). With our assumption that $\overline{k} = k$, we actu ally have an isomorphism. So we can write a line bundle for each integer.

We can form our function field as $K = k(t) =$ degree-0-piece of $S^{-1}k[x_0, x_1]$, where $t = \frac{x_1}{x_0}$, and S is the set of nonzero homogeneous elements of $k[x_0, x_1]$. We can write

$$S^{-1}k[x_0, x_1] = \bigoplus_{n \in \mathbf{Z}} R_n$$

The piece of degree zero is $R_0 = K$ What about the other pieces?

They are isomorphic to one another upon multiplication by a suitable power of x_0. So $\dim_K R_n = 1$. Thus they are one-dimensional vector spaces over K.

Each R_n has a line bundle structure of degree n.

We have that R_1 is our "nice" generator of Pic $\mathbf{P}^1$, having degree 1. The tautological bundle on $\mathbf{P}^1$ has degree -1, and so, as remarked above, it has no sections other than zero, because it corresponds to a divisor D of degree -1, and so $\mathcal{L}(C) = L(D) = 0$.

If we give R_1 a line bundle structure and call it R_1 also, then $x_0, x_1 \in R_1(C)$, i.e. x_0, x_1 are global sections.

Having seen these examples, let us again focus on finding a nice connection between morphisms from a curve to projective space and line bundles on the curve.

We will see that this connection is realized through some special sets of divisors (basepoint free linear systems on the curve), which we are about to define.

Also, we will end up with an additional vector space structure on the line bundles, and we will often be able to use the Riemann-Roch theorem to obtain information about this additional structure.

We are still assuming that $\overline{k} = k$, to save us some trouble.

Let K, k and C be as usual.

Definition: a **linear system** on C is a set S of effective divisors of C s.t. $\exists$ a divisor D' of C and a sub-k-vector space $V \subset L(D')$ of dimension n+1 s.t.

$$S = \{(f) + D' | f \in V - \{0\}\}$$

Definition: Let S be a linear system on C. We say that $P \in C$ is a **basepoint** of S if $\forall D \in S, D \geq P$.

We say that S is **basepoint free** if it has no basepoints.

Remark: Note that it is not required that a basepoint of S be an element of S.

We have an equivalence between, on one hand, non-degenerate morphisms from C to $\mathbf{P}^n$, up to Aut $\mathbf{P}^n$ (i.e. up to linear changes of coordinates), and, on the other hand, basepoint free linear systems on C.

The correspondence from the first set to the second is obtained as follows:

Given C, it will intersect an (n-1)-dimensional hyperplane of $\mathbf{P}^n$ at a finite number of points (count multiplicities), thus giving rise to an effective divisor. If we consider all such hyperplanes, we obtain a set S of effective divisors, whic h will be our basepoint free linear system on C.

Next time we will finally obtain the connection between the above morphisms and line bundles on C, with a certain additional structure. We will thus get another set (involving line bundles) which gives us equivalences to the above two sets.

Lecture 24 (October 23, 1995).
Scribe: Lawren Smitline

Today, Professor Lenstra wore a plaid jacket, striped shirt, and a red and navy blue striped tie with a narrow gold stripe.

Recall C is a curve corresponding to a function field K over k.

A *linear system* on C is a set S of effective divisors on C for which there exists a divisor D on C and a subspace $V \subset L(D)$ such that

$S = \{(f) + D : f \in V - \{0\}\}$.
(Note that the divisors (f) are elements of $\mathbf{P}V \cong (V - \{0\})/k^{\times}$.)

A point $P \in C$ is a *base point* for S if for all $D \subset S$, $D \geq P$.
S is called *base point free* if it has no base points.

Example 0. $S = \emptyset$. Take any D' and $V = \{0\}$. Every point is a base point.

Example 1. Take any D' and $V = L(D)$. The resulting linear system is called a complete linear system and is denoted $|D'|$.
$|D'| = \{D \geq 0 : D \sim D'\}$.
P is a base point for $|D'|$ if and only if $l(D' - P) = l(D')$.

Suppose S is a nonempty linear system. Then (D', V) is uniquely determined up to $D' \to D' + (g)$, $V \to g^{-1}V$, for $g \in K^{\times}$.
If D' and D'' give the same S, then they are linearly equivalent. So only the divisor class of D' is determined up to equivalence. So only the line bundle associated to D' is well defined in terms of S.

What does this V have to do with the linear system?
A nonempty linear system corresponds to a pear (of the bosc variety) consisting of a line bundle $\mathcal{L}$ plus a subspace $V \subset \mathcal{L}(C)$ of the space of global sections of $\mathcal{L}$ $(= \bigcap_{P \in C} \mathcal{L}_P.)$

P is a base point $\Leftrightarrow V \subset \mathfrak{m}_P \mathcal{L}_P$.
base point free $\Leftrightarrow$ the global sections in V generate $\mathcal{L}$.
You are supposed to be able to do that without thinking and hopefully will do that.

Now we have three equivalent formulations, depending on your language.
$\{$nondegenerate maps $C \to \mathbf{P}^n\}/ \cong_{\mathbf{P}^n} \leftrightarrow$
$\{$base point free linear systems on C where $\dim V = n + 1\} \leftrightarrow$
$\{$line bundles $\mathcal{L}$ plus V a dimension $n + 1$ space of global sections of $\mathcal{L}$ generating $\mathcal{L}\}$.

Let $f : C \to \mathbf{P}^n$, with image C'. Let $H \subset \mathbf{P}^n$ be a hyperplane. $H \cap C'$ gives an effective divisor on C, and the set $\{H \cap C' :$ hyperplane $H \subset \mathbf{P}^n\}$ has the structure of a projective space, and is the same as S. If $\mathcal{M}$ is the tautological line bundle on $\mathbf{P}^n$, then $S = f^*\mathcal{M}$.

Suppose C is a curve and one has an $n + 1$ dimensional space of global sections. Then one has $f_0 \ldots f_n$ not all 0 at any point, by base point freeness. So let
$f : P \mapsto (f_0(P) : \ldots : f_n(P)) \in \mathbf{P}^n$.

When we have $f : C \to \mathbf{P}^n$, we have C as an algebraic subset. How do we express the condition that C is a closed embedding?
A very ample line bundle is generated by its global sections....

Lecture 25 (October 25, 1995).
Scribe: Emiliano Gómez

Let $k \subset K$ and C be as usual, with k algebraically closed.

Recall that last time we got a "dictionary" (an equivalence) between the set of morphisms

$\varphi : C \longrightarrow \mathbf{P}^n$ (non-degenerate, and up to linear changes of coordinates of $\mathbf{P}^n$)

and the set of pairs

$(\mathcal{L}, V)$, where $\mathcal{L}$ is a line bundle on C and $V \subset \mathcal{L}(C)$ is an n+1-dimensional vector space of global sections of $\mathcal{L}$ such that "V generates $\mathcal{L}$."

(We will not define what it means, in general, for the global sections in V to generate $\mathcal{L}$. See Hartshorne, Ch.2, sec.7)

A question that comes up is: which pairs $(\mathcal{L}, V)$ give rise (under this equivalence) to closed embeddings (i.e. $\varphi : C \xrightarrow{\simeq} \varphi(C)$) ?

We will not answer this question in general. Let us consider only the case $V = \mathcal{L}(C)$ (i.e. the space of all global sections):

Recall that any line bundle $\mathcal{L}$ is isomorphic to $\mathcal{L}(D)$ (the bundle coming from the divisor D, defined some lectures ago) for some divisor D.

So let D be such that our line bundle $\mathcal{L}$ is isomporphic to $\mathcal{L}(D)$.

Let S be the complete linear system associated to D. We saw last time that P is a basepoint for S iff $l(D-P) = l(D)$. And we also remarked that S is basepoint free iff the global sections of V generate $\mathcal{L}$.

vCombining these two results, we see that

$V = \mathcal{L}(C)$ generates $\mathcal{L}$ iff $\forall P : l(D-P) < l(D)$.

Since we are assuming that $\overline{k} = k$ (so deg$P = 1$ for all $P \in C$ closed), the Riemann theorem tells us that $l(D-P)$ and $l(D)$ may differ by at most 1.

Therefore, the above inequality is equivalent to $l(D-P) = l(D) - 1$.

From this discussion we get the following result:

$(\mathcal{L}, V)$ with $V = \mathcal{L}(C)$ gives rise to a closed embedding if and only if $\forall P, Q$ (closed points of C), we have $l(D-P-Q) = l(D) - 2$.

Note that we can use the Riemann-Roch Theorem to check whether the last condition holds or not. Also note that for $P \neq Q$, this condition merely guarantees that φ is injective. But when we consider the case $P = Q$, we get that φ is a c losed embedding.

For example, if deg$D \geq 2g+1$, then $D, D-P$ and $D-P-Q$ all have deg $> 2g-2$, so that (recall that in such a case we have $c(*) = 0$)

$l(*) = \deg(*) + 1 - g$,

so the above condition is satisfied (because $\deg(D-P-Q) =$ deg$D$ - deg$P$ - deg$Q$ = deg$D$ - 2, since $\overline{k} = k$ implies deg$P$ = deg$Q$ = 1).

So we see that if we take a line bundle of large enough degree (i.e. $\mathcal{L} \cong \mathcal{L}(D)$ with $\deg D$ large enough), then we will have a closed embedding into projective space.

We finish this discussion with two facts which we will not prove:

Recall that the canonical divisor W_λ is defined, up to divisor class, independently of the Weil differential $\lambda \neq 0$. We have that

- $[\forall P, l(W_\lambda - P) < l(W_\lambda)]$ if and only if $g > 0$
- $[\forall P, Q$ (closed), $l(W_\lambda - P - Q) = l(W_\lambda) - 2]$ if and only if C is not a hyperelliptic curve.

Now we come back to the theory. We will talk about differentials:

Kähler differentials and Weil differentials

Eventually, we will get a connection between these two types of differentials (recall that we have already met the Weil differentials). Often times we will obtain isomorphism.

Let A be a ring (that is, a commutative ring with 1), let B be an A-Algebra (that is, a ring with a ring homomorphism $\phi : A \longrightarrow B$), and let M be a B-module.

Note that M has a natural A-module structure, and so does B.

Definition: an **A-derivation** $B \longrightarrow M$ is an A-linear map D such that $\forall x, y \in B$, $D(xy) = xD(y) + yD(x)$.

Note: in general, D will not be B-linear. Also, note that D is an additive group homomorphism (by definition of "A-linear map"), and that the composite map

$A \xrightarrow{\phi} B \xrightarrow{D} M = 0$.

To see this, we observe that for $x \in A$ and $y \in B$, we must have (by definition of "A-linear", again) $D(\phi(x)y) = \phi(x)D(y)$.

Taking $y = 1$ we have $D(\phi(x)) = \phi(x)D(1) = 0$, as claimed, because

$D(1) = D(1 \cdot 1) = D(1) + D(1)$ implies that $D(1) = 0$.

Note that if $D : B \longrightarrow M$ is an A-derivation and $\tau : M \longrightarrow M'$ is a B-linear map, then the composite map

$\tau \circ D : B \longrightarrow M'$ is an A-derivation from B to M'.

Universal Derivation:

Define the B-module $\Omega_{B/A}$ by generators and relations as follows:

generators: one symbol, db, for each $b \in B$.

relations: $d(b + b') = db + db'$ for all $b, b' \in B$.

$da = 0$ for all $a \in \phi(A)$.

$d(bb') = b \cdot db' + b' \cdot db$ for all $b, b' \in B$.

Definition: $\Omega_{B/A}$ is the module of **Kähler differentials** of B over A.

Note that the (obvious) map $d : B \longrightarrow \Omega_{B/A}$ is a derivation (simply because we forced it to be the case).

It is a universal derivation, in the sense that for all B-modules M, the map $\mathrm{Hom}_B(\Omega_{B/A}, M) \longrightarrow \mathrm{Der}_A(B, M)$, given by $g \longmapsto g \circ d$, is bijective.

Here $\mathrm{Der}_A(B, M)$ is the set of A-derivations $B \longrightarrow M$.

So, if placed in the right category. $\Omega_{B/A}$ is a universal object, hence it is unique (satisfying the universal property) up to isompophism .

Let $k \subset K$ be a field extension. Then one can check that $\mathrm{Der}_k(K, K) \cong$ (K-dual of $\Omega_{K/k}$).

Suppose that B is given by a "presentation" $B = A[X_i | i \in I]/(f_j | j \in J)$. Then one can show without much difficulty (although we will not do so here) that

$$\Omega_{B/A} = \Big(\sum_i B[dX_i]\Big) \Big/ \Big(B \sum_i \frac{\partial f_j}{\partial X_i}[dX_i] \;\Big|\; j \in J\Big)$$

Here dX_i is the formal symbol associated to X_i.

Since $\Omega_{B/A}$ is a universal object, we see that the right-hand side of this equation is actually independent of the presentation that we gave B.

Lecture 26. (October 27, 1995).
Scribe: Dylan Thurston

Kähler differentials and Weil differentials

This section is a survey of results. Proofs are omitted since they are

- not need in the sequel
- completely elementary

and • too long.

For $A \to B$ any map of rings, last time I defined a B-module $\Omega_{B/A}$ of Kähler differentials. This comes with an A-linear map $d : B \to \Omega_{B/A}$ satisfying the derivation property:

$$d(b_1 b_2) = b_1 db_2 + b_2 db_1$$

and a universal property: given $D : B \to M$ another derivation, there is a unique B-linear map $f : \Omega_{B/A} \to M$ so that $d \circ f = D$.

References: E. Kunz, *Kähler Differentials*, Vieweg, 1986. Hartshorne, *Algebraic Geometry*, Chapter II, Section 8, page 173.

Example: $B = a[X_i \mid i \in I]$. Then $\Omega_{B/A}$ is B-free on dX_i, $i \in I$ and the map $d : B \to \Omega_{B/A} = \bigoplus_{i \in I} B\, dX_i$ is

$$df = \sum_{i \in I} \frac{\partial f}{\partial X_i}, dX_i.$$

It's an easy check that this is a derivation and universal.

Rules:

1) For $S \subset B$ a multiplicative set,

$$\Omega_{S^{-1}B/A} = S^{-1}\Omega_{B/A} \ (= \Omega_{B/A} \otimes_B S^{-1}B)$$

In particular, if k is a field, then $\Omega_{k(X_i|i\in I)/k}$ is a vector space of $k(X_i)$ with basis dX_i. In this case, $\dim \Omega =$ transcendence degree of extension.

2) Base change: given a map $A \to A'$, there is a natural map $A' \to B' = B \otimes_A A'$ and

$$\Omega B'/A' = \Omega_{B/A} \otimes_B B'.$$

3) Quotients: for any ideal $I \subset B$, set $C = B/I$. Then $\Omega_{C/A}$ is a B-module and the map from $\Omega_{B/A}$ to $\Omega_{C/A}$ is surjective. Then formally,

$$\Omega_{C_A} = \underbrace{(\Omega_{B/A} \otimes_B C)}_{\Omega_{B/A}/I\Omega_{B/A}} / \text{“}dI\text{”}.$$

The notation “dI” means that there is an exact sequence of C-modules

$$\underbrace{I/I^2}_{I\otimes_B C} \xrightarrow{d} \Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to 0$$

(Note that d becomes C-linear when you mod out by I^2.) For instance, take $B = A[X_i \mid i \in I]$ and $C = B/(f_j \mid j \in J)$. Then

$$\Omega_{C/A} = \Big(\bigoplus_{i\in I} C \cdot dX_i\Big) \Big/ \Big(\sum_{j\in J} C \cdot \sum_{i \in I} \frac{\partial f_j}{X_i}\, dX_i\Big).$$

(This will be used to define *smoothness*, which is a better notion than *regular* for non-algebraically closed base fields.)

Hartshorne also considers the situation of three rings with maps $A \to B \to C$. There are three Kähler differentials: $\Omega_{B/A}$, $\Omega_{C/B}$, and $\Omega_{C/A}$, with an exact sequence relating them:

$$\Omega_{B/A} \otimes C \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

(The map between the last two C-modules is defined by the universal property, since any B-linear derivation is also A-linear.)

The ultra-classical case of this theory is **Kähler differentials of field extensions**. Suppose $k \subset K$ is any field extension; then the problem is to investigate $\Omega_{K/k}$.

Question: What is the dimension of $\Omega_{K/k}$ (as a K-vector space)?

$\underline{\operatorname{char} k = 0}$

By general field theory, K is an algebraic seperable extension of $k_0 = k(X_i \mid i \in I)$ for some I. Since the characteristic is 0, every generator of K/k_0 has a seperable irrudicible polynomial. By adding these generators one by one, at each stage getting a new generator and relation, one can show that

$$\Omega_{K/k} = \Omega_{k_0/k} \otimes_{k_0} K.$$

The following three facts are immediate: (1) If $x_1, \ldots, x_n \in K$ then $dx_1, \ldots, dx_n$ are linearly independent over K if and only if $x_1, \ldots, x_n$ are algebraically indpendent over K. (2) $\dim_K \Omega_{K/k} = \operatorname{tr}\deg[K/k]$. (3) $dx = 0$ if and only if x is algebraic over k. When $\operatorname{char} k = p > 0$, facts (1) and (3) fail badly; but, oddly enough, (2) is still true if K/k is seperably generated.

$\underline{\operatorname{char} k = p > 0}$

In this case, for any $\alpha \in K$ we have

$$d\alpha^p = p\alpha^{p-1}\, d\alpha = 0$$

so $\Omega_{K/k} = \Omega_{K/k\cdot K^p}$; i.e., we can reduce immediately to the case of an algebraic, heavily inseperable extension. If $x_1, \ldots, x_n \in K$, then

$$dx_1, \ldots, dx_n \text{ linearly independent over } K \iff [k \cdot K^p(x_1, \ldots, x_n) : k \cdot K^p] = n.$$

(This is the basis of the subject of "p-independence.") For instance, $[K : k \cdot K^p] = p^{\dim_K \Omega_{K/k}}$. (When the exponent is not finite, set $p^{\text{cardinal}} = \text{cardinal}$.)

