20.1 Degree theorem for morphisms of curves

Let us restate the theorem given at the end of the last lecture, which we will now prove.

Theorem 20.1. *Let $\phi\colon C_1 \to C_2$ be a morphism of curves defined over k. Then for each closed point Q of C_2/k,*

$$\deg \phi^*(Q) = \deg \phi \deg Q$$

Before beginning the proof, let us first show that we can assume without loss of generality that k is algebraically closed. If the closed point Q is the G_k-orbit $\{Q_1, \dots, Q_d\}$, with $d = \deg Q$, after base extension to $\bar{k}$ we have

$$\deg \phi^*(Q) = \deg \phi^*(Q_1 + \cdots + Q_d) = \deg \phi^*(Q_1) + \cdots + \deg \phi^*(Q_d),$$

since both the degree map and the pullback map $\phi^*\colon \mathrm{Div}_{\bar{k}}(C_2) \to \mathrm{Div}_{\bar{k}}(C_1)$ are group homomorphisms. If we assume the theorem holds over $\bar{k}$, then every term on the right is equal to $\deg \phi$ and the sum is $d \deg \phi = \deg \phi \deg Q$.

We now prove the theorem assuming $k = \bar{k}$, following the approach of [1, III.2].

Proof of Theorem 20.1. Fix $Q \in C_2$, and let $\mathcal{O}_Q$ be its local ring of regular functions. The set $\phi^{-1}(Q)$ is finite because ϕ is not constant and C_1 is an irreducible algebraic set of dimension one (so all its proper closed subsets are finite). Let $P_1, \dots, P_n \in C_1$ be the elements of $\phi^{-1}(Q)$, let $\mathcal{O}_1, \dots, \mathcal{O}_n$ be the corresponding local rings of regular functions, and define

$$\mathcal{O} = \bigcap_{i=1}^{n} \mathcal{O}_i.$$

By Lemma 20.4 below, there exist uniformizers $t_1, \dots, t_n$ for $\mathcal{O}_1, \dots \mathcal{O}_n$ such that

$$\mathrm{ord}_{P_i}(t_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

The maximal ideals of $\mathcal{O}$ are $(t_1), \dots, (t_n)$ and each nonzero $f \in \mathcal{O}$ factors uniquely as

$$f = u t_1^{e_1} \cdots t_n^{e_n},$$

with $u \in \mathcal{O}^\times$ and $e_i = \mathrm{ord}_{P_i}(f)$.

Under the map $\phi^*\colon k(C_2) \to k(C_1)$, for any $f \in \mathcal{O}_Q$ we have

$$\mathrm{ord}_{P_i}(\phi^* f) = \mathrm{ord}_{P_i}(f \circ \phi) = \mathrm{ord}_Q(f) \geq 0,$$

thus $\phi^*(\mathcal{O}_Q)$ is a subring of $\mathcal{O}$. If we now let t_Q be a uniformizer for $\mathcal{O}_Q$, and put $t = \phi^* t_Q$ we have

$$t = \phi^* t_Q = u t_1^{e_1} \cdots t_n^{e_n}$$

where $e_i = \mathrm{ord}_{P_i}(\phi^* t_Q) = e_\phi(P_i)$. Since $t_1, \dots, t_n$ are pairwise relatively prime (meaning that $(t_i) + (t_j) = \mathcal{O}$ for all $i \neq j$), by the Chinese remainder theorem we have

$$\mathcal{O}/(t) \simeq \bigoplus_{i=1}^{n} \mathcal{O}/(t_i^{e_i}) \tag{1}$$

as a direct sum of rings that are also k-vectors spaces (hence k-algebras). To prove the theorem we will compute the dimension of $\mathcal{O}(t)$ in two different ways, corresponding to the two sides of the equality $\deg \phi^*(Q) = \deg \phi$ that we are trying to prove.

