LECTURE 20, MONDAY MAY 03, 2004

FRANZ LEMMERMEYER

1. Intersection Numbers

Let $\mathcal{C}_f$ and $\mathcal{C}_g$ be affine plane curves. We want to define intersection numbers $I(P, f \cap g)$ measuring the multiplicity with which $\mathcal{C}_f$ and $\mathcal{C}_g$ intersect at P.

Our intersection numbers should have the following properties:

(1) $I(P, f \cap g) \in \mathbb{N}$ if P is not on a common component of $\mathcal{C}_f$ and $\mathcal{C}_g$, and $I(P, f \cap g) = \infty$ otherwise.
(2) $I(P, f \cap g) = 0$ if and only if $P \notin \mathcal{C}_f \cap \mathcal{C}_g$.
(3) $I(P, f \cap g$ depends only on the components of $\mathcal{C}_f$ and $\mathcal{C}_g$ passing through P.
(4) The intersection number is invariant under an affine change of coordinates T: if $T(P) = Q$, then $I(Q, \mathcal{C}_f^T \cap \mathcal{C}_g^T) = I(P, f \cap g)$.
(5) $I(P, f \cap g) \ge m_P(\mathcal{C}_f) \cdot m_P(\mathcal{C}_g)$, with equality if and only if $\mathcal{C}_f$ and $\mathcal{C}_g$ do not have a common tangent at P.
(6) Intersection numbers are "additive" in the following sense: if $f = f_1 f_2$, then $I(P, f \cap g) = I(P, f_1 \cap g) + I(P, f_2 \cap g)$.
(7) For any $h \in K[X, Y]$ we have $I(P, f \cap g) = I(P, f \cap (g + hf))$.

The big theorem now is

Theorem 1.1. *These properties determine the intersection number completely, and we have*

$$I(P, f \cap g) = \dim_K \mathcal{O}_P(\mathbb{A}^2)/(f, g).$$

The proof can be found in Fulton's book *Algebraic Curves*. There is a reader-friendly account of the core of the proof in the appendix of Silverman's & Tate's *Rational Points on Elliptic Curves*; they actually start investigating $\dim R/(f, g)$ for $R = K[X, Y]$ and only later show that $I(P, f \cap g) \le \dim R/(f, g)$.

2. Picard Groups

The main theorem of the theory of algebraic curves is the theorem of Riemann-Roch. This theorem relates the dimensions of a few vector spaces, and its formulation does not convey its power at all.

In the following, let $\mathcal{C} : f(X, Y) = 0$ be a smooth irreducible algebraic curve (the theorem of Riemann-Roch also works for singular curves, but I want to avoid introducing even more notation).

Note that each point P on $\mathcal{C}$ defines a local ring $\mathcal{O}_P$; since $\mathcal{C}$ is smooth, the local ring is a discrete valuation ring, hence every point P defines a valuation $v = v_P$. These valuation attain nonnegative values on $\mathcal{O}_P$, but we can extend the multiplicatively to the quotient field $F = K(\mathcal{C})$ of $\mathcal{O}_P$, and then $v : F^\times \longrightarrow \mathbb{Z}$ is a group homomorphism whose kernel consists of the elements with valuation 0, that is, of the units $\mathcal{O}_P^\times$.

Recall that discrete valuation rings R are Noetherian local rings whose maximal ideal is principal. In particular, DVRs are Dedekind rings: these are essentially rings in which every ideal can be written uniquely as a product of prime ideals, and DVRs certainly have this property, since every ideal is just a power of $\mathfrak{m}$.

Now recall the following analogy we have already mentioned:

ring	$\mathbb{Z}_{(p)}$	$\mathcal{O}_P$
maximal ideal	(p)	$\mathfrak{m}_P$
quotient field	$\mathbb{Q}$	$K(\mathcal{C})$

In algebraic number theory, one looks at rings of integers $\mathcal{O}_K$ in finite extensions $K/\mathbb{Q}$ and studies the prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$. The rings $\mathcal{O}_K$ are also Dedekind rings, and every ideal $\mathfrak{p}$ defines a discrete valuation. The analogs of $\mathbb{Z}_{(p)}$ are the rings $\mathcal{O}_{(\mathfrak{p})} = \{\frac{\alpha}{\beta} \in K^\times : \mathfrak{p} \nmid \beta\}$.