One can show that if $\operatorname{char} = p > 0$ and K/k is finitely generated, then $\dim_K \Omega_{K/k} \geq \operatorname{tr}\deg K/k$, with equality if and only if K/k is seperably generated; in particular, if k is perfect. The condition "finitely generated" is necessary. For instance, if K is a perfect field in $\operatorname{char} k \neq 0$, then for all $\beta \in K$, $d\beta = 0$.

Proof that if k is perfect and K/k is finitely generated, $[K : k \cdot K^p] = p^{\operatorname{tr}\deg(K/k)}$. Let $x_1, \ldots, x_n$ be a transcendence basis for K over k and set $k_0 = k(x_1, \ldots, x_n)$. The fields K, K^p, k_0, and $k_0^p = k(x_1^p, \ldots, x_n^p)$ form a square of field extensions. The p'th power map takes the field extension K/k_0 to K^p/k_0^p, so in particular $[K : k_0] = [K^p : k_0^p]$; therefore

$$[K : K^p] = \frac{[K : k_0^p]}{[K^p : k_0^p]} = \frac{[K : k_0][k_0 : k_0^p]}{[K^p : k_0^p]} = p^n$$

as desired.

As a special case, for function fields over perfect k, the Kähler differentials are 1-dimensional. (This is also true for seperably generated function fields, but only when k is perfect is there a canonical isomorphism of the Kähler differentials with the Weil differentials.)

Lecture 27 (October 30, 1995).
Scribe: Nghi Nguyen

Kahler Differentials vs Weil Diffierentials

Relevant fact from last time: Suppose K/k is a finitely generated field extension. Then $dim_{\mathrm{K}}\Omega_{\mathrm{K/k}} \geq$ tr.deg(K/k) with equality occurs iff K/k is separably generated.

An example of Kahler differentials from number theory: Let $\mathcal{O}$ be the ring of integers in an algebraic number field. Then $\Omega_{\mathcal{O}/\mathbf{Z}} \cong_{\mathcal{O}} \mathcal{O}/\mathcal{D}_{\mathcal{O}/\mathbf{Z}}$, here $\mathcal{D}$ denotes the different.

Definition: a point P on an n-dimensional variety X over a field k is called non-singular or smooth if $\Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}}$ is free of rank n as an $\mathcal{O}_{\mathrm{P}}$-module.

Remarks:

i) If P is non-singular, then $\mathcal{O}_{\mathrm{P}}$ is a regular ring. And the converse is true if k is a perfect field.

ii) Suppose K/k is a finitely generated field extension of transcendence degree 1. Then $\Omega_{\mathrm{K/k}} \cong_{\mathrm{K}} \mathrm{K}$ (so the generic point is always non-singular.). If $\mathrm{P} \in \mathrm{C(K)}$ is non-singular, then $\Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}} \cong_{\mathcal{O}_{\mathrm{P}}} \mathcal{O}_{\mathrm{P}}$.

For the rest of the lecture we will assume that there exists a $\mathrm{t} \in \mathrm{K}$ such that $\mathrm{K} \supset \mathrm{k(t)}$ is finite separable. Then $\dim_{\mathrm{K}} \Omega_{\mathrm{K/k}} = 1$. We want to compare $\Omega_{\mathrm{K/k}}$ and $\mathrm{Diff}_{\mathrm{K}}$. There is a natural homomorphism $\Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}} \longrightarrow \Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}} \otimes_{\mathcal{O}_{\mathrm{P}}} \mathrm{K} = \Omega_{\mathrm{K/k}} = \mathrm{K.dt}$. Since $\mathcal{O}_{\mathrm{P}}$ is a PID, $\Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}} \cong \mathcal{O}_{\mathrm{P}}{}^{\oplus \cdots} \oplus (\text{torsion})$. Therefore the image of $\Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}}$ in $\Omega_{\mathrm{K/k}}$ is free of rank 1. Infact, for almost all P one has $\Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}} \cong \mathcal{O}_{\mathrm{P}}.\mathrm{dt}$ (hence P is smooth.) So $\Omega_{\mathrm{K/k}}$ plus the images of the $\Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}}$'s form a line bundle.

Theorem: Suppose that K/k is separably generated of tr.deg=1. Then there is a K-vector space isomorphism $\mathrm{c}:\Omega_{\mathrm{K/k}} \longrightarrow \mathrm{Diff}_{\mathrm{K}}$ such that $\mathrm{c}((\Omega_{\mathrm{K/k}})_{\mathrm{p}}) \subseteq (\mathrm{Diff}_{\mathrm{K}})_{\mathrm{p}}$ for all P, and that the inclusion becomes = for all smooth P.

Before giving the proof of this theorem we recall that $\mathrm{Diff}_{\mathrm{K}} = \{$ continuous k-linear maps $\mathbf{A}_{\mathrm{K}} \longrightarrow \mathrm{k}$, zero on K $\}$ and $(\mathrm{Diff}_{\mathrm{K}})_{\mathrm{P}} = \{$ elements in $\mathrm{Diff}_{\mathrm{K}}$ which are also zero on $\hat{\mathcal{O}_{\mathrm{P}}}\}$. We also have the following fact:

$$\mathrm{P}\ (\text{closed point}) \in \mathrm{C} \text{ is smooth} \Longleftrightarrow \Omega_{\mathcal{O}_{\mathrm{P}/\mathrm{k}}} \cong (\Omega_{\mathrm{K/k}})_{\mathcal{O}_{\mathrm{P}}}$$

$$\Longleftrightarrow \exists \alpha \in \mathcal{O}_{\mathrm{P}} \text{ such that } \mathcal{O}_{\mathrm{P}}/\underline{\mathrm{m}}_{\mathrm{P}} = \mathrm{k}(\alpha \bmod \underline{\mathrm{m}}_{\mathrm{P}})$$

$$\text{and if } f = \text{irreducible polynomial of } (\alpha \bmod \underline{\mathrm{m}}_P) \text{ over k then } f(\alpha) \in \underline{\mathrm{m}}_{\mathrm{P}} - \underline{\mathrm{m}}_P^2$$

$$(\text{ie, } \underline{\mathrm{m}}_P = \mathcal{O}_{\mathrm{P}}.f(\alpha))$$

Now we begin the proof of the theorem: (cf. J.Tate, Residues of Differentials On Curves, Ann. Scient. Ec. Nom. Sup. 1 (1968), pp. 149-159, or K.Iwasawa, Algebraic functions, AMS 1993, Appendix)

First we need some facts about vector space endomorphisms. Let V be a vector space over a field k. An endomorphism $f\colon \mathrm{V} \longrightarrow \mathrm{V}$ is called *finite potent* if $\exists \mathrm{n} \geq 0$ such that $dim_{\mathrm{k}} f^{\mathrm{n}}(\mathrm{V})$ is finite. This is equivalent to saying that there exists a finite subspace $\mathrm{W} \subset \mathrm{V}$ such that $f(\mathrm{W}) \subset \mathrm{W}$ and f is nilpotent on V/W.

Suppose that f is finite potent, we define

$$\mathrm{Tr}(f) = \mathrm{Tr}(f \mid \mathrm{W})$$

, where W is the subspace above. Then the followings are true:

i) If V' is a subspace of V such that $f(\mathrm{V}') \subset \mathrm{V}$ then $\mathrm{Tr}_{\mathrm{V}}(f) = \mathrm{Tr}_{\mathrm{V}'}(f) + \mathrm{Tr}_{\mathrm{V}/\mathrm{V}'}(f)$.

ii) If $f\colon \mathrm{V} \longrightarrow \mathrm{U}$and $g\colon \mathrm{U} \longrightarrow \mathrm{V}$ are such that fg is finite-potent, then gf is also finite-potent and we have $\mathrm{Tr}_{\mathrm{V}}(gf) = \mathrm{Tr}_{\mathrm{U}}(fg)$.

Remark: If f, g, and $f+g$ are all finite-potent, it is not always true that $\mathrm{Tr}(f+g) = \mathrm{Tr}(f) + \mathrm{Tr}(g)$.

Lecture 28 (November 1, 1995).
Scribe: Wayne Whitney

As usual, we let $K \supset k$ be a function field of a curve, that is we ask that $K \supset k$ be finitely generated of transcendence degree 1. Furthermore, today we impose the condition that $K \supset k$ is separably generated. We will discuss the following theorem of Tate:

Theorem There exists a K-linear isomorphism $c : \Omega_{K/k} \to \mathrm{Diff}_{K/k}$ such that c induces a map $\Omega_{O_P/k} \to (\mathrm{Diff}_{K/k})_P$ for each $P \in C$, and this induced map is an isomorphism if and only if P is a smooth point. Thus if C is smooth, c is an isomorphism of line bundles.

Classical Approach to the Theorem

Giving a K-linear map $c : \Omega_{K/k} \to \mathrm{Diff}_{K/k}$ is equivalent to giving a k-linear derivation $D : K \to \mathrm{Diff}_{K/k}$, by the universal property of $\Omega_{K/k}$. Then for $y \in K$, we want $D(y) \in \mathrm{Diff}_{K/k}$, that is $D(y)$ should be a continuous k-linear map $\mathbf{A}_K \to k$ with $K \subset \ker D(y)$.

Then for $x \in \mathbf{A}_K$ and $y \in K$ as above we have a pairing $(x, y) \mapsto D(y)(x)$; this should be k bilinear, and in order to make D a derivation, it should satisfy, for $z \in K$:

$$D(yz)(x) = D(z)(xy) + D(y)(xz)$$

Classical Case $k = \mathbf{C}$

For $x \in \mathbf{A}_K$, write $x = (x_P)_{P \in C}$, where $x_P \in K_P$. Then we use

$$D(y)(x) = \sum_{P \in C} \mathrm{res}_P(x_P dy)$$

where $\mathrm{res}_P(x_P dy)$ can be defined using integration or as follows: $K_P \cong k((t))$, so we can write $x_P = \sum_i a_i t^i$, and since $y \in K \subset K_P$, we can also write $y = \sum_j b_j t^j$. Let $dy = \sum_j j b_j t^{j-1}$, and we define

$$\mathrm{res}_P(x_P dy) = \text{ the coefficient of } t^{-1} \text{ in } x_P dy = \sum_{i+j=0} j a_i b_j$$

Then for $D(y)$ to be a Weil differential, for $x \in K$ we want $D(y)(x) = 0$. This is tantamount to the residue theorem: the sum of the residues of a global differential is 0.

Classical Case $k \neq \mathbf{C}$

To generalize to $k \neq \mathbf{C}$, we can try to use the algebraic formula above to define $\mathrm{res}_P(x_P dy)$. Two problems may arise:

(1) The isomorphism $K_P \cong k((t))$ may fail; but it will hold if we assume $k = \bar{k}$, so we can first establish the result for $\bar{k}$. Then for $k \neq \bar{k}$ we can use Galois theory if $\bar{k} \supset k$ is Galois (for example, when k is perfect).

(2) We need to show that $\sum_{i+j=0} j a_i b_j$ is independent of the choice of isomorphism $K_p \cong k((t))$. It is true if $\mathrm{char} k = 0$ by integration. As the desired statement is a formal identity is some large polynomial ring over $\mathbf{Z}$, then it is true formally.

(3) Lastly, we need to prove the residue theorem. We verify it for $K = k(t)$ and then show that it holds for finite separable extensions of $k(t)$.

Tate's Approach

Some preliminary linear algebra: Let V be a vector space over k; the concepts here are interesting only when $\dim_k V = \infty$. Then $f \in \mathrm{End}(V)$ is "finite-potent" if there exists $n \in \mathbf{Z}$, $n \geq 0$ such that $\dim_k f^n V < \infty$. For a finite-potent map f, we can define $\mathrm{Tr}\, f = \mathrm{Tr}(f|_{f^n V})$ for any n with $\dim_k f^n V < \infty$. This definition is independent of the choice of n, as for $n_2 > n_1$ with $\dim_k f^{n_1} V < \infty$, $f|_{f^{n_1} V}$ maps $f^{n_2} V$ to itself and is nilpotent on $f^{n_1} V / f^{n_2} V$.

Formal Properties of Tate's Tr

(1) If $\{0\} \subset W \subset V$ and $f(W) \subset W$, then $f|_V$ is finite-potent $\iff$ $f|_W$ and $f|_{V/W}$ are finite-potent. In this case, $\mathrm{Tr}_V\, f = \mathrm{Tr}_W\, f|_W + \mathrm{Tr}_{V/W}\, f|_{V/W}$.

(2) If $f : V \to W$ and $g : W \to V$, then gf is finite-potent on V $\iff$ fg is finite-potent on W. In this case, $\mathrm{Tr}_V(gf) = \mathrm{Tr}_W(fg)$.

(3) For f, $g \in \mathrm{End}(V)$, it is not true that f and g finite-potent implies $f+g$ is finite-potent. So suppose that f, g, and $f+g$ are all finite-potent. Is it true that $\mathrm{Tr}(f+g) = \mathrm{Tr}\, f + \mathrm{Tr}\, g$? Any finite-potent map can be decomposed as the sum of a nilpotent map and a map with finite-dimensional image. Then Tate shows it is true if the subvector space of $\mathrm{End}(V)$ spanned by f and g can be simultaneously decomposed.

If there is a counterexample, then there is a counterexample with f and g nilpotent, by the above decomposition, so we need only consider nilpotent maps. Furthermore, if $f^2V = g^2V = 0$, then it is true that $\mathrm{Tr}(f+g) = \mathrm{Tr}\, f + \mathrm{Tr}\, g = 0$.

(For f nilpotent, let the order of f be the least n such that $f^n = 0$. After the date of this lecture, Professor Bergmann did find a counterexample, where f, g, and $f+g$ each had order 3. He conjectures that any counterexample will have $(\mathrm{ord}\, f)^{-1} + (\mathrm{ord}\, g)^{-1} + (\mathrm{ord}\, f+g)^{-1} \leq 1$.)

Uses of Tate's Tr

We consider $V = K_P$. $K_P \supset \hat{O}_P$ with $\hat{O}_P$ a k-linear subspace. So choose $\pi : K_P \to \hat{O}_P$ a k-linear projection. Define $f = f_{x,y} \in \mathrm{End}(V)$ by $f(v) = \pi(xyv) - y\pi(xv)$ for $v \in V$. f is finite-potent as $\dim_k f^2V < \infty$: $fV \subset \hat{O}_p + y\hat{O}_p = \hat{m}_P^a$ for some a. $\ker f \supset (\hat{O}_p : xy) \cap (\hat{O}_p : x) \supset \hat{m}_P^b$ for some b. If $b \geq a$, then $f^2 = 0$ as $fV \subset \ker f$. Otherwise, f descends to a surjective map $\hat{m}_P^a / \hat{m}_P^b \to f^2V$, and $\dim_k \hat{m}_P^a / \hat{m}_P^b = \deg P(a-b) < \infty$.

Two exercises on f

(1) $\mathrm{Tr}\, f_{x,y}$ is independent of the choice of π. Use Property (2) of Tr and the fact that $\pi_1 - \pi_2$ is nilpotent, hence finite-potent.

(2) If $\hat{O}_P = k[[t]]$, then $K_P = k((t))$. For $x = \sum_i a_i t^i$, $y = \sum_j b_j t^j$, then $\mathrm{Tr}\, f_{x,y} = \sum_{i+j=0} j a_i b_j$. Use $\pi(\sum_i c_i t^i) = \sum_{i \geq 0} c_i t_i$.

Local Inner Product

Now we can define a local inner product $\langle x, y \rangle_P = \mathrm{Tr}\, f_{x,y}$; by the exercises, $\langle x, y \rangle_P$ is well defined and agrees with $\mathrm{res}_P(x_P dy)$ in the classical case.

Next time we will put the the local inner products together to define D, and give an overview of Tate's proof of the theorem.

Lecture 29 (November 3, 1995).
Scribe: Wayne Whitney

So last time we were about to get to Tate's proof of the theorem relating $\Omega_{K/k}$ with $\mathrm{Diff}_{K/k}$, using the trace of finitepotent maps Tate defined. As usual, let $K \supset k$ be the function field of a curve over k, that is $K \supset k$ is finitely generated and has transcendence degree 1. We also require today that $K \supset k$ is separably generated.

Overview of the Proof

Let $P \in C$, P a closed point. Then $\hat{O}_p \subset K_p$ and is a k-linear subspace of K_p. We make a choice π: $K_p \to \hat{O}_p$ which is a k-linear projection. Then for x, $y \in K_p$, define $f_{x,y} : K_p \to K_p$ by $f_{x,y}(v) = \pi(xyv) - y\pi(xv)$ for $v \in K_p$. We saw that $f_{x,y}$ was finite-potent, and $\mathrm{Tr}\, f_{x,y}$ was independent of the choice of π, so we could define $\langle x, y\rangle_P = \mathrm{Tr}\, f_{x,y}$.

Now one needs to check that $\langle \cdot, \cdot\rangle_P : K_p \times K_p \to K_p$ is k-bilinear, and that one has $\langle x, yz\rangle_P = \langle xy, z\rangle_P + \langle xz, y\rangle_P$. Then we can define a derivation $D : K \to \mathrm{Diff}_{K/k}$ by: for $y \in K$ and $x = (x_P) \in \mathbf{A}_K$,

$$D(y)(x) = \sum_{P\in C} \langle x_P, y\rangle_P$$

The sum above is a finite sum: if $x, y \in \hat{O}_P$, then $f(K_P) \subset \hat{O}_P$ and $f(\hat{O}_P) = 0$, so $f^2 = 0$ and $\mathrm{Tr}\, f = 0$. Thus for all but finitely many P, $\langle x_P, y\rangle_P = 0$.

Now one needs to check that $D(y) : \mathbf{A}_K \to k$ is continous, and that the residue theorem holds, so that $K \subset \ker D$. These details may be found in Tate's paper.