On the LHS of the equality we wish to prove, the degree of the divisor $\phi^*(Q)$ is

$$\deg \phi^*(Q) = \sum e_\phi(P_i) \deg P_i = \sum e_i, \tag{2}$$

since we have $\deg P_i = 1$ for $k = \bar{k}$. We claim that this is precisely the dimension of $\mathcal{O}(t) \simeq \bigoplus_i \mathcal{O}/(t_i^{e_i})$ as a k-vector space, which we will prove below.

On the RHS of the equality, after identifying $k(C_2)$ with its image $\phi^*(k(C_2))$ we have

$$\deg \phi = [k(C_1) : k(C_2)],$$

which we claim is equal to the rank of $\mathcal{O}$ as an $\mathcal{O}_Q$-module ($\mathcal{O}_Q$ is embedded in $\mathcal{O}$ via ϕ^*). The ring $\mathcal{O}$ is an integral domain that is finitely generated as a module over the principal ideal domain $\mathcal{O}_Q$, so it is torsion free and isomorphic to $\mathcal{O}_Q^{\oplus r}$ for some integer r (by the structure theorem for modules over PIDs), hence it makes sense to speak of its rank r.

The fields $k(C_1)$ and $\phi^*(k(C_2))$ are the fraction fields of the rings $\mathcal{O}$ and $\mathcal{O}_Q$, respectively, and it follows that the maximal number of elements of $\mathcal{O}$ that are linearly independent over $\mathcal{O}_Q$ is exactly the same as the maximal number of elements of $k(C_1)$ that are linearly independent over $k(C_2)$, which is precisely $[k(C_1) : k(C_2)] = \deg \phi = d$. If we choose a basis $\alpha_1, \dots, \alpha_d$ for $k(C_1)$ over $k(C_2)$ and let $e = \min\{\operatorname{ord}_{P_i}(\alpha_j) : 0 \le i \le n, 0 \le j \le d\}$, then the functions $\alpha_1/t^e, \dots, \alpha_d/t^e$ are regular at all the P_i and therefore lie in $\mathcal{O}$. They are linearly independent over $\mathcal{O}_Q$, thus $r \ge d$, and clearly $r \le d$, since any r elements of $\mathcal{O} \subseteq k(C_1)$ that are linearly independent over $\mathcal{O}$ are also linearly independent over its fraction field $k(C_2)$. We have $\mathcal{O}_Q/(t) \simeq k$, since (t) is a maximal ideal, so $\dim_k \mathcal{O}/(t) = r = d = \deg \phi$.

To prove $\dim_k \mathcal{O}(t) = \deg \phi^*(Q)$, by (1) and (2) it suffices to show that $\dim_k \mathcal{O}/(t_i^{e_i}) = e_i$. We claim that for any positive integer n, each function $f \in \mathcal{O}$ can be written uniquely as

$$f \equiv a_0 + a_1 t_i + \cdots + a_{n-1} t_i^{n-1} \bmod t_i^n,$$

with each $a_i \in k$. Applying this with $n = e_i$ will yield the desired result.

For $n = 1$ we let $a_0 = f(P_i) \in k$. We then have $\operatorname{ord}_{P_i}(f - a_0) = \operatorname{ord}_{P_i}(f - f(P_i)) \ge 1$, so $f \equiv a_0 \bmod t_i$ as desired, and clearly a_0 is uniquely determined. We now proceed by induction on n, assuming that $f \equiv g = a_0 + a_1 t_i + \cdots a_{n-1} t_i^{n-1} \bmod t_i^n$. The $\operatorname{ord}_{P_i}(f - g) \ge n$, so $h = t_i^{-n}(f - g)$ is regular at P_i and therefore lies in $\mathcal{O}$ (since $\operatorname{ord}_{P_j}(t_i) = 0$ for $j \ne i$). Now let $a_n = h(P_i) \in k$. Then $\operatorname{ord}_{P_i}(t_i^n(h - a_n)) \ge n + 1$ and we have $f \equiv g + a_n t^n \bmod t^{n+1}$ as desired. □

The key to the proof of Theorem 20.1 is Lemma 20.3, which gave us the independent uniformizers $t_1, \dots, t_n$ we needed. In order to prove the lemma we need a tight form of the (nonarchimedean) triangle inequality for valuations.