In all three cases, we can form the intersection of the local rings; these consist of all elements in the field all of whose valuations are nonnegative:

- $\bigcap_{P\in\mathcal{C}} \mathcal{O}_P = K[\mathcal{C}]$;
- $\bigcap_p \mathbb{Z}_{(p)} = \mathbb{Z}$;
- $\bigcap_p \mathcal{O}_{(\mathfrak{p})} = \mathcal{O}_K$.

Thus the common notion is that of a valuation:

- for function fields of smooth curves, valuations correspond to points;
- for the rational numbers, valuations correspond to primes;
- for number fields, valuations correspond to prime ideals.

Note that, in the function field case, we only talked about the situation over algebraically closed fields; if you look at the field $\mathbb{R}(x)$ of rational functions over $\mathbb{R}$, then the prime x^2+1 defines a valuation which does not seem to correspond to a point on the real line as we know it. Setting up a correspondence between valuations and points for general fields requires some Galois theory.

In general, let R be a Dedekind ring with quotient field F, and assume that $v(r) \ge 0$ for all $r \in R$ and all valuations v of $F^\times$. Then we define $\mathrm{Div}(R)$ to be the set of all formal sums $\sum n_v v$, where v runs through all valuations of R and where n_v are integers, only finitely many of which are nonzero. The divisors form an abelian group $\mathrm{Div}(R)$, the free abelian group on the valuations.

- Consider the function field of the parabola $Y = X^2$; $D_1 = 2(0,0) - (2,4)$ and $D_2 = (1,1) - (0,0)$ are divisors, and their sum is $D_1 + D_2 = (0,0) + (1,1) - (2,4)$.
- the sum $4v_2 - 2v_3$ is a divisor in $R = \mathbb{Z}$, where v_2 and v_3 are the valuations for the primes 2 and 3.

Free abelian groups are quite boring. You can construct interesting objects out of free abelian groups by factoring out a free subgroup. We do this as follows:

- Every $r \in \mathbb{Q}^\times$ defines a divisor $\mathrm{div}(r)$ as follows: write $r = \pm\prod p^{a(p)}$ and define $\mathrm{div}(r) = \sum_p a(p)v_p$. Note that only finitely many $a(p)$ are nonzero.
- For every $g \in K(\mathcal{C})$ and any $P \in \mathcal{C}$, write $g = a/b$ for $a, b \in K[\mathcal{C}]$, and put $v_P(g) = v_P(a) - v_P(b)$. Now define $\mathrm{div}(g) = \sum_P v_P(g)P$. Note that $v_P(g) > 0$ if g has a zero at P, and $v_P(g) < 0$ if g has a pole at P. In particular, $v_P(g) = 0$ for all P except at most finitely many.

Divisors of the form $\mathrm{div}(g)$ for $g \in F$ are called principal divisors, and they form a subgroup $\mathrm{Pr}(R)$ of $\mathrm{Div}(R)$. The factor group $\mathrm{Pic}(R) = \mathrm{Div}(R)/\mathrm{Pr}(R)$ is

called the **Picard group** of R. If $R = \mathbb{Z}$, any divisor is principal: if, for example, $D = 3v_5 - 2v_2$, then $D = \operatorname{div}(2^{-2}5^3)$. Thus $\operatorname{Pic}(\mathbb{Z}) = 0$. For number fields, we have $\operatorname{Pic}(\mathcal{O}_K) = \operatorname{Cl}(K)$, the ideal class group. This should convince you that Picard groups are important objects.

Let us now compute a few divisors of rational functions on the affine line $\mathbb{A}^1\mathbb{C}$:

- $\operatorname{div}(x) = (0)$;
- $\operatorname{div}(x^n) = n(0)$;
- $\operatorname{div}(x^2 + 1) = (i) + (-i)$;
- $\operatorname{div}(\frac{x^2+1}{x^2}) = (i) + (-i) - 2(0)$.