Then D is k-linear, once you realize that the k-vector space structure on $\mathrm{Diff}_{K/k}$ is given by $z\lambda(x) = \lambda(zx)$ for $\lambda \in \mathrm{Diff}_{K/k}$, $x \in \mathbf{A}_K$ and $z \in k$. Also, $D(yz) = yD(z) + zD(y)$.

Thus D is k-derivation of K. So D gives rise to a K-linear map $c : \Omega_{K/k} \to \mathrm{Diff}_{K/k}$, such that $D = cd$, where $d : K \to \Omega_{K/k}$ is the natural map. c is the map desired for Tate's theorem.

Extensions of Function Fields of Curves

We now move to a new topic. Consider a function field of a curve over k, $K \supset k$, and a finite extension $L \supset K$. Then L itself is a function field of a curve. The inclusion $K \subset L$ corresponds to a dominant (non-constant in this case) morphism $C_L \to C_K$.

Note that if k is the exact field of constants of K, that is $K \cap \bar{k} = k$, it may not be the case that k is the exact field of constants of L. That is to say, we will have to consider the situation $L \cap \bar{k} \neq k$. So previous results which assumed $K \cap \bar{k} = k$ may need to be reformulated.

So for any function field of a curve $K \supset k$, set $k_0 = K \cap \bar{k}$, the exact field of constants of K. Then $k_o \supset k$, and $[k_0 : k] < \infty$.

Now consider the statement of Riemann-Roch. All dimensions involved are properly over k_0. But if we multiply through by $[k_0 : k]$, all dimensions will be over k. This will have the effect of changing the 1 in Riemann-Roch to $[k_0 : k]$.

With these preliminaries, we can again consider an extension of functions fields $L \supset K \supset k$. Ultimately we will prove the Hurwitz formula, also known as the Riemann-Hurwitz formula or the Hurwitz-Zeuthen formula. This formula links g_L, the genus of L, to g_K. The proof of this formula will come from a consideration of the map D from the previous section, now indexed by the field in question. We will show that:

$$D_L(y)(x) = D_K(y)(\mathrm{Tr}_{\mathbf{A}_L/\mathbf{A}_K}\, x)$$

where $y \in K$ and $x \in \mathbf{A}_L$. Of course, to do this, we will need to define the trace $\mathrm{Tr}_{\mathbf{A}_L/\mathbf{A}_K}$.

A Basis-Free Definition of Tr

Let A be a ring, and let B be an A-algebra which is a finite, free A-module (or locally free). Then we will construct a map $\mathrm{Tr}_{B/A} : B \to A$ which is given by $\mathrm{Tr}_{B/A}(b) =$ the trace of the the A-linear map $B \to B$ given by $x \mapsto bx$.

So we have the natural map $B \to \mathrm{Hom}_A(B, B)$ given by $b \mapsto (x \mapsto bx)$. Now for any two A-modules C and D, there is a natural map $\mathrm{Hom}_A(D, A) \otimes_A C \to \mathrm{Hom}_A(D, C)$ given by $f \otimes c \mapsto (d \mapsto f(d)c)$. When $C = A$, this map is evidently an isomorphism, and the map respects $\oplus$, so it is an isomorphism when $B \cong A^n$ (or if B is a direct summand of a finite free module, that is a finite projective module, equivalently a finite locally free module).

Thus we have shown $\mathrm{Hom}_A(B, B) \cong \mathrm{Hom}_A(B, A) \otimes_A B$. Evidently, we have a natural map $\mathrm{Hom}_A(B, A) \otimes_A B \to A$: just $f \otimes b \mapsto f(b)$. Composing the isomorphism with this map, we get $Tr_{B/A} : B \to A$.

Back to the Adeles

So to define $\mathrm{Tr}_{\mathbf{A}_L/\mathbf{A}_K}$, it suffices to show that $\mathbf{A}_L$ is a finite free $\mathbf{A}_K$ module. To that end:

Theorem If $L \supset K \supset k$ with $L \supset K$ finite and $K \supset k$ finitely generated of transcendence degree 1, then the natural map $L \otimes_K \mathbf{A}_K \to \mathbf{A}_L$ is an isomorphism.

Proof First we do have a natural map: $L \subset \mathbf{A}_L$ in a natural way, and as $K_P \subset L_Q$ for every $Q \mapsto P$, we have a map $\mathbf{A}_K \to \mathbf{A}_L$ given by $(x_P) \mapsto (y_Q)$ where if $Q \mapsto P$, then $y_Q = x_P$. Hence we have a natural map $L \otimes_K \mathbf{A}_K \to \mathbf{A}_L$.

Next times we will give a "funny" proof using divisors that this map is an isomorphism.

Lecture 30 (November 6, 1995).
Scribe: Nick Meyer

As always, let $k \subset K$ be a finitely generated field extension of transcendence degree 1. Let $K \subset L$ be a finite field extension.

Then the inclusion $K \to L$ induces the map $C_L \to C_K$. For point $Q \in C_L$ mapping to point $P \in C_K$, we have $\mathcal{O}_p = \mathcal{O}_q \cap K$. We recall that $e(Q/P) = [L^* : \hat{\mathcal{O}}_q^{\,*} \cdot K^*]$ and $f(Q/P) = [k(Q) : k(P)]$, and note that $\hat{\mathcal{O}}_q$ is a module over $\hat{\mathcal{O}}_p$ free of rank $e \cdot f = [L_Q : K_P]$, where L_Q is the completion of L with respect to Q. We see that if we fix P, then

$$\sum_{Q\to P} e(Q/P)f(Q/P) = [L:K].$$

Finally, we note that

$$L\otimes_K K_P \leftrightarrow \prod_{Q\to P} L_Q$$

defines an isomorphism of K_P-algebras.

We now proceed with a theorem.

Theorem: The natural map $L\otimes_K \mathbf{A_K} \to \mathbf{A_L}$ is an isomorphism of $\mathbf{A_K}$-algebras. I.e.: if L is given a basis - $L=\sum_{i=1}^{[L:K]} K\cdot\omega_i$ - then the ω_i, viewed as elements of $\mathbf{A_L}$, form an $\mathbf{A_K}$ basis for $\mathbf{A_L}$. (Note: the ω_i form a K_P basis for $\prod_{Q\to P} L_Q$, where L_Q is defined as above).

Proof: It suffices to prove that for almost all P, the ω_i form a basis of $\prod_{Q\to P}\hat{\mathcal{O}}_q$ over $\hat{\mathcal{O}}_p$, since

$$L\otimes_K \mathbf{A_K} \cong \oplus_{i=1}^{[L:K]}\mathbf{A_K}\cdot\omega_i = \prod_P{}' \oplus_i K_P\cdot\omega_i,$$

(where the restricted product is taken with respect to $\oplus_i\hat{\mathcal{O}}_p\cdot\omega_i$), and

$$\mathbf{A_L} = \prod_P{}' \prod_{Q\to P} L_Q,$$

(where the restricted product is taken with respect to $\prod_{Q\to P}\hat{\mathcal{O}}_q$). So we get an isomorphism $f_P:\oplus K_P\cdot\omega_i\to\prod_{Q\to P} L_Q$.

Now all we need to do is show that if $y\in\prod_{Q\to P}\hat{\mathcal{O}}_q$, $y=\sum_i\chi_i\omega_i, (\chi_i\in K_P, P\notin$ some finite set depending only on the ω_i), then $\chi_i\in\hat{\mathcal{O}}_p$. (I.e., the χ_i are "integral").

To show this, we do something unnatural and strange. First, we view y as an element of $\mathbf{A_L}$ and x as an element of $\mathbf{A_K}$, supplementing with zeros as necessary. First, we find divisor $A=\sum_{P'} a_{P'}P'$ of K such that $K+\mathbf{a}=\mathbf{A_K}$, where $\mathbf{a}=\prod_{P'}\hat{\mathfrak{m}_{P'}}^{a_{P'}}$; now, we find divisor $B=\sum_{Q'} b_{Q'}Q'$ of L (we will assume, WLOG, that the $b_{Q'}\ge 0$), such that $\sum_i \mathbf{a}\cdot\omega_i\subseteq\mathbf{b}$, where $\mathbf{b}=\prod_{Q'}\hat{\mathfrak{m}_{Q'}}^{b_{Q'}}$; finally, we find $C=\sum_{P'} c_{P'}P'$ of K such that $K+\mathbf{a}=\mathbf{A_K}$, where $L\cap\mathbf{b}$ (which is finite over k, since $l(-B)$ is finite) is contained in $\sum_i \mathbf{c}\omega_i$, where $\mathbf{c}=\prod_{P'}\hat{\mathfrak{m}_{P'}}^{c_{P'}}$.

Claim: We can draw the conclusion we wish, now, if $a_{P'}\ge 0, c_{P'}\ge 0$.

Proof: $y=\sum\chi_i\omega_i\in\mathbf{A_L}.\mathbf{A_K}\ni\chi_i=k_i+a_i$, where $k_i\in K, a_i\in \dashv$. Now $y=l+b$, where $l=\sum k_i\cdot\omega_i\in L$, $b=\sum a_i\cdot\omega_i\in\mathbf{b}$. So $y\in\mathbf{b}$, since y has everywhere integral coordinates; thus $l\in\mathbf{b}\subset L\cap\mathbf{b}$. This yields, finally, that $k_i\in\mathbf{c}$, which was what we required. The proof is complete. (Note: when we completed fields first before taking the product in our definition of the adele ring, it was with this proof in mind).

On to another topic! Let λ be a Weil differential of K; i.e., $\lambda : \mathbf{A_K} \to k$, with λ k-linear, continuous, surjective, and 0 on K. Then we associate to λ the **canonical divisor** W_λ. We have that $\deg W_\lambda = 2g_K - 2[K \cap \bar{k} : k]$.

Let's look at the dual space $\mathrm{Hom}_K(L, K)$. This is a vector space over K with dimension $[L : K]$. It's also an L-vector space; for $c \in L$, $f \in \mathrm{Hom}$, we define $cf(x)$ to be equal to $f(cx)$. Now $\dim_L \mathrm{Hom}_K(L, K) = 1$. And this is wonderful!

Lecture 31 (November 8, 1995).
Scribe: Nick Meyer

If $K \subset L$ is finite separable, then $\mathrm{Hom}_K(L, K)$ is spanned by $\mathrm{Tr}_{L/K}$.

Back to function fields for the moment. Let k, K, L be as above. Take $\lambda \in \mathrm{Diff}_K - 0$. To each λ is associated a canonical divisor $W_\lambda = \sum_{P \in C_K} n(P) \cdot P$, where P ranges over the closed points of C_K and $n(P) = \max n \in \mathbf{Z} \mid \lambda = 0$ on $\mathfrak{m}_P^{-n} \subset \mathbf{A_K}$. Now $\deg W_\lambda = 2g_K - 2[K \cap \bar{k} : k] = \sum n(P) \deg P$.

Now let's get back to proving the Hurwitz Formula. Our strategy: take a $\lambda \in \mathrm{Diff}_K$, use it to concoct a $\mu \in \mathrm{Diff}_L$, and use it to calculate g_L.

To this end, choose $t : L \to K$. It's a surjective K-linear map (i.e., t is unique up to L^*). Write $t' = t \otimes 1 : \mathbf{A_L} \cong L \otimes_K \mathbf{A_K} \to \mathbf{A_K}$. Several things here should be noted: first, surjectivity is guaranteed since $\otimes$ is right-exact); second, t' is $\mathbf{A_K}$-linear. Finally, the isomorphism between $\mathbf{A_L}$ and $L \otimes_K \mathbf{A_K}$ is a topological isomorphism as well - ${\mathbf{A_K}}^n \cong \oplus_{i=1}^n \omega_i \otimes \mathbf{A_K}$.

Now let $\mu = \lambda \circ t' : \mathbf{A_L} \to k$.

Claim: $\mu \in \mathrm{Diff}_L$.

Proof: Continuity follows form the topological isomorphism above; μ is k-linear by composition; $\mu(L) = 0$ since $t'(L) = K$. So we're done.

Basic Fact: Write $\mathbf{D}_t = \sum_{Q \in C_L} m(Q) \cdot Q$, where Q ranges over the closed points of C_L, $m(Q) = \max n \in \mathbf{Z} \mid t'(\hat{\mathfrak{m}}_Q^{-n}) \subset \hat{\mathcal{O}}_p$ ($\mathcal{O}_p = K \cap \mathcal{O}_q$). Then:

i) This is a divisor of L.

ii) $\mathbf{D}_{f \cdot t} = \mathbf{D}_t + (f)$, where $f \in L^*$.

iii) $W_\mu = i(W_\lambda) + \mathbf{D}_t$, where i is the group homomorphism $i : \mathrm{Div}_K \to \mathrm{Div}_L$ taking $P \to \sum_{Q \to P} e(Q/P) Q$.

(Remark: This part of the theorem is analogous to a result from algebraic number theory. If $K \subset L \subset M$, $\mathbf{D}_{M/K} = \mathbf{D}_{M/L} \cdot \mathbf{D}_{L/K}$. The two on the right-hand side don't sit in the same ring - we let $i(\mathbf{D}_{L/K}) = \mathbf{D}_{L/K} \cdot \mathcal{O}_M$).

iv) $2g_L - 2[L \cap \bar{k} : k] = (2g_K - 2[K \cap \bar{k} : k])[L : K] + \deg \mathbf{D}_t$.

Proof: t' takes $\mathbf{A_L} = \prod'_P \prod_{Q\to P} L_Q \to \mathbf{A_K} = \prod' K_P$. So t' is really made up of maps $t_Q : L_Q \to K_P$, where each t_Q is K_P-linear.

Now, we prove (i) and (iii): Let $r \in \mathbf{Z}$.

$$\begin{aligned} r \leq \mathrm{ord}_Q W_\mu &\leftrightarrow \mu(\hat{\mathfrak{m}}_Q^{-r}) = 0 \\ &\leftrightarrow \lambda(t_Q(\hat{\mathfrak{m}}_Q^{-r})) = 0 \\ &\leftrightarrow t_Q(\hat{\mathfrak{m}}_Q^{-r}) \subseteq \hat{\mathfrak{m}}_P^{-\mathrm{ord}_P W_\lambda} \\ &\leftrightarrow t_Q(\hat{\mathfrak{m}}_P^{-\mathrm{ord}_P W_\lambda}) \subseteq \hat{\mathcal{O}}_p \\ &\leftrightarrow -e(Q/P)\mathrm{ord}_P W_\lambda + r \leq \mathrm{ord}_Q \mathbf{D}_t \text{ (since } \hat{\mathfrak{m}}_P \cdot \hat{\mathcal{O}}_q = \hat{\mathfrak{m}}_Q^{e(Q/P)} \text{ by def).} \\ &\leftrightarrow r \leq \mathrm{ord}_Q \mathbf{D}_t + e(Q/P) \cdot \mathrm{ord}_P W_\lambda \end{aligned}$$

Therefore, for each Q, $\mathrm{ord}_Q W_\mu = \mathrm{ord}_Q \mathbf{D}_t + e(Q/P) \cdot \mathrm{ord}_P W_\lambda$. Thus $\mathbf{D}_t = W_\mu - i(W_\lambda)$ is a divisor. So we've proven (i) and (iii). (ii) is left as an exercise for the reader.

To get (iv), we take degrees on both sides of (iii); it suffices to verify that $[L : K] \deg = \deg \circ i$ as maps from $\mathrm{Div}_K \to \mathbf{Z}$. Well,

$$\begin{aligned} \deg(i(P)) &= \sum_{Q\to P} e(Q/P) \deg Q \\ &= \sum_{Q\to P} e(Q/P)[k(Q) : k] \\ &= \sum_{Q\to P} e(Q/P)[k(Q) : k(P)][k(P) : k] \\ &= \sum_{Q\to P} e(Q/P) f(Q/P) \deg(P) \\ &= \deg(P)[L : K] \end{aligned}$$

Lecture 32 (November 10, 1995).
Scribe: Matt Baker

Here is a slightly more general setup to consider [think of it as a modification of our previous assumptions].

Let $k \subset K$, with K a finitely generated extension of k of transcendence degree 1, as before. Let l and L be finite extensions of k and K, respectively.

Then the formula from last time:

$$2g_L - 2[L \cap \overline{k} : k] = (2g_K - 2[K \cap \overline{k} : k]) * [L : K] + deg(\mathcal{D}_t),$$

where $t : L \to K$ is a K-linear map, can be souped-up to our new setup in an obvious way to yield the following formula:

$$2g_{L/l} - 2[L \cap \bar{l} : l] = (2g_{K/k} - 2[K \cap \bar{k} : k]) * [L : K] + deg_l(\mathcal{D}_t) * [l : k].$$

The Riemann-Hurwitz formula will essentially be a translation of this formula into more familiar language in the separable case. When k is perfect, we have the following result.

Theorem: Suppose k is perfect, and let $L_{sep} = \{x \in L : x \text{ is separable over } K\}$. Then $g_{L/k} = g_{L_{sep}/k}$.

Proof: General field theory tells us that $L^q \subset L_{sep}$, where $q = [L : L_{sep}]$. A degree calculation similar to a previous calculation done in class shows that $L_{sep} = L^q$. Thus we have $g_{L/k} = g_{L^q/k^q} = g_{L^q/k} = g_{L_{sep}/k}$.

Assume now that $L \supset K$ is **separable** and take $t := Tr_{L/K}$.

Remark: Separability is equivalent to the trace being nonzero by basic field theory.

Recall that $\mathcal{D}_t = \sum m(Q) \cdot Q$, where the sum is taken over the closed points Q of C_L, and where $m(Q)$ is defined as the largest $n \in \mathbf{Z}$ such that $t_Q(\mathfrak{m}_Q^{-n}) \subset \widehat{O_P}$. Here P is the point in C_K lying under Q, and t_Q is the (nonzero) trace map from L_Q to K_P.

We have a couple of useful formulas for traces, which can be verified without too much suffering:

1. If $B' = B \bigotimes_A A'$, then $Tr_{B'/A'} = Tr_{B/A} \bigotimes id_{A'}$.
2. If $B = B_1 \bigoplus B_2$, then $Tr_{B/A} = Tr_{B_1/A} + Tr_{B_2/A}$.