It is clear that, given any divisor, there is a rational function with this divisor: if $D = \sum n_a(a)$, then clearly $f(x) = (x - a)^{n_a}$ does the trick, and this function is unique up to constants. Thus every divisor of the affine line is principal, and we have $\operatorname{Pic}(\mathbb{A}^1\mathbb{C}) = 0$.

Let me also compute the divisor of the function $(x+y)$ for the affine parabola $\mathcal{C}$: $Y - X^2 = 0$. Note that if $P \in \mathcal{C}$ is not on the line $Y = -X$, then $v_P(x+y) = 0$. Thus we only have to look at $P = (-1, 1)$ and $Q = (0, 0)$. We have $\mathfrak{m}_P = (x + 1, y - 1)$, hence $x + y = x + 1 + y - 1 \in \mathfrak{m}_P$ as expected; moreover, $\mathfrak{m}_P = (x + 1) = (y - 1)$, since neither $X = -1$ nor $Y = 1$ are tangents at P. Now $x + y = x + x^2 = x(x + 1)$, hence $v_P(x + y) = 1$. Similarly, $\mathfrak{m}_Q = (x, y) = (x)$, hence $f_Q(x + y) = 1$ as well. This shows that $\operatorname{div}(x + y) = P + Q$.

What happens if we look at rational functions on the projective line $\mathbb{P}^1\mathbb{C}$? There we have one more point, namely the point at infinity, which we will denote by ∞. Does this point correspond to a valuation as well? It does: we simply put $v_\infty(a/b) = v_\infty(a) - v_\infty(b) = \deg b - \deg a$ for polynomials $a, b \in \mathbb{C}[X]$. Observe that $g(x) = x^2 + 1$ tends to infinity for $x \to \infty$, hence should have a pole there, and actually we have $v_\infty(g) = 2$. Thus over the projective line we have

- $\operatorname{div}(x) = (0) - (\infty)$;
- $\operatorname{div}(x^n) = n(0) - n(\infty)$;
- $\operatorname{div}(x^2 + 1) = (i) + (-i) - 2(\infty)$;
- $\operatorname{div}(\frac{x^2+1}{x^2}) = (i) + (-i) - 2(0)$.

The **degree** of a divisor is the sum of its coefficients: $\deg(\sum n_P P) = \sum n_P$. Note that $\deg(D_1 + D_2) = \deg D_1 + \deg D_2$, hence $\deg : \operatorname{Div}(C) \longrightarrow \mathbb{Z}$ is a group homomorphism; its kernel is the subgroup $\operatorname{Div}^0(C)$ of divisors of degree 0. The examples above seem to suggest that the divisors of rational functions on the projective line all have degree 0; this is in fact true:

Proposition 2.1. *If $f \in \mathbb{C}(X)$ is a nonzero rational function, then* $\deg \operatorname{div}(f) = 0$.

This implies that not every divisor on the projective line is principal: for example, there is no rational function with divisor (0), i.e., there is no function with a zero at $x = 0$ and no pole. In fact, we have

Proposition 2.2. *The map* $\deg : \operatorname{Pic}(\mathbb{P}^1\mathbb{C}) \longrightarrow \mathbb{Z}$ *is an isomorphism.*

Thus in general Picard groups are not finite. Now let $\mathcal{C}$ be a smooth plane projective curve defined over some field K; since $\operatorname{Pr}(\mathcal{C})$ is a subgroup of $\operatorname{Div}^0(\mathcal{C})$, the group of divisors of degree 0, we can define $\operatorname{Pic}^0(\mathcal{C}) = \operatorname{Div}^0(\mathcal{C})/\operatorname{Pr}(\mathcal{C})$.

Theorem 2.3. *For smooth plane projective curves $\mathcal{C}$, principal divisors have degree* 0*, and the Picard group* $\operatorname{Pic}^0(\mathcal{C})$ *of degree* 0 *is finite.*

3. Riemann-Roch

Let $\mathcal{C}$ be a smooth plane projective curve. Recall that we have met divisors before: the points of intersection of two $\mathcal{C}$ and another curve $\mathcal{C}_g$ is a divisor of the form $\sum n_P P$, where $P \in \mathcal{C} \cap \mathcal{C}_g$, and where $n_P \ge 0$ is the multiplicity of the intersection at P. Divisors such as these, namely with $n_P \ge 0$ for all $P \in C$, are called **effective** or **positive**. Given two divisors D, D', we say that $D \ge D'$ if $D - D'$ is effective.