Also, recall that $t' : \mathbf{A}_L \to \mathbf{A}_K$ defined by $t' = t \bigotimes id_{\mathbf{A}_K}$ was built up from the maps $t_Q : L_Q \to K_P$. It follows from formula 1 that $t' = Tr_{\mathbf{A}_L/\mathbf{A}_K}$.

Prop: If Q lies over P then $L \supset K$ is inseparable iff $L_Q \supset K_P$ is inseparable.

Proof: Suppose $L \supset K$ is inseparable. Then $Tr_(L/K)$=0, so $Tr_(L_Q/K_P) = 0$. Conversely, if $L \supset K$ is separable, then $L_Q = L \cdot K_P \supset K_P$ is separable by field theory. In particular, $t_Q = Tr_(L_Q/K_P) \neq 0$.

We will now make some remarks that apply more generally, for example to the situation of algebraic number theory. So let A be a complete DVR [in our case, $\widehat{O_P}$] with field of fractions E [which for us is K_P], let $F \supset E$ be a finite separable extension [$=L_Q$ in disguise], and let B [i.e. $\widehat{O_Q}$] be the unique valuation ring of F lying over A.

Let $e = e(B/A), f = f(B/A)$, and define $m[= m(B/A)]$ to be the largest n such that $Tr_{F/E}(\mathfrak{m}_B^{-n}) \subset A$. This m is called the 'differential exponent'. Note that $m \geq 0$, since $Tr(B) \subset A$. Our old quantity $deg_l(\mathcal{D}_t)$ is just $\sum_Q m(Q/P) \cdot deg_l Q$.

Remark: In number theory, $\mathcal{D}_{B/A} = \mathfrak{m}_B^{m(B/A)}$ is called the 'different'; it is an ideal of B. Similarly, the quantity $\Delta_{B/A} = \mathfrak{m}_A^{m(B/A)\cdot f(B/A)}$ is called the 'discriminant'; it is an ideal of A.

Def: B is called **unramified** over A if $e(B/A) = 1$ and $A/\mathfrak{m}_A \subset B/\mathfrak{m}_B$ is separable.

We have $[F : E] = e(B/A) \cdot f(B/A) = e(B/A) \cdot f_{\text{ins}}(B/A) \cdot f_{\text{sep}}(B/A)$, and B/A is unramified iff $e(B/A) \cdot f_{\text{ins}}(B/A) = 1$. We say that B/A is **ramified** if it is not unramified.

Next time, we will prove the following theorem.

Theorem: $m(B/A) = 0 \Leftrightarrow B \supset A$ is unramified. More generally, we have $m(B/A) \geq e(B/A) - 1$, with equality iff B over A is **tamely ramified**, i.e. $\text{char}(A/\mathfrak{m}_A)$ does not divide $e \cdot f_{\text{insep}}$.

Lecture 33 (November 13, 1995). Scribe: Diane Maclagan

Let A be a complete discrete valuation ring, and E its field of fractions. Let F be a finite separable extension of E. From earlier this semester we know that there is exactly one valuation ring, B, of F lying over A. Now

$$[F : E] = e(B/A)f(B/A)$$

We are interested in

$$m(B/A) = \max\{n \in \mathbf{Z} \text{ s.t. } \text{Tr}(\mathbf{m}_B^{-n}) \subseteq A\}$$

Last time we defined the different, $\mathcal{D}_{B/A} = \mathbf{m}_B^{m(B/A)}$, which is analogous to the different from Algebraic Number Theory.

In Number Theory we have the situation where $L \subseteq K$ is a finite extension of number fields, and B and A are their respective rings of integers. If E is a fractional B ideal, we define $E^{'} = \{x \in L s.t. \text{Tr}(xE) \subseteq A\}$. The classical definition of the different is that $\mathcal{D}_{B/A} = B^{'}$. We can write $\mathcal{D}_{B/A} = B^{'}$ as

$$\prod_{\mathbf{q}} \mathbf{q}^{m(\hat{B}_q/\hat{A}_p)}$$

We say B is unramified over A if $e(B/A)f_{\text{ins}}(B/A) = 1$ where f_{ins} is defined as follows: given any field extension $l \subseteq k$, we define l_{sep} to be the elements of l separable over k. Now $f(B/A) = [l : k]$ where $l = B/\mathbf{m}_B$ and $k = A/\mathbf{m}_A$. $f_{\text{ins}}(B/A) = [l : l_{\text{sep}}]$.

B is said to be ramified if it is not unramified, and B is tamely ramified over A if $\mathrm{char}(A/\mathbf{m}_A)$ does not divide $e(B/A)f_{\mathrm{ins}}(B/A)$. If the residue characteristic is zero, all extensions are tamely ramified. The opposite of tamely ramified is wildly ramified.

For more details on this, and on compositums of of (un)ramified extensions, see Lang

We thus break up field extensions as follows:

$$E \subseteq F_{ur} \subseteq F_{tr} \subseteq F$$

where F_{ur} is the unramified piece, and F_{tr} is the tamely ramified piece.

It is important to distinguish between the characteristic of the residue class and that of the field extension.

Theorem:
$m(B/A) = 0 \Leftrightarrow B$ is unramified over A
$m(B/A) \geq e(B/A) - 1$
$m(B/A) = e(B/A) \Leftrightarrow B$ is tamely ramified over A.
Proof:

Tensor $\mathrm{Tr}_{B/A} : B \to A$ with $A/\mathbf{m}_A$ over A. We get

$$\mathrm{Tr}_{B/A} \otimes id = \mathrm{Tr}_{\overline{B}/\overline{A}} : \overline{B} \to \overline{A}$$

where $\overline{B} = B/\mathbf{m}_B$ and $\overline{A} = A/\mathbf{m}_A$. Now $\mathbf{m}_B^{e(B/A)} = \mathbf{m}_A B$, so $x \in \mathbf{m}_B$ means $\overline{x} \in \overline{B}$ is nilpotent.

$$\mathrm{Tr}_{B/A}(\mathbf{m}_B) = \overline{0} \in \overline{A}$$

$$\mathrm{Tr}_{B/A}(\mathbf{m}_B) \subseteq \mathbf{m}_A$$

$$\mathbf{m}_A^{-1}\mathrm{Tr}_{B/A}(\mathbf{m}_B) \subseteq A$$

$$\mathrm{Tr}_{B/A}(\mathbf{m}_A^{-1}\mathbf{m}_B) \subseteq A$$

$$\mathrm{Tr}_{B/A}(\mathbf{m}_B^{-e(B/A)+1}) \subseteq A$$

So $m(B/A) \geq e(B/A) - 1$

We now consider when equality is reached. If this is not the case, then

$$m(B/A) \geq e(B/A)$$

$$\Leftrightarrow \mathrm{Tr}_{B/A}(\mathbf{m}_B^{-e(B/A)}) \subseteq A$$

$$\Leftrightarrow \mathrm{Tr}_{B/A}(B) \subseteq \mathbf{m}_A$$

$$\Leftrightarrow \mathrm{Tr}_{\overline{B}/\overline{A}} = 0$$

$$\Leftrightarrow p | e(B/A) \text{ or } \mathrm{Tr}_{\overline{B}/\overline{A}} = 0$$

$\Leftrightarrow B/A$ is tamely ramified.

The formula for $m(B/A)$ in the wild case depends on higher ramification. The reference for this material is Serre's *Corps Locaux*, which is available in translation.

We make the assumption that $A/\mathbf{m}_A$ is perfect. This assumption is also made by Serre.

Finite separable extensions F of E correspond to finite sets S together with a continuous transitive $G-$action on$S$. (Recall 21st century Galois Theory earlier in the semester).

For $\sigma \in G$, $\sigma \neq id$ let $j(\sigma)$ be the largest j for which σ induces the identity on $A'/\mathbf{m}_{A'}^j$ where A' is the ring sitting above A in E. Then

$$m(B/A)f(B/A) = \sum_{\sigma \in G, \sigma \neq id} +(\#S - \#s^\sigma)\frac{j(\sigma)}{e(A'/A)}$$

Plugging this into the Riemann-Huriwitz formula, we get:

$$2g_{L/l} - 2[L \cap \overline{l} : l] = (2g_{K/k} - 2[K \cap \overline{k} : k])\frac{[L : K]}{[l : k]} + \sum_{\text{ramified} Q \in C} (\deg_l Q) m(Q/P)$$

Often this formula can be simplified a lot - for example, it is often the case that $[L \cap \overline{l} : l] = [K \cap \overline{k} : k] = 1$. This happens in particular when $\overline{k} = k$. We then have $[l : k] = 1$, however there are interesting cases where this is not the case. If it is tamely ramified, we can replace $m(Q/P)$ by $e(Q/P) - 1$.

Lecture 34 (November 15, 1995).
Scribe: Diane Maclagan

Reference for today: Artin, *Algebraic Numbers and Algebraic Functions*. Artin also considers things in slightly more generality. We will only cover the important results, rather than giving a general survey of the field.

We consider the situation:

$$\begin{array}{ccc} l & \subset & L \\ \cup & & \cup \\ k & \subset & K \end{array}$$

where $[L : lk]$ is finite. Artin does not require this assumption.

We say that we have a "constant field extension" if $L = lk$.

Theorem. *Let $k \subset K$ be a finitely generated field extension of transcendence degree 1 and let $l \supset k$ be a finite separable extension for which $L = l \otimes_k K$ is a field (e.g. if $\overline{k} \cap K = k$). Then $g_{L/l} = g_{K/k}$.*

Proof:

$$(2g_{L/l} - 2[\overline{l} \cap L : l] = (2g_{K/k} - 2[\overline{k} \cap K : k])\frac{[L : K]}{[l : k]} + \sum_{Q \mapsto P} m(Q/P) \deg_l Q.$$

Now $[\overline{l} \cap L : l] = [\overline{k} \cap K : k]$ (exercise). So we need to show $\sum_{Q \mapsto P} m(Q/P) \deg_l Q = 0$. We know it is non-negative, so $g_{L/l} \geq g_{K/k}$. We show genus can't go up.

$$\begin{aligned} g &= \dim_k \mathbf{A}_k/(K + \hat{\mathcal{O}}) \\ &= \dim_l l \otimes (\mathbf{A}_k/K + \hat{\mathcal{O}}) \\ &= \dim_l((l \otimes_k \mathbf{A}_k)/(\underbrace{l \otimes_k K}_{L} + l \otimes_k \hat{\theta})) \\ &= \dim_l \mathbf{A}_L/(L + (\text{ some subspace of } \hat{\mathcal{O}} \text{ for } L)) \\ &\geq g_{L/l} \end{aligned}$$

where the last two lines follow because

$$l \otimes_k \hat{\mathcal{O}} \subseteq l \otimes_k \mathbf{A}_k = l \otimes_k K \otimes_k A_k = L \otimes \mathbf{A}_k = \mathbf{A}_L$$

$$\text{image}(l \otimes \hat{\mathcal{O}} \text{ in } \mathbf{A}_L) \subseteq (\hat{\mathcal{O}} \text{ for } L).$$

Consider the following situation:
$L = lk$, $\overline{k} \cap K = k$, $\overline{l} \cap L = l$.
Then:
$g_{L/l} \leq g_{K/k} \equiv g_{L/l} mod (p-1)/2$ (Tate 1952)
$g_{L/l} = g_{K/k}$ if k is perfect (see Artin).
$K \supset k$ is called conservative if we have equality for all $L \supset l$.
Exercise: K is conservative iff $g_{K/k} = 0$ or C_K is nonsingular.
Recall from last time $m(Q/P) = e(Q/P) - 1$ (tamely ramified).
If $\mathcal{G}_P$ is the Galois group of K_P^{sep} over K_P, and S is a $\mathcal{G}_K$ set (where $\mathcal{G}_K$ is the absolute Galois group ($Gal(K^{sep}/K)$), then

$$\{Q \text{ over } P\} \longleftrightarrow \{\text{orbits of } S \text{ under } \mathcal{G}_P\}$$

This material can be found in a text on Algebraic Number Theory or Valuation Theory or Serre *Local Fields*.

We have the following situation, where $\mathrm{Tr} : L \mapsto K$

$$\begin{array}{ccc} L \otimes_K \mathrm{Diff}_{K/k} & \xrightarrow{Tr} & \mathrm{Diff}_{L/l} \\ \cup & (2) & \\ (\mathrm{Diff}_{K/k})_p & & \end{array}$$

From Hartshorne, p.300, we have: (1) $L \otimes_K \Omega_{K/k} \to \Omega_{L/l}$

In Tate's paper he develops maps shown in the following diagram:

$$\begin{array}{ccc} \Omega_{K/k} & \xrightarrow{C} & \mathrm{Diff}_{K/k} \\ \uparrow & & \cup \\ \Omega_{\theta_p}/k & \xrightarrow{C_P} & (\mathrm{Diff}_{K/k})_p \end{array}$$

If $K \supset k$ separably generated then injective iff P is nonsingular. C is an isomorphism iff $K \supset k$ is separably generated. C_P is an isomorphism iff P is nonsingular.
The following are conjectures:

Guess 1. If $K \supset k$ is not separably generated then $c = 0$.

Guess 2. K/k separably generated, then $\dim_k \ker C_P = \dim_k \mathrm{coker} C_P (< \infty)$.

Guess 3. These two guesses follow by comparing maps (1) and (2).

There is thus still research left to do at this level.

Other areas of importance are $k = \mathbf{C}$, and Jacobians. We have

$$0 \to \mathrm{Pic}_k^0 \to \mathrm{Pic}_K \to \mathbf{Z}$$

where Pic_k^0 is a compact abelian group when given a decent topology. We can also make it into an Abelian variety.

A lot of this theory (except Kähler differentials) was developed in the 30's by Hasse, Artin, and Deuring. They were mostly using field theoretic ideas – Weil was the first person to break away and use geometric ideas. He was also the first to prove Riemann hypothesis for curves. More information on this can be found in Cornell-Silverman or any text on Arithmetic Geometry.

Lecture 35 (November 17, 1995).
Scribe: Ezra Miller

For Exercise 22, it might be useful to have the following fact. (Let K/k be as usual: finitely generated of transcendence degree = 1.)

Theorem: Let $P \in C_K$. If deg $P = 1$ then P is non-singular.

Corollary: If there is a point of degree 1, then K/k is separably generated (i.e. the generic point is non-singular).

Question: If deg:$\mathrm{Div}_K \to \mathbf{Z}$ is surjective, does it follow that K/k is separably generated?

§ Zeta Functions over Finite Fields

Notation: k = finite field of order q (i.e. $k = \mathbf{F}_q$)
$k_n = \mathbf{F}_{q^n}$ = degree n extension of k
K = f.g. extension of k of transcendence degree = 1 with $\bar{k} \cap K = k$
$\zeta,\ \zeta_{K/k},\ Z,\ Z_{K/k}$ = zeta functions of K/k
$C_{K/k} = C$ = the usual curve

Lemma: For each $n \geq 0$ there exist only finitely many divisors of degree n.

Proof: It suffices to consider prime divisors, and the case for K follows from the case for $k(t)$, where t is transcendental over k. Now each prime of $k(t)$ of degree n is obtained from an irreducible polynomial of degree n over k (except for the single prime ∞), and the result is now obvious.

Definition: $Z_{K/k} = Z_{K/k}(T) \in Z[[T]] \subset \mathbf{C}((T))$ is defined as

$$\sum_{\substack{D \in \mathrm{Div}_{K/k} \\ D \geq 0}} T^{\deg D} = \sum_{n=0}^{\infty} A_n T^n$$

where

$$A_n = \# \left\{ D \geq 0 \;\middle|\; \deg D = n \right\}$$

and $A_0 = 1$.

Example: $K = k(t)$. If we have

$$D = \sum_P n_P \cdot P = n_\infty \cdot \infty + \sum_{\substack{f \text{ monic} \\ \text{irred.}}} n_f \cdot P_f$$

then we get

$$n = \deg D = n_\infty + \sum_{\substack{f \text{ monic} \\ \text{irred.}}} n_f \cdot \deg f$$

so that

$$\begin{aligned} A_n &= \sum_{i=0}^{n} \# \left\{ \text{monic polynomials in } k[t] \text{ of degree } n-i \right\} \\ &= 1 + q + q^2 + \cdots + q^n. \end{aligned}$$

Thus

$$Z_{k(t)/k} = \sum_{\substack{n \geq 0 \\ 0 \leq i \leq n}} q^i T^n = \sum_{\substack{n \geq 0 \\ i+j=n}} q^i T^i T^j = \left(\sum_i q^i T^i \right) \left(\sum_j T^j \right) = \frac{1}{(1-T)(1-qT)}.$$

Euler Product:

$$Z_{K/k} = \prod_P \left(\sum_{n=0}^{\infty} T^{\,n\cdot \deg(P)} \right) = \prod_P \left(1 - T^{\,\deg(P)} \right)$$

This Euler product is quite analogous to the one for the ζ-function of Number Theory:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}} \right)$$

In the present case, we have

$$\zeta_{K/k}(s) = Z_{K/k}(q^{-s}) = \prod_P \left(\frac{1}{1 - (q^{\,\deg(P)})^{-s}} \right)$$

where $q^{\,\deg(P)} = \# k(P)$ is the size of the residue class field, and in some sense measures the "size" of the point P. In terms of the Number Theory analogy, this "size" compares well with the norm of an ideal (which actually appears in the Dedekind ζ-function of a number field).

We will frequently be interested in the **rational points** on our curves, so we make the following definition.

Definition: $C(k) = \{P \in C_K \mid \deg(P) = 1\}$
$B_n = \# \{P \in C_K \mid P \text{ is closed of degree } \deg(P) = n\}$

Definition: Let l/k be any field extension. Using scheme-theoretic language, we define

$$C(l) = \left\{ \text{scheme homomorphisms} \quad \begin{array}{ccc} \operatorname{Spec} l & \longrightarrow & C \\ & \searrow \quad \swarrow & \\ & \operatorname{Spec} k & \end{array} \right\}$$

in general, and in our case this becomes

$$C(l) = \{(P, \varphi) \mid P \in C \text{ and } \varphi \text{ is a local ring homomorphism over } k \text{ mapping } \mathcal{O}_P \to l\}$$

where a **local ring homomorphism** φ is such that φ is zero on the maximal ideal of $\mathcal{O}_P$ and the following diagram commutes:

$$\begin{array}{ccc} \mathcal{O}_P & \longrightarrow & k(P) = k_{\deg(P)} \\ & \searrow \quad \swarrow & \\ & l & \end{array}$$

Thus,

$$C(k_n) = \{(P, \varphi) \mid P \text{ is a closed point of degree dividing } n \text{ and } \varphi\colon k(P) \hookrightarrow k_n\}.$$

Proposition: $\#C(k) = \#C(k_1) = A_1$
$\#C(k_2) = \#C(k_1) + 2 \cdot \#\{P \mid \deg(P) = 2\}$
$\#C(k_n) = \sum_{r|n} r \cdot B_r$

Proof: Use Galois theory of finite fields to count embeddings.

Alternative Definition: $C(k_n) = \{P \text{ of } k_n \cdot K \mid \deg_{k_n}(P) = 1\}$. (Note that $\deg_{k_n}(P) = 1 \Rightarrow \deg_k(P) = n$.)Using this definition gives (unsurprisingly) the same formulas as above.

Definition: The **logarithmic derivative** $\frac{d\log}{dT}$ is

$$\frac{d\log}{dT} f = \frac{f}{f'}.$$

We make immediate use of this definition:

$$T\frac{d\log}{dT} Z_{K/k}(T) = T \cdot \sum_P \frac{\deg(P) \cdot T^{\deg(P)-1}}{1 - T^{\deg(P)}} = \sum_{r=1}^{\infty} B_r \frac{rT^r}{1-T^r}$$
$$= \sum_{n=1}^{\infty} \left(\sum_{r|n} rB_r \right) T^n = \sum_{n=1}^{\infty} \#C(k_n) T^n$$

Example: $K = k(t),\ C = \mathbf{P}^1_k,\ Z = 1/\big((1-T)(1-qT)\big)$

$$T\frac{d\log}{dT} Z_{K/k}(T) = \frac{T}{1-T} + \frac{qT}{1-qT} = \sum_{n=1}^{\infty} (q^n + 1)T^n$$

where we note that $q^n + 1 = \#\mathbf{P}^1(k_n)$ is the number of points on the projective line over k_n.

Lecture 36 (November 20, 1995).
Scribe: Dylan Thurston

Let $k = \mathbf{F}_q \subset K$ be a field extension of transcendence degree 1 with $\bar{k} \cap K = k$.

Last time we defined the zeta function

$$\begin{aligned} Z_{K/k} &= Z_{K/k}(T) \in \mathbf{Z}[[T]] \\ &= \sum_{D \text{ divisor} \geq 0} T^{\deg D} \\ &= \prod_{\substack{P \in C_k \\ \text{closed}}} \frac{1}{1 - T^{\deg P}}. \end{aligned}$$

We had a relation between the logarithmic derivative of the zeta function and the number of points of K defined over some extension of k, with one hole in the proof to be filled in today.

Consider the following way of writing the zeta function:

$$\begin{aligned}
Z_{K/k} &= \sum_{x\in Pic_{K/k}} \sum_{\substack{D\geq 0\\ [D]=x}} T^{degD} \\
&= \left(\frac{q^{l(x)}-1}{q-1}\right) T^{\deg x}
\end{aligned}$$

We derive the second equality by looking at $\#\{D\geq 0 : [D]=x\}$, which we saw earlier when studying complete linear systems. Pick E any divisor so that $x=[E]$. Then if $[D]=[E], D\geq 0$, we find $D=(f)+E$ for some f and $(f)+E\geq 0 \Leftrightarrow f\in L(E)-\{0\}$. Thus the number of possible D is the number of possible f divided by the number that give the same result, $q-1$:

$$\#\{D\geq 0 : [D]=x\} = \frac{\#L(E)-1}{q-1} = \frac{q^{l(x)}-1}{q-1}.$$

In particular, we now see that Z is a proper power series, as the terms are positive and non-zero for sufficiently large $\deg x$ (??). By the Riemann-Roch theorem, if $\deg x > 2g-2$, then $l(x) = \deg x - g + 1$. Thus if we know $\#\deg^{-1}(m)$ for $m\in \mathbf{Z}$, we will know the asymptotic behaviour. When this is non-zero, it is equal to $\#\ker(\mathrm{Pic}\to\mathbf{Z}) = \#\mathrm{Pic}_0 = h$ and so

$$\#\deg^{-1}(n) = \begin{cases} 0 & \text{if } n\notin \mathrm{im}(\deg) \\ h & \text{if } n\in \mathrm{im}(\deg) = \delta\mathbf{Z} \text{ for some } \delta>0,\ \delta\in\mathbf{Z},\ \delta|2g-2 \end{cases}.$$

(To see that h is finite, consider the coefficient of Z at $T^{2g-2^2\delta} = h\underbrace{\frac{q^{g-1+2\delta}-1}{q-1}}_{>0} \in \mathbf{Z}$. Since we've already shown that this is finite, we see that h is finite.)

We'll soon prove that $\delta=1$ and then all these formulas become much nicer.

We can now work out the sum expression for the zeta function:

$$\begin{aligned}
Z_{K/k}(T) &= \begin{pmatrix}\text{polynomial in } T^\delta \\ \text{of degree} \leq \frac{2g-2}{\delta}\end{pmatrix} + h\sum_{m=\frac{2g-2}{\delta}+1}^{\infty} \frac{q^{\delta-g+1}+1}{q-1}T^{m\delta} \\
&= (\text{polynomial}) + \frac{h}{q-1}\left(\frac{q^{g-1+\delta}T^{2g-2+\delta}}{1-(qT)^\delta} - \frac{T^{2g-2+\delta}}{1-T^\delta}\right).
\end{aligned}$$

In particular, the zeta function is a rational function of T.

Take $n > 0$, and let k_n be an extension of k of degree n. Consider the function field $k_n \cdot K$.

Proposition.

$$Z_{(k_n \cdot K)/k_n}(T^n) = \prod_{\substack{\zeta \in \mathbf{C} \\ \zeta^n = 1}} Z_{K/k}(\zeta T) \qquad (*)$$

(We have $Z_{K/k} \in \mathbf{Q}(t) \subset \mathbf{C}(t)$, so this makes sense.)

It's not surprising that some formula like (*) exists, as the zeta function encodes information about the points lying over various extensions of k, in particular those extensions containing k_n. This formula is a special case of ζ functions splitting up into a product of L functions for an Abelian variety.

In a moment, we'll prove (*) by a local computation using the Euler product, but let's see a consequence first. If $Z_{K/k} = \frac{f(T)}{g(T)}$ with f, g coprime then (as a consequence of our earlier formula) $g = (1-(qT)^\delta)(1-T^\delta)$. Now compare the denominators in (*) when $n = \delta$. First, $Z_{K/k}(\zeta T) = Z_{K/k}(T)$ (since only powers of $T^{n=\delta}$ occur). The precise denominator of the right hand side is

$$(1-(qT)^\delta)^\delta(1-T^\delta)^\delta$$

while the precise denominator of the left hand side is

$$(1-(q^nT^n)^{\delta'})(1-T^{n\delta'})$$

(where δ' is the δ for $k_n \cdot K$). Comparing these two, we see that $\delta = 1$.

Proof of (*). First, let's examine the splitting behaviour of $P \in C_K$ when we pass to $C_{k_n \cdot K}$.

Claim (a). If P has degree d,

$$\#\{Q : Q \text{ lies over } P\} = \gcd(n,d)\}$$

and each such Q has $e(Q/P) = 1$ and $f(Q/P) = \frac{n}{\gcd(n,d)}$.

To find the Q's lying over P, consider

$$K_P \otimes_k k_n \cdot K = k_n \otimes_k K_P \overset{\text{(canonically)}}{\simeq} \prod_Q (k_n \cdot K)_Q.$$

Here $k_n \otimes_k K_P$ is an algebra defined over K_P, the field of fractions of $\hat{\mathcal{O}}_P$, which is a complete d.v.r with residue class field $\hat{\mathcal{O}}_P/\mathfrak{m}_P = k(P) \simeq k_d$.

Claim (b). $\hat{\mathcal{O}}_P \to k_d \to 0$ has a section.

This is true for $d = 1$ and follows in general be Hensel's Lemma. Alternatively, you can use the fact that k_d is finite: for any $\alpha \in k_d$, take $a \in \hat{\mathcal{O}}_P$ so that $a \mapsto \alpha$. Then define

$$\omega(\alpha) = \lim_{n\to\infty} a^{q^{nd}}$$

(so that $\omega(\alpha)^{q^d} = \omega(\alpha)$; this is independent of the choice of a and gives an embedding of k_d in $\hat{\mathcal{O}}_P$.

(This is not true in general: if k is inseperable, you only get a left modulo $\mathfrak{m}^2$ if the point P is singular.) As a result of Claim (b), $\hat{\mathcal{O}}_P \simeq_k k_d[[t]]$ and $K_P \simeq_k k_d((t))$, and Claim (a) is reduced to a computation which is left as the following exercise.

Exercise. Show that

$$k_n \otimes_k k_d = (k_{\operatorname{lcm}(n,d)})^{\gcd(n,d)}$$

and

$$\begin{aligned} K_p \otimes_k k_n &\simeq (k_n \otimes k_d)((t)) \\ &= \left(k_{\operatorname{lcm}(n,d)}((t))\right)^{\gcd(n,d)} \end{aligned}$$

Next time, we'll deduce (*) from Claim (a), locally (taking each P individually). For Q's of degree q, we have in particular $k(Q) = k_n$ and $f(Q/P)\deg P = n$; since $\deg P = d$, we see that we get points of degree 1 exactly when $\deg P | n$.

Lecture 37 (November 22, 1995).
Scribe: Matt Baker

We are finishing a computation from last time.

As before, we have a finite field k with q elements, $k \subset K, \overline{k} \cap K = k, k_n \supset k$ of degree n.

Claim: $Z_{K\cdot k_n/k_n}(T^n) = \prod_{\zeta^n=1} Z_{K/k}(\zeta T)$.

Pf: We will use the Euler product $Z_{K/k}(T) = \prod \frac{1}{1-T^{deg(P)}}$, where the sum runs over the closed points P of C_K, and prove the desired formula P-wise. Using the fact that $n \cdot deg_{k_n}(Q) = n \cdot [k(Q) : k_n] = [k(Q) : k] = f(Q/P) \cdot deg(P)$, we see that the LHS is:

$$Z_{K\cdot k_n/k_n}(T^n) = \prod\prod \frac{1}{1 - T^{n\cdot deg_{k_n}(Q)}},$$

where the first product is taken over all closed points P of C_K and the second over all closed points Q in $C_{K\cdot k_n}$ lying over P. Using the formulas from the previous class, we see that this expression is equal to

$$\prod_P \left(\frac{1}{1 - T^{deg(P)\cdot\frac{n}{gcd(n,deg(P))}}}\right)^{gcd(n,deg(P))}.$$

On the other hand, the RHS of the expression in the claim is:

$$\prod_P \prod_{\zeta^n=1} \frac{1}{1-(\zeta T)^{deg(P)}}.$$

So it remains to show (taking $d = deg(P)$) that

$$\left(1 - T^{lcm(d,n)}\right)^{gcd(d,n)} = \prod_{\zeta^n=1} (1-(\zeta T)^d).$$

Exercise: Check that the roots and their multiplicities work out correctly in the above expression.

Recall: This proves that deg:Pic $\to \mathbf{Z}$ is surjective.

Also, this shows that $Z \in Q(T)$ with exact denominator equal to $(1-T)(1-qT)$.

Now we will prove the functional equation for the zeta function, which is basically a reformulation of Riemann-Roch.

Theorem(Functional Equation):

$Z(T) = q^{g-1} \cdot T^{2g-2} \cdot Z(\frac{1}{qT})$ [in $Q(T)$], i.e.,

$T^{1-g} \cdot Z(T)$ is invariant under the automorphism $T \mapsto \frac{1}{qT}$ of $\mathbf{Q}(T)$, i.e.,

$q^{(g-1)s} \cdot \zeta(s)$ is invariant under the automorphism $s \leftrightarrow 1-s$.

Also, one has $Z(T) = \frac{L(T)}{(1-T)(1-qT)}$, where

$L(T) = \prod_{i=1}^{2g}(1-\omega_i T) \in \mathbf{Z}[T]$ has degree $2g$, and $\omega_i \in \mathbf{C}$.

Finally, letting h = order of Pic^0, we have $L(1) = h$, and $\omega_i \cdot \omega_{g+1} = q$ for $1 \leq i \leq g$.

Proof: We have

$$Z(T) = \sum_{x \in Pic} \frac{q^{l(x)}-1}{q-1} T^{deg(x)} \in \mathbf{Z}[[T]].$$

We're going to work in the module

$$M = \{\sum_{i \in \mathbf{Z}} a_i T^i : a_i \in \mathbf{Q}\}.$$

M is a module over $\mathbf{Q}[T, T^{-1}]$, and $T \mapsto \frac{1}{qT}$ is an involution of M and of $\mathbf{Q}[T, T^{-1}]$. Let $U = \frac{1}{T}$.

Claim:

$$T^{1-g}(Z(T)+\sum_{x\in Pic}\frac{T^{deg(x)}}{q-1})=T^{1-g}(Z(T)+\frac{h}{q-1}\cdot\sum_{i\in\mathbf{Z}}T^i)$$

is fixed under the involution $T\leftrightarrow U$.

Proof of claim: Multiplying by $q-1$, this expression is just $\sum_{x\in Pic}q^{l(x)}T^{deg(x)+1-g}=\sum_{x\in Pic}U^{-l(x)}T^{-(l(x)+g-1-deg(x))}$.

But by Riemann-Roch, $-(l(x)+g-1-deg(x))$ is just $l(y)$, where $y\in Pic$ is such that $xy=[W]$, where $[W]$ is the class of the canonical divisor. So the previous sum is just $\sum U^{-l(x)}T^{-l(y)}$, where the summation is performed over all $x,y\in Pic$ such that $xy=[W]$. This expression is clearly fixed under $T\leftrightarrow U$, and the claim follows.

We can now finish the proof of the functional equation. Since

$\sum_{x\in Pic}U^{-l(x)}T^{-(l(x)+g-1-deg(x))}$ is fixed under $T\leftrightarrow U$, it must live in M as a sum of the form

$$\frac{h}{q-1}\sum_{i\leq g}T^i+\left(1+\frac{h}{q-1}\right)T^{1-g}+\ldots+\left(1+\frac{h}{q-1}\right)(qT)^{g-1}+\frac{h}{q-1}\cdot\sum_{i\geq g}(qT)^i.$$

Multiplying this by $-(1-T^{-1})(1-U^{-1})=T^{-1}(1-T)(1-qT)$, we end up in $\mathbf{Q}[T,T^{-1}]$ with the expression

$$T^{-g}(1-T)(1-qT)\cdot Z=T^{-g}+\ldots+(qT)^g,$$

which is invariant under the involution $T\leftrightarrow U$. This expression comes from the fact that $\sum_{i\in\mathbf{Z}}T^i$ is killed by $T-1$. This proves that $T^{1-g}Z(T)$ is invariant under $T\leftrightarrow U$. Since the LHS of the above expression is just $T^{-g}\cdot L(T)$, we see that $L(T)$ is a polynomial of degree $2g$ in $Z[T]$ with constant term 1, as claimed.

Also, we have

$$T^{-g}(1-T)(1-qt)=(1-qt)\cdot\frac{-h}{q-1}T^{g-1}+(1-T)P[T,T^{-1}]$$

for some polynomial P in T and T^{-1}. Therefore $L(1)=h$.

Finally, since T^{-g} is fixed under $T\leftrightarrow\frac{1}{qT}$, we see that $\omega\leftrightarrow\frac{q}{\omega}$ permutes the ω_i, including multiplicities.

It remains to show that the $\omega_i's$ pair up as asserted. It suffices to show that $\omega=-\sqrt{q}$ occurs with even multiplicity. But this follows from the fact that the constant term of L is 1 , not -1. This finishes the proof of the functional equation.

As a final note, recall that $T\cdot\frac{\mathrm{dlog}}{\mathrm{dT}}Z=\sum_{n=1}^{\infty}\#C(k_n)T^n$. Therefore we have just shown that

$$\#C(k_n)=q^n+1-\sum_{i=1}^{g}(\omega_i^n+\omega_{g+i}^n).$$

Exercise: This is sufficient to show that $1<|\omega_i|<q$.

Next time, we will begin proving the Riemann Hypothesis for curves, which states that we have a much stronger statement: $|\omega_i|=\sqrt{q}$.

Lecture 38 (November 27, 1995).
Scribe: David Jones

Let k be a finite field such that $\#k=q, k\subset K, \bar{k}\cap K=k$.
Then we defined $Z_{K/k}(T)=\frac{\prod_{i=1}^{2g}(1-\omega_i T)}{(1-T)(1-qT)}=\frac{L(T)}{(1-T)(1-qT)}$ such that $L(T)\in\mathbf{Z}[T]$ and $\omega_i\cdot\omega-i+g=q$.

GOAL: The Riemann Hypothesis: $|\omega_i|=\sqrt{q}$.
We have $N_n=\#C(k_n)=q^n+1-\sum_{i=1}^{2g}\omega_i^n$, specifically $N_1=\#C(k)$. Once we know the Riemann hypothesis, then we will have $|N_n-(q^n+1)|\leq 2g\sqrt{q}^n$.

Proposition. *If q is a square and $q>(g+1)^4$, then $N_1<q+1+(2g+1)\sqrt{q}$.*
Proof: Let $m=\sqrt{q}-1, n=\sqrt{q}+2g$.

Fix some $P\in C(k)$. We are going to construct $G\in K, G\neq 0$, which vanishes ot a high order in all $Q\in C(k), Q\neq P$, and with a "not too bad" pole in P.