We now want to define vector spaces of functions whose divisors satisfy certain conditions; in order to make sure that these vector spaces contain the 0 element, we now formally introduce a divisor $\operatorname{div}(0)$ with the property that $\operatorname{div}(0) \ge D$ for all divisors D. Then, for any divisor D, we set

$$H^0(D) = \{f \in K(\mathcal{C}) : \operatorname{div}(f) + D \ge 0\}.$$

Observe that $H^0(D)$ is a K-vector space: if $f, g \in H^0(D)$, then so are $f+g$ and cf for $c \in K$.

Let K be an algebraically closed field and $D = \sum n_P P$ an effective divisor. Then $H^0(D)$ is the set of all functions in $K(\mathcal{C})$ with poles of order at most n_P at P, and no poles outside of the P. The set $H^0(D)$ for the zero divisor $D = 0$ consists of all functions without poles. It can be shown that the only such functions are constants, hence $H^0(D) = K$ in this case. If D is a divisor with $\deg D < 0$, then $H^0(D) = \{0\}$: in fact, for $f \in K(\mathcal{C})^\times$ we have $\deg(\operatorname{div}(f) + D) = 0 + \deg D < 0$, hence $\operatorname{div}(f) + D$ is never effective.

Proposition 3.1. *The set $H^0(D)$ is a finite dimensional K-vector space.*

Let $h^0(D)$ denote the dimension of $H^0(D)$.

Theorem 3.2 (Riemann's Theorem)**.** *We have*

$$h^0(D) \ge \deg(D) + 1 - g,$$

where g is the genus of $\mathcal{C}$.

Riemann's Theorem is an existence theorem: if $\deg(D) > g - 1$, the space $h^0(D)$ is nonempty, and there exist functions whose poles are "bounded" by D.

There are two problematic points here: first, the genus g was defined geometrically; there should be a definition in the language of divisors. Second, Riemann's theorem is an inequality. Can the difference between the two sides be measured somehow?

In order to take care of the first problem, for each divisor $D = \sum n_P P$ and each point P on $\mathcal{C}$ we define

$$\mathcal{L}(D)_P = \{f \in K(\mathcal{C}) : v_P(f) \ge -n_P\}.$$

This is again a K-vector space, as is $K(\mathcal{C})$. The map

$$\phi_D : K(\mathcal{C}) \longrightarrow \bigoplus_{P \in \mathcal{C}} K(\mathcal{C})/\mathcal{L}(D)_P : f \longmapsto \oplus_{P \in \mathcal{C}} (f + \mathcal{L}(D)_P)$$

is K-linear, and its kernel consists of all $f \in \bigcap \mathcal{L}(D)_P$; but $\bigcap \mathcal{L}(D)_P = H^0(D)$, hence $\ker \phi_D = H^0(D)$. Let us denote the cokernel of this map by $H^1(D)$. By definition, it is a K-vector space.

Of course nobody who sees this definition for the first time will have any idea of what this space 'actually' is. So don't worry.

Proposition 3.3. *$H^1(D)$ is a finite dimensional K-vector space.*

Let us denote the dimension of $H^1(D)$ by $h^1(D)$. The integer $h^1(D)$ for the zero divisor $D = 0$ now turns out to be nothing but the genus of the curve:

Theorem 3.4. *We have $h^1(0) = g$.*

Finally, here's the

Theorem 3.5 (Theorem of Riemann-Roch)**.** *Let $\mathcal{C}$ be a smooth plane projective curve. Then there exists a divisor $K \in \mathrm{Div}(\mathcal{C})$ such that*

$$h^0(D) = \deg(D) + 1 - g + h^0(K - D).$$

Next time I'll compute a few spaces $H^0(D)$ for some divisors D and the field $\mathbb{C}(X)$ of rational functions.