Let $L(mP)^{\sqrt{q}}=\{f^{\sqrt{q}}|f\in L(mP)\}$. We get a multiplication map $L(nP)\otimes L(mP)^{\sqrt{q}}\stackrel{\cdot}{\to} L((n+m\sqrt{q})P)$.

Claim. *This map is not injective.*
Proof: $n+m\sqrt{q}>n>m>(g+1)^2-1=g^2+2g>2g-2$ so Riemann-Roch implies $\ell(nP)=n+1-g, \ell(mP)=m+1-g, \ell((n+m\sqrt{q})P)=n+m\sqrt{q}+1-g$. So the claim will follow as long as $(n+1-g)\cdot(m+1-g)>n+m\sqrt{q}+1-g$. The following algebra yields the result:
$q>(g+1)^4\Rightarrow\sqrt{q}>(g+1)^2\Rightarrow-\sqrt{q}<-(g+1)^2\Rightarrow q-(g+1)^2>q-\sqrt{q}\Rightarrow(\sqrt{q}-(g+1))\cdot(\sqrt{q}+(g+1))>q-\sqrt{q}\Rightarrow(n+1-g)\cdot(m-g)>m\sqrt{q}\Rightarrow(n+1-g)\cdot(m+1-g)>n+m\sqrt{q}+1-g$

Note that we may pick a basis $f_1,f_2,...,f_{m+1-g}$ for $L(mP)/k$ such that the numbers $\mathrm{ord}_P f_i$ are *pairwise distinct* and $0\leq\mathrm{ord}_P f_i\leq m=\sqrt{q}-1$. So each element of $L(nP)\otimes L(mP)^{\sqrt{q}}$ has a unique representation of the form $\sum_{i=1}^{m+1-g}s_i\otimes f_i^{\sqrt{q}}$ with $s_i\in L(nP)$. Hence there exist $s_i\in L(nP)$, not all zero, such that $\sum_{i=1}^{m+1-g}s_i f_i^{\sqrt{q}}=0$.

We will take $G = \sum_{i=1}^{m+1-g} s_i^q \cdot f_i^{\sqrt{q}} = (\sum_{i=1}^{m+1-g} s_i^{\sqrt{q}} \cdot f_i)^{\sqrt{q}}$. Also denote $\Gamma = G^{1/\sqrt{q}} = \sum_{i=1}^{m+1-g} s_i^{\sqrt{q}} \cdot f_i$.

Claim. $G \neq 0$.
Proof: Suppose $G = 0$. Then $\Gamma = 0 \Rightarrow \sum s_i^{\sqrt{q}} f_i = 0$. This means $\exists i \neq j$ such that $\mathrm{ord}_P(s_i^{\sqrt{q}} f_i) = \mathrm{ord}_P(s_j^{\sqrt{q}} f_j)$. Thus, we have $\mathrm{ord}_P f_i \equiv \mathrm{ord}_P f_j (\bmod \sqrt{q})$. This contradicts $\mathrm{ord}_P f_i$ distinct and between 0 and $m = \sqrt{q} - 1$. This finishes the proof of the claim.

So now $\Gamma \in L((\sqrt{q} \cdot n + m)P)$. If $Q \in C(k), Q \neq P$, then Γ has no pole at Q. We have (Image of Γ in $k(Q)$) $= \sum_i s_i(Q)^{\sqrt{q}} f_i(Q) = (\sum_i s_i(Q) f_i(Q)^{\sqrt{q}})^{\sqrt{q}} = 0^{\sqrt{q}} = 0$. (Note $k(Q) \cong k$ since $Q \in C(k)$.) Hence $\Gamma \in L((\sqrt{q} \cdot n + m)P - \sum Q) \neq 0$ (where $\sum Q$ is taken over all $Q \neq P, Q \in C(k)$) so $\ell((\sqrt{q} \cdot n + m)P - \sum Q) > 0$.
Hence $\deg((\sqrt{q} \cdot n + m)P - \sum Q) \geq 0$ so $n\sqrt{q} + m \geq N_1 - 1$. Rearranging and plugging in m and n yields $N_1 < q + 1 + (2g+1)\sqrt{q}$ which proves the proposition.

The above proof is due to Bombieri and Stepanov.

Look at $Z_{K \cdot k_n / k_n}(T^n) = \prod_{\zeta^n = 1} Z_{K/k}(\zeta T) = \frac{\prod_i (1 - \omega_i^n T^n)}{(1 - T^n)(1 - q^n T^n)}$.
Thus, $Z_{K \cdot k_n / k_n}(T) = \frac{\prod_i (1 - \omega_i^n T)}{(1 - T)(1 - q^n T)}$.

Claim. $|\omega_i| \leq q$.
Proof: $[K : k(t)] = m, N_1 \leq (q+1) \cdot m, N - n \leq (q^n + 1) \cdot m$. So we have that $\sum N_n T^n$ has radius of convergence $\geq 1/q$. But $\sum N_n T^n = \frac{1}{1-T} + \frac{1}{1-qT} - \sum_i \frac{1}{1 - \omega_i T}$. This finishes the proof of the claim.

Thus, we also have $|\omega_i| \geq 1$ since $\omega_i \cdot \omega_{i+g} = q$.
Claim. $1 < |\omega_i| < q$.
Proof: Suppose $\omega \cdot \bar{\omega} = 1$. ω is an algebraic integer and $|\sigma\omega| \geq 1, \forall \sigma \in \mathrm{Aut}\mathbf{C}$. So $\prod |\sigma\omega| = 1 \Rightarrow |\sigma\omega| = 1 \forall \sigma$. Thus, ω is a root of unity. This contradicts $\omega_i \neq 1$ when viewed over k_n since the ω's for k_n are the n^{th} powers of the ω_i's for k.
Lecture 39 (November 29, 1995).
Scribe: Dylan Thurston

Consider the matrices

$$T = \begin{pmatrix} 0 & 0 & \cdots \\ 1 & 0 & \cdots \\ 0 & 1 & \\ \vdots & & \ddots \end{pmatrix}$$

(the right shift acting on an ∞-dimensional vector space) and

$$S = \begin{pmatrix} 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \\ \vdots & \vdots & & \ddots \end{pmatrix}$$

(the left shift acting on the same space). Then $ST = \mathrm{id}$ while TS is the projection on to the span of all basis vectors but the first.

Now consider the matrices

$$A = \begin{pmatrix} 0 & T - \mathrm{id} & 0 \\ 0 & 0 & T - \mathrm{id} \\ 0 & 0 & 0 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 0 & 0 & 0 \\ \mathrm{id} & \mathrm{id} & \mathrm{id} \\ -S & -\mathrm{id} & -\mathrm{id} \end{pmatrix}$$

(both acting on a 3∞-dimensional space). Clearly $A^3 = 0$ so $\mathrm{Tr}(A) = 0$ (using Tate's definition of traces of finite-potent maps). The lower right 2×2 corner of B has square 0, so we also have $B^3 = 0$ and $\mathrm{Tr}(B) = 0$. But a computation shows that

$$(A + B)^3 \simeq ...$$

and that $\mathrm{Tr}(A + B) \neq 0$.

This example was produced by George Bergman. (I was careless enough to ask him.) He believes that such examples cannot be constructed with exponents p, q, r with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$ in place of 3, 3, and 3 above, but that for all other choices of exponents the additivity of trace will not hold. (Note that the case $p = 2$, $q = 2$ is a special case.)

Decomposition and Inertia Groups Consider $K \subset L$ a finite Galois extension of function fields (with Galois group $\mathcal{G}$), containing the discrete valuation rings $A \subset B$ respectively. Let k and l be the respective residue class fields. Recall that the *decomposition group* $\mathcal{G}_B$ is

$$\mathcal{G}_B = \{\sigma \in \mathcal{G} : \sigma B = B\}.$$

There is a natural map $\mathcal{G} \to \mathrm{Aut}\,_k l$. The kernel is I_B, the *inertia group*.

Theorem.

(a) $\#\mathcal{G}_B = e(B/A)f(B/A)$ and ever d.v.r. B' of L extending A is of the form σB for some $\sigma \in \mathcal{G}$.

(b) Assume k perfect*. Then $k \subset l$ is Galois, $\mathcal{G}_B \to \mathrm{Gal}(l/k)$ is onto, and I_B has $e(B/A)$ elements.

Proof of (a). We have the diagram

$$
\begin{array}{ccccc}
 & & \hat{L} = L \cdot \hat{K} & & \\
 & / & & \backslash & \\
L & & & & \hat{K} \\
\text{Galois}\backslash & & & / & \\
 & & K & &
\end{array}
$$

(using the ambiguous notation $\hat{K}$ = field of fractions of $\hat{A}$, etc.) By general Galois theory, $\hat{L}/\hat{K}$ is Galois and $\mathrm{Gal}(\hat{L}/\hat{K}) \hookrightarrow \mathrm{Gal}(L/K)$. We claim that the image is $\mathcal{G}_B$. If $\sigma \in \mathcal{G}$, then $\sigma \in \mathcal{G}_B \Leftrightarrow \sigma \in \mathrm{Gal}(\hat{L}/\hat{K}) \Leftrightarrow \sigma$ can be extended to a continuous automorphism of $\hat{B} \Leftrightarrow \sigma B = B$. By an old formula, the local degree is $\#\mathcal{G}_B = [\hat{L} : \hat{K}] = e \cdot f$. Thus we have

$$\#\{\sigma B : \sigma \in \mathcal{G}\} = \frac{\#\mathcal{G}}{\mathcal{G}_B} = \frac{[L : K]}{e \cdot f}$$

(note that e and f are the same for all σB) and

$$\sum_{B' = \sigma B} e \cdot f = e \cdot f \frac{[L : K]}{e \cdot f} = [L : K]$$

so there cannot be any B' not of the form σB.

Proof of (b). It suffices to show that

$$l^{\mathrm{im}(\mathcal{G}_B)} = k.$$

$\supset$: obvious.

$\subset$: Take any $x \in l^{\mathrm{im}(\mathcal{G}_B)}$. By definition, there is some $y \in \hat{B}$ mapping to x. We want to show that x is the image of an element of $\hat{A}$. Define a subgroup S of $\mathcal{G}_B$ as follows:

$$S = \begin{cases} \text{Sylow } p\text{-subgroup of } \mathcal{G}_B, & \text{if } p = \mathrm{char}\, k > 0; \\ \{\mathrm{id}\}, & \mathrm{char}\, k = 0 \end{cases}$$

Then consider

$$z = \sum_{\tau S \in \mathcal{G}_B / S} \tau \prod_{\sigma \in S} \sigma y \in \hat{A}.$$

* *Exercise:* figure out what happens if not

z maps to $[\mathcal{G}_B : S]x^{\#S} \in l$. But $[\mathcal{G}_B : S]$ is coprime to p by our choice of S, so we have shown that

$$\left(l^{\mathrm{im}(\mathcal{G}_B)}\right)^{\#S} \subset k$$

which implies (since k is perfect)

$$l^{\mathrm{im}(\mathcal{G}_B)} \subset k.$$

So $\mathcal{G}_B$ maps surjectively on to $\mathrm{Gal}(l/k)$. Q.E.D.

Suppose k is a finite field: $\#k = q < \infty$. Then $\mathrm{Gal}(l/k)$ is the group generated by the Frobenius automorphism, Frob, with

$$\mathrm{Frob}(\alpha) = \alpha^q.$$

We call $\sigma \in \mathcal{G}_B$ a *Frobenius* for B if $\sigma \mapsto \mathrm{Frob}$. By the above theorem, the number of Frobenii for B equals $e(B/A)$. For $Q \in C_K$ a closed point in a function field, a Frobenius for Q is a Frobenius for its local ring $\mathcal{O}_Q$.

Let k be a finite field, $q = \#k$, and let $L \supset k$ be a finitely-generated field extension of transcendence degree 1. (We do not assume that $\bar{k} \cap L = k$.) Let $\sigma \in \mathrm{Aut}\ _kL$ be such that $\mathrm{order}(\sigma) < \infty$.* Define

$$N(\sigma) = \sum_{\forall x \in \mathcal{O}_Q \colon \sigma x \equiv x^q \bmod \mathfrak{m}_Q} [k(Q) : k]$$

(We'll see this is less than infinity in a moment.)

Proposition. Suppose $k \subset E \subset L$ with L finite and Galois over E. Then

$$(\#\{P \in C_E | k(P) = k\} \ =) \ \ N_1(E) = \frac{1}{[L : E]} \sum_{\sigma \in \mathrm{Gal}(L/E)} N(\sigma).$$

(It follows that $N(\sigma) < \infty$: consider $E = L^{\langle\sigma\rangle}$.)

Proof. Let's look at the set of Q's contributing to the sum. If $\forall x \in \mathcal{O}_Q$, $\sigma x = x^q \bmod \mathfrak{m}_Q$ then $\sigma\mathcal{O}_Q = \mathcal{O}_Q$ (since σ is of finite order). If Q lies over $P \in C_K$, then $\sigma|_{k(P)}$ is the identity and $\sigma|_k(Q)$ is the q'th power map. It follows that q'th powering is the identity on $k(P)$; i.e., $k(P) = k$ and σ is a Frobenius for Q over P. (This argument can be turned around, as well.)

So

$$\begin{aligned}\sum_{\sigma \in \mathrm{Gal}(L/E)} N(\sigma) &= \sum_{\substack{P \in C_K \\ k(P) = k}} \sum_{\substack{Q \in C_L \\ Q \mapsto P}} \underbrace{[k(Q) : k]}_{f(Q/P)} \cdot \underbrace{(\#\text{Frobenii for } Q \text{ over } P)}_{e(Q/P)} \\ &= [L : E] \cdot \#P\text{'s} \\ &= [L : E] \cdot N_1(E).\end{aligned}$$

---

* This is a superfluous condition. *Exercise:* $\#\mathrm{Aut}\ L < \infty$.

Q.E.D.

This proposition gives an expression for N_1 in terms of $N(\sigma)$. Next lecture we'll go the other way, expressing $N(\sigma)$ in terms of N_1.

Proposition. With E, L as above, assume $E \cap \bar{k} = k$, and suppose $k_m \subset L$ is a finite extension of k (of degree m). We have $\mathrm{Gal}(L/E) \Rightarrow \mathrm{Gal}(k_m/k)$. If $\sigma \in \mathrm{Gal}(L/E) \not\mapsto \mathrm{Frob}$, then $N(\sigma) = 0$.

Proof. For any closed $Q \in C_L$, $k_m \hookrightarrow k(Q)$, so $\sigma|_{k(Q)} \neq \mathrm{Frob}$ and Q does not contribute to the sum for $N(\sigma)$. Q.E.D.

Lecture 40 (December 4, 1995).
Scribe: Emiliano Gómez

Throughout this lecture, k denotes "the" field of q elements, and k_m denotes an extension of degree m over k.

Let E be a function field over k, let L be a finite Galois field extension of E, and let $\sigma \in \mathrm{Aut}_k L$. Recall that

$$N(\sigma) \stackrel{\text{def}}{=} \sum_{Q} \deg Q$$

where the sum is taken over those closed points $Q \in C_L$ for which $\sigma x \equiv x^q \bmod m_Q$ for all $x \in \mathcal{O}_Q$.

We have the following three facts (the first two were proved last time):

Fact 1:

$$[L:E] \cdot N_1(E) = \sum_{\sigma \in \mathrm{Gal}(L/E)} N(\sigma)$$

Fact 2: If $k_m \subset L$ and $\sigma|_{k_m} \neq \mathit{Frob}$, then $N(\sigma) = 0$.

Fact 3: Suppose that $k_m \subset L$, $\mathrm{Gal}(L/E)$ is annihilated by m, $E \cap \overline{k} = k$, and $\sigma|_{k_m} = \mathit{Frob}$. Then

$L \cap \overline{k} = k_m$, $N(\sigma) = m \cdot N_1(L^{\langle\sigma\rangle})$, and $L^{\langle\sigma\rangle} \cap \overline{k} = k$.

Proof:

We have surjective maps $\mathrm{Gal}(L/E) \longrightarrow \mathrm{Gal}(L \cap \overline{k}/k) \longrightarrow \mathrm{Gal}(k_m/k)$.

Since $\mathrm{Gal}(L/E)$ is killed by m, so is $\mathrm{Gal}(L \cap \overline{k}/k)$.

The latter is therefore a cyclic group killed by m which maps onto a cyclic group of order m (namely $\mathrm{Gal}(k_m/k)$).

Therefore $\mathrm{Gal}(L \cap \overline{k}/k) \cong \mathrm{Gal}(k_m/k)$. So $L \cap \overline{k} = k_m$, proving the first statement.

Next, we apply Fact 1 to $L^{\langle\sigma\rangle}$ in the role of E, and get

$$m \cdot N_1(L^{\langle\sigma\rangle}) = \sum_{\tau \in \langle\sigma\rangle} N(\tau)$$

But by Fact 2, all the τ which do not restrict to $Frob$ have $N(\tau) = 0$. So this last sum is simply $N(\sigma)$, proving the second statement.

Finally, $L^{\langle\sigma\rangle} \cap \overline{k} = (L \cap \overline{k})^{\langle\sigma\rangle} = k_m^{\langle\sigma\rangle} = k$, concluding the proof.

Proposition:

Let K be a function field over k (i.e finitely generated and with trascendence degree 1 over k). Suppose that $K \cap \overline{k} = k$.

Let t be such that $k(t) \subset K$ is finite and separable (such t exists because k is perfect, being a finite field).

Let M be an extension of K which is finite and Galois over $k(t)$.

Assume also that q is a square, and that $q > (g' + 1)^4$, where

$g' = g_{M/M \cap \overline{k}}$. Then

$N_1(K) \geq (q+1) - \big([K : k(t)] - 1\big) \cdot (2g' + 1)\sqrt{q}$

Proof:

Choose m such that m kills $\mathrm{Gal}(M/k(t))$, and put $L = k_m \cdot M$.

Since $\mathrm{Gal}(L/k(t))$ injects into $\mathrm{Gal}(M/k(t)) \times \mathrm{Gal}(k_m/k)$, we see that $\mathrm{Gal}(L/k(t))$ is killed by m. We have

$$[L : K] \cdot N_1(K) = \sum_{\sigma} N(\sigma)$$

where the sum is taken over $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \mapsto Frob$. We split this sum as

$$\sum_{\sigma \in \mathrm{Gal}(L/k(t))} N(\sigma) \qquad - \sum_{\sigma \in \mathrm{Gal}(L/k(t)) - \mathrm{Gal}(L/K)} N(\sigma)$$

again with the understanding that we sum over those σ which yield $Frob$.

Let S be the indexing set for the second sum of this last expression.

By the above remark about m and our previous results, the last expression equals

$$[L : k(t)] \cdot N_1\big(k(t)\big) - m \cdot \sum_{\sigma \in S} N_1\big(L^{\langle\sigma\rangle}\big)$$

Now we claim that $g_{L^{\langle\sigma\rangle}} \leq g'$. We will prove this shortly, but let us assume it for the moment. Then we have

$q > (g_{L^{\langle\sigma\rangle}} + 1)^4$, and so, by a result from Monday, the last expression is greater than or equal to

$$[L : k(t)] \cdot (q+1) - m \cdot \mathrm{card}(S) \cdot \big(q + 1 + (2g' + 1)\sqrt{q}\big)$$

An easy count gives $\mathrm{card}(S) = \frac{1}{m}\big([L : k(t)] - [L : K]\big)$.

Putting these things together, we have

$$[L:K]\cdot N_1(K) \geq [L:k(t)]\cdot(q+1) - \big([L:k(t)]-[L:K]\big)\cdot\big(q+1+(2g'+1)\sqrt{q}\big)$$

or equivalently, after simplifying a little,

$$[L:K]\cdot N_1(K) \geq [L:K]\Big((q+1) - \big([K:k(t)]-1\big)\cdot(2g'+1)\sqrt{q}\Big)$$

Dividing thru by $[L:K]$, this proves the proposition.
It only remains to prove our claim that $g_{L\langle\sigma\rangle} \leq g'$:
We have
$g_{L\langle\sigma\rangle} = g_{L\langle\sigma\rangle\cdot k_m/k_m} \leq g_{L/k_m}$, by the Hurwitz formula.
And it is easy to see that
$g_{L/k_m} = g_{M/M\cap\overline{k}} = g'$.
This concludes the proof.

Recall

$$Z_{K/k}(T) = \frac{\prod_{i=1}^{2g}(1-w_iT)}{(1-T)(1-qT)}$$

Theorem: (Weyl, 1948)
$|w_i| = \sqrt{q} \ \ \forall i$.
Proof:
Pick t and M as in the above proposition. Replace k by a finite extension (and q by the corresponding power) such that the new q is a square and
$q > (g'+1)^4$. It is not hard to see that our g' remains the same under these changes.
Then by the last proposition, we have

$$\big|N_1(K)-(q+1)\big| \leq [K:k(t)]\cdot(2g'+1)\sqrt{q}$$

and also, for all $n>0$, we have

$$\big|N_1(K\cdot k_n/k_n)-(q^n+1)\big| \leq [K:k(t)]\cdot(2g'+1)\sqrt{q^n}$$

The factor $[K:k(t)]\cdot(2g'+1)$ on the right is independent of n.
The expression inside the absolute value on the left is $-\sum w_i^n$.
So we see that $\sum_n\sum_i w_i^nT^n$ has radius of convergence $\geq \frac{1}{\sqrt{q}}$.
So all $|w_i| \leq \sqrt{q}$. Since the w_i come in pairs with $w_iw_{g+i}=q$, we have $|w_i| = \sqrt{q} \ \ \forall i$, indeed.

Lecture 41 (December 4, 1995).
Scribe: Lawren Smitline

A few things are suggested by last week's proof of the Riemann Hypothesis.

Let E be a function field over k of order q. Let L/E be a finite Galois extension of fields with Galois group $\mathcal{G}$.

Let $\sigma \in Aut_k L$. Let C' be the set of closed points $Q \in C_L$ such that $\sigma x \equiv x^q$ $(\mathfrak{m}_Q)$ for all $x \in \mathcal{O}_Q$. Let $N(\sigma) = \Sigma_{Q \in C'}[k(Q) : k]$.

Here are two exercises.

Let M/E be a finite Galois extension. Let $\sigma \in \mathcal{G}$. Let $H = \{\tau : \tau \in Gal(M/E),\ \tau|_L = \sigma\}$. We have $N(\sigma)[M : L] = \Sigma_{\tau \in H} N_M(\tau)$.

If $\sigma|_{L\cap\bar{k}} \neq Frob$, then $N(\sigma) = 0$. Otherwise, $N(\sigma) = [L \cap \bar{k} : k]N_1(L \cdot \bar{k}^{\phi})$, for $\phi|_L = \sigma$, $\phi|_{\bar{k}} = Frob$.

(This last is at most $[L \cap \bar{k} : k](q + 1 + 2g_{L/L\cap\bar{k}}\sqrt{q})$.)

The Chebotarev Density Theorem
Algebraic Number Theory Version

Let $L \supset K$ be number fields with $L : K$ Galois. Let $\mathfrak{p} \subset K$ be prime and $\mathfrak{q} \subset L$ lie over $\mathfrak{p}$ with $e(\mathfrak{q}/\mathfrak{p}) = 1$. For notational convenience, we refer to these primes as the points P and Q. We have $\mathcal{G} \supset \mathcal{G}_Q \cong G_Q/I_Q = \langle Frob_Q \rangle$, with $|I_Q| = e(Q/P)$. Observe $Frob_{\sigma Q, L/K} = \sigma Frob_{Q,L/K} \in \mathcal{G}$ for $\sigma \in \mathcal{G}$.

$Frob_P = \{Frob_Q : Q \text{ lies over } P\}$ = a conjugacy class in $\mathcal{G}$, since P is unramified in L/K.

For example, $\mathbf{Q}(i)/\mathbf{Q}$: $\mathcal{G} = \{1, \bar{\cdot}\}$, and $Frob_P = 1$ for $P \equiv 1$ (4), $FrobP = \bar{\cdot}$ for $P \equiv -1$ (4).

Chebotarev density theorem 1923. Let $C \subset G$ be a conjugacy class.
Then $\lim_{x\to\infty} \frac{|\{\mathfrak{p} : \mathfrak{N}\mathfrak{p} \leq x,\ Frob_{\mathfrak{p},L/K} = C\}|}{|\{\mathfrak{p} : \mathfrak{N}\mathfrak{p} \leq x\}|} = \frac{|C|}{|\mathcal{G}|}$.

Function field version. Let k be a finite field of order q. Let $K \supset k$ be a finitely generated field extension of transcendence degree 1, with exact field of constants k_0. Let $L : K$ be a finite Galois extension with Galois group $\mathcal{G}$. Let $C \subset \mathcal{G}$ be a conjugacy class. For $P \in C_K(k)$, define $f_C(P) = \frac{|Frob_{Q/P} \cap C|}{e(Q/P)}$ where $Q \in C_L$ lies over P, and $Frob_{Q/P}$ is the coset in $\mathcal{G}_Q/I_Q$ mapping to $Frob$ under the isomorphism $\mathcal{G}_Q/I_Q \to \mathcal{G}al(k(Q) : k)$. This is independent of the choice of Q.

Note that $f_C(P)$ is a rational number in $[0, 1]$, and $f_C(P)$ is 0 or 1 if P is unramified.

Result. $\Sigma_{P \in C_K(k)} f_C(P)$ is zero if the elements of C do not restrict to
$Frob \in \mathcal{G}al(L \cap \bar{k}/k)$; otherwise, it is $\frac{|C|}{|\mathcal{G}|}[L \cap \bar{k} : k](q + 1 + 2g_{L/L\cap\bar{k}}\sqrt{q})$.

This is $\frac{|C|}{|\mathcal{G}|}(q+1+2g\sqrt{q}$ if we assume $L \cap \bar{k} = k$.

Proof. exercise.

Additional inequalities exist for N_i, the number of points on curves, when the genus goes to infinity and q is fixed.

Lecture 42 (December 6, 1995).
Scribe: Nick Meyer

Let $k \subset K, K \cap \bar{k} = k, |k| = q$.

Recall that $N_n(K) = |C_K(k_n)|; N_1(K) = q+1-\sum_{i=1}^{2g}\omega_i; N_n(K) = q^n+1-\sum_{i=1}^{2g}\omega_i^n$.

Remember too that $\prod(T-\omega_i) \in \mathbf{Z}[T])$, and that $|\omega_i| = \sqrt{q}$.

So, in general, $|N_1-(q+1)| \leq 2g\sqrt{q}$. But if we fix q sufficiently large, we can achieve a sharper bound.

Theorem: (Serre). $|N_1-(q+1)| \leq g[2\sqrt{q}]$.

Proof: We want $|\sum_{i=1}^{2g}\omega_i| \leq g[2\sqrt{q}]$. Set $\alpha_i = \omega_i + (q/\omega_i)$ (note that $q/\omega_i = \omega_{i+g} = \bar{\omega}_i$). So we want $|\sum_{i=1}^{g}\alpha_i| \leq g[2\sqrt{q}]$.

Lemma: Let $\alpha_1, \ldots, \alpha_g$ be real algebraic integers, stable under $\mathrm{Gal}(\bar{Q}/Q)$. Then $g \cdot \lceil \min \alpha_i \rceil \leq \sum_{i=1}^{g}\alpha_i \leq g \cdot \lfloor \max \alpha_i \rfloor$. Note that this lemma immediately implies the theorem we wish to prove.

Proof of Lemma: It is sufficient to prove one of the two inequalities (one can prove one inequality from the other by replacing α_i with $-\alpha_i$). So let's prove the first inequality. We may assume that $\lceil \min \alpha_i \rceil = 1$ - i.e., that all $\alpha_i > 0$. Then $\prod_{i=1}^{g}\alpha_i$ is a positive rational integer. So $\prod_{i=1}^{g}\alpha_i \geq 1 \Rightarrow (\prod_{i=1}^{g}\alpha_i)^{1/g} =$ geometric mean ≥ 1. But $\sum \alpha_i/g =$ arithmetic mean $\geq$ geometric mean. So $\alpha_i \geq g$, as required.

Theorem (Drinfeld-Vladut): For fixed q, one has $N_1(K) \leq g \cdot (\sqrt{q}-1+O(1))$ for $1 \leq g \to \infty$.

Key Idea: Suppose $N_1 = q+1-\sum_{i=1}^{2g}\omega_i$ is "close" to $2g\sqrt{q}$. Then "most ω_i" are close to $-\sqrt{q}$. But $N_2 = q^2+1-\sum\omega_i^2 \approx -2gq < 0$. This is patently impossible. We'll try to exploit this fact in the upcoming proof.

Proof: Let $M > 0, M \in \mathbf{Z}$. Write $\omega_i = \beta_i\sqrt{q}$, $|\beta_i| = 1, \bar{\beta}_i = \beta_i^{-1}$. Now

$$\begin{aligned} 0 \leq \sum_{i=1}^{g}|\sum_{n=0}^{M-1}\beta_i^n|^2 &= \sum_{i=1}^{g}(\sum_{n=0}^{M-1}\beta_i^n)(\sum_{m=0}^{M-1}\beta_i^{-m}) \\ &= \sum_{i=1}^{g}(M+\sum_{n=1}^{M-1}(M-n)(\beta_i^n+\beta_i^{-n})) \\ &= Mg + \sum_{n=1}^{M-1}(M-n)\sum_{i=1}^{g}(\beta_i^n+\beta_i^{-n}) \end{aligned}$$

Recall that $N_n = q^n + 1 - \sum_{i=1}^{g}(\omega_i^n + \bar{\omega}_i^n) = q^n + 1 - q^{n/2}\sum_{i=1}^{g}(\beta_i^n + \bar{\beta}_i^n)$. So

$$Mg + \sum_{n=1}^{M-1}(M-n)\sum_{i=1}^{g}(\beta_i^n + \beta_i^{-n}) = Mg - \sum_{n=1}^{M-1}(M-n)(N_n - q^n - 1)/q^{n/2}$$

$$\leq Mg - N_1\sum_{n=1}^{M-1}(M-n)q^{-n/2} + \text{ function of } q \text{ and } M.$$

Thus $N_1\sum_{n=1}^{M-1}(1-(n/M))q^{-n/2} \leq g +$ (a function of q and M) .

So for fixed q and M, $\limsup_{K,g\to\infty} N_1/g \leq (\sum_{n=1}^{M-1}(1-(n/M))q^{-n/2})^{-1}$. Therefore, $\limsup_{K,g\to\infty} N_1/g \leq (\lim_{m\to\infty}\sum_{n=1}^{M-1}(1-(n/M))q^{-n/2})^{-1} = (\sum_{n=1}^{\infty} q^{-n/2})^{-1} = \sqrt{q}-1$. And we're done. For more on this type of argument, ask Oesterle (if he can find his notes).

Let $A(q) = \limsup_{K,g\to\infty} N_1/g$. We've just proved that $A(q) \leq \sqrt{q}-1$. We will now list some related results.

$\exists c > 0 \forall q : a(q) \geq c\log q A(2) \geq 2/9; A(3) \geq 1/2; A(5) \geq 1/2$.

How about $A(4)$? Well,

Theorem: If q is a square, then $A(q) = \sqrt{q}-1$.

This theorem has dramatic impact on coding theory, as we'll see next time.

Result (A. Garcia, H. Steichtenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound", Invent. Math. 121 (1995), 211-222): Let q be a square. For all n, let $K_n = \mathbf{F}_q(x_1, x_2, x_3, \ldots, x_n)$, where x_1 is transcendental over $\mathbf{F}_q$, and $x_2, x_3, \ldots$ are defined inductively by the equation $(x_{i-1}x_i)^{\sqrt{q}} + x_{i-1}x_i = x_{i-1}^{(\sqrt{q}+1)}$, for $2 \leq i \leq n$. (Parenthetical note: Artin-Schreier extensions are of the form $X^p - X - a$, where $p =$ char k).

Now, if n is odd,

$$g(K_n) = (\sqrt{q}+1)q^{(n-1)/2} - \sqrt{q}^{(n+1)/2} - 2\sqrt{q}^{(n-1)/2} + 1.$$

If n is even,

$$g(K_n) = (\sqrt{q}+1)q^{(n-1)/2} - (1/2)\sqrt{q}^{(n/2)+1} - (3/2)\sqrt{q}^{n/2} - \sqrt{q}^{(n/2)-1} + 1$$

Finally, $N_1(K_n) = (q-1)q^{(n-1)/2} + C$, where $C = 2$ if $n = 1$; $C = \sqrt{q}+1$ if $n = 2$; $C = 2\sqrt{q}$ if $n \geq 3, q$ odd or $n = 3, Q$ even; $C = q + \sqrt{q}$ if $n = 4$, q even; $C = 2q$ if $n \geq 5$, q even.

Lecture43 (December 8, 1995).
Scribe: Nghi Nguyen

Let $\mathbf{F}_q$ be the finite field with q elements. A code (or linear code) is a subspace $C \neq 0$ of $\mathbf{F}_q^n$. We call n the word length of C, $k = \dim C$, and k/n the information rate.

Define weight function ω: $\mathbf{F}_q^n \longrightarrow \{0, 1, \ . \ . \ . \ , n\}$ such that

$\omega((x_i)_{i=1}^n) = \#\{i \mid x_i \neq 0\}$

d = (distance of C) = min $\{\omega(x) \mid x \in C \backslash \{0\}\}$

Now we show $k + d \leq n + 1$: Consider the linear subspace $W \subset \mathbf{F}_q^n$ given by

$$W = \{(a_1, \dots , a_n) \in \mathbf{F}_q^n \mid a_i = 0 \text{ for all } i \geq d\}$$

Any $a \in W$ has weight $\leq d - 1$, hence $W \cap C = 0$. As $\dim W = d - 1$ we obtain

$k + (d - 1) = \dim C + \dim W = \dim(C + W) + \dim(C \cap W) = \dim(C + W) \leq n$

Every C gives a point $(d/n\ ,\ k/n)$ in the unit square. Let

U_q = {set of limit points of all $(d/n\ ,\ k/n)$}

It is known that there is a continuous function α_q: [0,1] $\longrightarrow$ [0,1] such that

$$U_q = \{(x,y) \colon y \leq \alpha(x)\}$$

Moreover, $\alpha_q(0) = 1$, $\alpha_q(x) = 0$ for $1 - q^{-1} \leq x \leq 1$, and α_q decreasing in the interval $0 \leq x \leq 1 - q^{-1}$.

There is a lower bound for α_q proved by Gilbert-Varshamov around 1982:

If $0 \leq x \leq (q-1)/q$ then $\alpha_q \geq 1 - H_q(x)$, where H_q, called the *q-ary entropy function*, is defined as follows:

$H_q = 0$

$H_q = \frac{x log(q-1) - x log x - (1-x) log(1-x)}{log q}$

Bounds of α_q from Algebraic Geometry:

Let $K/\mathbf{F}_q$ be a finitely generated field extension of transcendence degree 1. Suppose $P_1, \dots , P_n \in C_K(\mathbf{F_q})$. Take any divisor D of degree $degD < n$, $\quad D = \sum n(p)P$. We consider the obvious projection map:

$\mathcal{L}(D) = K \cap \prod_P \hat{m}_P^{-n(P)} \longrightarrow \prod_{i=1}^n \hat{m}_{P_i}^{-n(P_i)} / \hat{m}_{P_i}^{-n(P_i)+1}$

It is easy to see that the right-hand-side is $\cong \mathbf{F}_q^n$. Let C be the image of $\mathcal{L}(D)$ in $\mathbf{F}_q^n$. Let $x \in \mathcal{L}(D)$, $x \neq 0$, $x \mapsto y \in C$. Then y has $\omega(y)$ non-zero coordinates. So it has $n - \omega(y)$ coordinates $= 0$. Then $x \in \mathcal{L}(D - \sum_{i \text{ such that } y_i = 0} P_i)$. Hence $deg(D - \sum_{i \text{ such that } y_i = 0} P_i) \geq 0$. That is, $degD - (n - \omega(y)) \geq 0$. So $\omega(y) \geq n - degD$, $\quad y \neq 0$ so $\mathcal{L}(D) \cong C$. And we have $d \geq n - degD$, $\quad k = l(D) \geq degD + 1 - g$. Thus $(d/n,\ k/n)$ lies to the northeast of $(1 - degD/n,\ degD/n + 1/n - g/n)$ in the unit square. So a lower bound of α_q is given approximately by $x + y = 1 - g/n$ (since $1/n \to 0$ as $n \to \infty$.)

If q = a square, then one can choose a sequence of K's with $g \longrightarrow \infty$, $n/g \longrightarrow \sqrt{q} - 1$. So $\alpha(x) \geq 1 - \frac{1}{\sqrt{q}-1} - x$. This is called the Tsfasman-Vladut-Zink Bound.

Exercises

Scribe: Hendrik Lenstra

All rings in this course are commutative with 1.

Exercise 1. Find all valuation rings of the field $\mathbf{Q}$ of rational numbers.

Exercise 2. Prove that every discrete valuation ring is Euclidean.

Exercise 3. Let A be a unique factorization domain that is not a field, and let $\mathfrak{p}$ be a minimal non-zero prime ideal of A. Prove that $\mathfrak{p}$ is principal, and that the localization $A_{\mathfrak{p}}$ is a discrete valuation ring.

Exercise 4. Let $k \subset K$ be an algebraic field extension, and let R be a valuation ring of K over k. Prove that $R = K$.

Exercise 5. In this exercise an overhead bar denotes algebraic closure. A field is called *perfect* if every algebraic extension of the field is separable.
(a) Let k be a perfect field, let A be a domain containing k, and let K be the field of fractions of A. Prove that the following three assertions are equivalent: $\bar{k} \otimes_k A$ is a domain; $\bar{k} \otimes_k K$ is a field; and $\bar{k} \cap K = k$, where the intersection is formed inside $\bar{K}$.
(b) Give an example to show that the equivalence in (a) may break down if k is not perfect.

Exercise 6. Let R be a ring. An R-*algebra* is a ring A provided with a ring homomorphism $R \to A$. An R-algebra A is *of finite type* if for some non-negative integer n there exists a surjective R-algebra homomorphism $R[X_1, \ldots, X_n] \to A$. This exercise is about R-algebras of finite type that are fields.

Let K be an R-algebra that is a field, and let $K_0 \subset K$ be the field of fractions of the image of R in K.
(a) Let $K(\alpha)$ be a field extension of K that is generated by a single element α. Prove: $K(\alpha)$ is of finite type as an R-algebra if and only if K is of finite type as an R-algebra and α is algebraic over K.
(b) Prove: K is of finite type as an R-algebra if and only if K_0 is of finite type as an R-algebra and $[K : K_0] < \infty$.
(c) Give a direct description of all R-algebras of finite type that are fields in the following cases: R is a field; R is an algebraically closed field; $R = \mathbf{Z}$; and $R = \mathbf{Z}_{(p)}$, the localization of $\mathbf{Z}$ at a prime number p.

Exercise 7. Let K be a field and let Ω be an algebraically closed field. In class we considered the set $\Sigma = \{(B, g) : B \text{ is a subring of } K \text{ and } g \colon B \to \Omega \text{ is a ring homomorphism}\}$.

Prove that Σ is empty if and only if $\operatorname{char}\Omega \neq \operatorname{char} K > 0$.

Exercise 8. Let $R_1, \ldots, R_n$ be n pairwise distinct discrete valuation rings of a field K, and put $R = \bigcap_{i=1}^{n} R_i$. Prove that R is a principal ideal domain with field of fractions K, and that the number of non-zero prime ideals of R equals n. (*Note.* If you cannot find a straightforward proof, look up the *approximation theorem* for (real-valued) valuations.)

Exercise 9. (a) Let R be a *complete* discrete valuation ring with maximal ideal $\mathfrak{m}$ and residue class field $k = R/\mathfrak{m}$, and put $1 + \mathfrak{m} = \{1 + a : a \in \mathfrak{m}\}$; this is the kernel of the natural group homomorphism $R^* \to k^*$. Prove that for each positive integer n that is not divisible by $\operatorname{char} k$ the map $1 + \mathfrak{m} \to 1 + \mathfrak{m}$ sending x to x^n is a group automorphism of $1 + \mathfrak{m}$.
(b) Let k be an algebraically closed field, and let L be a finite extension of the Laurent series field $k((t))$ for which $n = [L : K]$ is not divisible by $\operatorname{char} k$. Show that there is a unique valuation ring T of L that extends $R = k[[t]]$, that it satisfies $f(T/R) = 1$, $e(T/R) = n$, and that t is an nth power in T.
(c) Let k be an algebraically closed field of characteristic 0. Prove that $\bigcup_{n \geq 1} k((t^{1/n}))$ is an algebraic closure of $k((t))$.

Exercise 10. Let R be a complete discrete valuation ring, with field of fractions K. The purpose of this exercise is to show that R is the only discrete valuation ring of K. Let R' be a discrete valuation ring of K. Define $S = \{x \in K^* : x$ is an nth power in K^* for infinitely many positive integers $n\}$. Prove that $1 + \mathfrak{m} \subset S \subset R'^*$, where $\mathfrak{m}$ denotes the maximal ideal of R. Conclude that $\mathfrak{m} \subset R'$ and that $R = R'$.

Exercise 11. Let R be a ring, let $\pi \in R$, and write $\hat{R}$ for the projective limit of the rings $R/\pi^n R$, $n \geq 0$.
(a) Prove that there is a surjective ring homomorphism $f \colon R[[t]]/(t - \pi) \to \hat{R}$ sending the residue class of a power series $\sum_i r_i t^i$ to $(\sum_{i=0}^{n-1} r_i \pi^i)_{n=0}^{\infty}$.
(b) Prove that f is an isomorphism if π is not a zero-divisor of R.
*(c) Can you show that f is an isomorphism if R is noetherian? Can you construct an example in which f is *not* an isomorphism?

In Exercises 12–16, we let k be a field and K a finitely generated field extension of k of transcendence degree 1. We write C or C_K for the set of valuation rings of K over k.

Exercise 12. Let $x \in K$, and suppose that x is not algebraic over k. Write A for the integral closure of $k[x]$ in K.
(a) Prove that C can be written as a disjoint union $C_0 \cup C_1$, where $C_0 = \{P \in C : x \notin \mathcal{O}_P\}$

is finite and where $C_1 = \{A_\mathfrak{p} : \mathfrak{p}$ is a prime ideal of $A\}$.
(b) Define $D = \sum_{P \in C_0} P$. Prove that $\bigcup_{n \geq 0} L(nD) = A$.
Note. Give a reference for results about Dedekind rings that you may need.

Exercise 13. Let g be a non-negative integer, and let a, $b \in k[X]$ be such that $\deg a \leq g$ (allowing $a = 0$) and $\deg b = 2g + 1$.
(a) Show that the polynomial $F = Y^2 + aY + b \in k[X, Y]$ is irreducible. In the rest of this exercise we let K be the field of fractions of $k[X, Y]/(F)$, and we write x and y for the images of X and Y in K, respectively. We write ∞ for the only pole of x in $C_{k(x)} (= \mathbf{P}^1_k)$.
(b) Prove that $[K : k(x)] = 2$, that the set C_0 from Exercise 12 has exactly one point, P_∞ (say), that $\deg P_\infty = 1$, and that $e(P_\infty/\infty) = 2$.
(c) Prove: the integral closure A of $k[x]$ in K contains $k[x, y]$, and $\dim_k(A/k[x, y]) < \infty$.

Exercise 14. Let the notation be as in the previous exercise, and assume that $\operatorname{char} k \neq 2$. Let $f = a^2 - 4b \in k[X]$. Consider the statements: (a) $A = k[x, y]$; (b) f is not divisible by the square of an irreducible polynomial in $k[X]$; (c) the discriminant of f is non-zero. Prove that one has (a)$\Leftrightarrow$(b)$\Leftarrow$(c), and that if k is perfect one has (a)$\Leftrightarrow$(b)$\Leftrightarrow$(c).

Exercise 15. Let the notation be as in Exercise 13, and suppose that $\operatorname{char} k = 2$. Consider the statements: (a) $A = k[x, y]$; (b) there do not exist u, $v \in k[X]$, with v irreducible, for which v divides a and v^2 divides $u^2 + au + b$; (c) $\gcd(a, ba'^2 + b'^2) = 1$, where $'$ denotes differentiation with respect to X. Prove that (a)$\Leftrightarrow$(b)$\Leftarrow$(c), and that if k is perfect one has (a)$\Leftrightarrow$(b)$\Leftrightarrow$(c).

Exercise 16. Let the notation be as in Exercise 13, and suppose that $A = k[x, y]$. Find, for every non-negative integer n, a k-basis of $L(nP_\infty)$, and compute the genus of K.

Exercises 17–20 are applications of Riemann-Roch. We denote by k a field and by K a finitely generated field extension of k of transcendence degree 1. We assume that every element of K that is algebraic over k is in k. As in class, we write C for the set of valuation rings of K over k. By $\mathbf{A}_K$ we denote the adele ring, and by $\hat{\mathcal{O}}$ the subring $\prod_P \hat{\mathcal{O}}_P$ of $\mathbf{A}_K$, the product ranging over all closed points in C. We write g for the genus of K, and Div_K for the group of divisors.

Exercise 17. Let C_0 be a subset of C. Prove that the following two assertions are equivalent: (a) C_0 is finite and non-empty, and does not contain the generic point; (b) there exists $x \in K$, $x \notin k$, for which $C_0 = \{P \in C : x \notin \mathcal{O}_P\}$.

Exercise 18. As in Exercise 12, let $x \in K$, $x \notin k$. Write C_0 for the finite set $\{P \in C : x \notin$

$\mathcal{O}_P\}$, and denote by A the integral closure of $k[x]$ in K.
(a) Show that the natural map $K \to \bigoplus_{P \notin C_0} K_P/\hat{\mathcal{O}}_P$ is surjective; here P ranges over the closed points in C that are not in C_0.
(b) Deduce that $\mathbf{A}_K/(K + \hat{\mathcal{O}})$ is isomorphic to the cokernel of the natural map $A \to \prod_{P \in C_0} K_P/\hat{\mathcal{O}}_P$, and that this cokernel has dimension g over k. (Do you see the connection with Exercise 16?)

Exercise 19. Suppose that $g = 0$. Prove that the degree map $\deg\colon \mathrm{Pic}_K \to \mathbf{Z}$ is injective.

Exercise 20. Let m be the least integer in $\deg(\mathrm{Div}_K)$ that is greater than or equal to g, and let $D_0 \in \mathrm{Div}_K$ have degree m. Prove that every divisor class of degree 0 of K contains a divisor of the form $D - D_0$, where D is an effective divisor of degree m.

Exercise 21. Let $\mathcal{L}$ be the one-dimensional K-vector space Diff_K consisting of the Weil differentials, and for each closed point $P \in C$ let $\mathcal{L}_P \subset \mathcal{L}$ consist of those Weil differentials that are 0 on $\hat{\mathcal{O}}_P$ (viewing $\hat{\mathcal{O}}_P$ as a subset of $\mathbf{A}_K$ in the natural manner). Prove that $\mathcal{L}$ and the $\mathcal{L}_P$ constitute a line bundle on C. Prove also that this line bundle, under the isomorphism of $\mathrm{Pic}\, C$ with the divisor class group, corresponds to the canonical divisor class.

Exercises 22–24 concern the line bundle of Kähler differentials on the "hyperelliptic curves" from Exercises 13–16. The notation in these exercises is as in Exercise 13: k is a field, g is a non-negative integer, and a, $b \in k[X]$ are such that $\deg a \le g$ and $\deg b = 2g + 1$; we write $K = k(x, y)$ for the field defined by $y^2 + a(x)y + b(x) = 0$, and let P_∞ be the unique pole of x on $C = C_K$. We assume that the integral closure of $k[x]$ in K equals $k[x, y]$ (cf. Exercises 14 and 15). By Ω we denote the various modules of Kähler differentials.

Give precise formulations of results about Kähler differentials that you do not prove.

Exercise 22. (a) Prove that K is separably generated over k, and that P_∞ is a non-singular point of C.
(b) Prove that dx forms a basis of $\Omega_{K/k}$ over K if and only if K is separable over $k(x)$, and if and only if $\mathrm{char}\, k \neq 2$ or $a \neq 0$.

Exercise 23. In this exercise we denote by $'$ differentiation with respect to X.
(a) Let $P \neq P_\infty$ be a closed point of C. Prove that P is non-singular if and only if $2y + a(x)$ and $a'(x)y + b'(x)$ generate the unit ideal of the ring $\mathcal{O}_P$.
(b) Prove that C is non-singular if and only if $2y + a(x)$ and $a'(x)y + b'(x)$ generate the unit ideal of the ring $k[x, y]$, if and only if $a^2 - 4b$ and $ba'^2 - b'aa' + b'^2$ are coprime in $k[X]$. Use this to verify that C is non-singular if k is perfect.

Exercise 24. In this exercise we assume that C is non-singular, so that for every $P \in C$ the natural map $\Omega_{\mathcal{O}_P/k} \to \Omega_{K/k}$ may be viewed as an inclusion. Assume also that K is separable over $k(x)$, and put $\omega = (2y + a(x))^{-1} dx \in \Omega_{K/k}$.
(a) Prove: $\Omega_{\mathcal{O}_P/k} = \mathcal{O}_P \cdot \omega$ for all $P \in C$, $P \neq P_\infty$, and $\Omega_{\mathcal{O}_{P_\infty}/k} = \mathcal{O}_{P_\infty} \cdot x^{g-1}\omega$.
(b) Verify that $(\Omega_{\mathcal{O}_P/k})_{P \in C}$ makes $\Omega_{K/k}$ into a line bundle of degree $2g - 2$ on C.
(c) Write down a k-basis for the space $\bigcap_{P \in C} \Omega_{\mathcal{O}_P/k}$ of global sections of this line bundle.

Exercise 25. Let L be a finite field extension of the field $k((t))$ of formal Laurent series over a field k, and let A be the unique valuation ring of L extending $k[[t]]$. Let x, $y \in L$.
(a) Let $\pi: L \to A$ be a k-linear map that restricted to A is the identity. Prove that the k-linear map $f: L \to L$ defined by $f(v) = \pi(xyv) - y \cdot \pi(xv)$ is finite potent, and that its trace is independent of the choice of π. Formulate the properties of traces of finite potent maps that you use.
(b) Suppose that L equals $k((t))$, and write $x = \sum_i a_i t^i$, $y = \sum_j b_j t^j$, with $a_i = b_j = 0$ for i and j sufficiently small. Let f be as in (a). Prove: $\operatorname{Tr} f = \sum_{i+j=0} j a_i b_j$.

Exercise 26. Let A be a complete discrete valuation ring, E its field of fractions, and suppose that $p = \operatorname{char} E$ is nonzero. Let $\operatorname{ord}: E^* \to E^*/A^* \cong \mathbf{Z}$ denote the valuation. Let $a \in E$, $a \notin E^p$, and let F be the purely inseparable extension of E obtained by adjoining a pth root α of a to E. The E-linear function $t: F \to E$ is defined by $t(\sum_{i=0}^{p-1} c_i \alpha^i) = c_{p-1}$ (with $c_i \in E$). The unique valuation ring of F extending A is denoted by B, and its maximal ideal by $\mathfrak{m}_B$. In this exercise the ramification index $e = e(B/A)$, the residue class field degree $f = f(B/A)$, and the integer $m = \max\{n \in \mathbf{Z} : t(\mathfrak{m}_B^{-n}) \subset A\}$ are expressed in terms of an integer s that expresses how close a is to a pth power in E.
(a) Prove that $s = \max\{\operatorname{ord}(b^p - a) : b \in E\}$ exists.
(b) Prove: if p divides s, then one has $e = 1$, $f = p$, and $m = -(p-1)s/p$.
(c) Prove: if p does not divide s, then one has $e = p$, $f = 1$, and $m = -(p-1)(s-1)$.
(d) Prove that $m \leq 0$ if $a \in A$.

Exercise 27. Let k be a field of characteristic $p > 0$, and let K be a finitely generated field extension of k of transcendence degree 1. Let a be an element of K that is not a pth power in K, and put $L = K(\alpha)$ where $\alpha^p = a$. Denote by g_K and g_L the genera of K and L over k.
(a) Prove: $g_L \equiv g_K \bmod (p-1)/2$ (in the sense that $(g_L - g_K)/((p-1)/2) \in \mathbf{Z}$).
(b) Prove that there are only finitely many closed points $P \in C_K$ with the property that K contains an element b with $b^p - a \in \mathfrak{m}_P^2$; here $\mathfrak{m}_P$ denotes the maximal ideal of the local ring $\mathcal{O}_P$.

Exercise 28. Let k, p, K, a, L be as in the previous exercise, with the added assumption

that $a \in k$. Let l be the subfield $k(\alpha)$ of L, and denote by $g_{K/k}$ and $g_{L/l}$ the genera of K over k and of L over l, respectively.
(a) Prove that $g_{L/l} \leq g_{K/k}$, and that $g_{L/l} - g_{K/k}$ is divisible by $(p-1)/2$.
(b) Suppose that C_K is non-singular over k. Prove that C_L is non-singular over l, and that $g_{L/l} = g_{K/k}$.

Problem. Let p be a prime number, and let g_1, g_2 be integers satisfying $g_1 \geq g_2 \geq 0$, $g_1 \equiv g_2 \bmod (p-1)/2$. Do there exist k, a, K, L as in Exercise 28 such that $g_{K/k} = g_1$ and $g_{L/l} = g_2$?