Lemma 20.2 (Triangle equality)**.** *Let $v\colon F^\times \to \Gamma$ be a valuation on a field F. For any $x, y \in F^\times$ such that $v(x) \ne v(y)$ we have $v(x + y) = \min((v(x), v(y))$.*

Proof. Assume $v(x) < v(y)$. By the triangle inequality, $v(x + y) \ge \min(v(x), v(y))$. If this is not tight, $v(x + y) > v(x)$, but then $v(x) = v((x + y) - y) \ge \min(v(x + y), v(y)) > v(x)$, a contradiction. □

We now prove the main lemma we need, which is more generally known as the theorem of *independence of valuations* for function fields.

Lemma 20.3 (Independence of valuations)**.** *Let $P_1, \dots, P_n$ be distinct places of a function field F. Then there exist $t_1, \dots, t_n$ so that $v_i(t_j) = \delta_{ij}$ (Kronecker delta), where v_i denotes the valuation for P_i.*

Proof. If $n = 1$, we can take t_1 to be any uniformizer for P_1. We now proceed by induction, assuming that $t_1, \dots, t_{n-1}$ satisfy $v_i(t_j) = \delta_{ij}$. It suffices to find t_n with $v_n(t_n) = 1$ and $v_i(t_n) = 0$ for $0 \le i < n$. With such a t_n, we can then replace each t_i with t_i/t_n^e, where $e = v_n(t_i)$, so that $v_n(v_i) = 0$ and $v_i(t_j) = \delta_{ij}$ as required.

If $v_n(t_i) = 0$ for $0 \le i < n$, we can simply pick a uniformizer for P_n and multiply it by suitable powers of the t_i so that this is achieved, so let us assume otherwise. We now pick $s_1, \dots, s_{n-1}$ in $\mathcal{O}_{P_n}$ with $s_i \notin \mathcal{O}_{P_i}$; this is possible because none of the $\mathcal{O}_{P_i}$ contain $\mathcal{O}_{P_n}$, by Theorem 18.5. Then $v_n(s_i) \ge 0$ and $v_i(s_i) < 0$ for $0 \le i < n$. By replacing each s_i with $s_i^{e_i}$ for some suitably large $e_i > 0$ we can arrange it so that at each valuation v_j, for $0 \le j < n$, the value $\min\{v_j(s_i^{e_i}) : 0 \le i < n\}$ is achieved by a unique $s_i^{e_i}$ (possibly the same $s_i^{e_i}$ for different v_j's). For $s = \sum s_i^{e_i}$ we then have $v_j(s) < 0$ for $0 \le j < n$, by the triangle equality, and $v_n(s) \ge 0$.

Now let t be a uniformizer for $\mathcal{O}_{P_n}$, so $v_n(t) = 1$. If $v_n(s) = 0$ then we can replace t by $s^e t$ for some suitable e so that $v_i(t) < 0$ for $0 \le i < n$ and $v_n(t) = 1$, and if $v_n(s) > 0$ we can achieve the same goal by replacing t with $s^e + t$ (again by the triangle equality).

Now let w be the product of t with suitable powers of $t_1, \dots, t_{n-1}$ so that $v_i(w) = 0$ for $0 \le i < n$. If $v_n(w) = 0$ then apply the same procedure to $t + t^e$ for some suitably chosen $e > 0$ so that this is not the case (we have $v_n(t_i) \ne 0$ for some t_i, so this is always possible). Finally, if $v_n(w) < 0$ then replace w with $1/w$ so $v_n(w) > 0$. We than have $v_i(w) = 0$ for $0 \le i < n$ and $v_n(w) > 0$.

Now let $z = w + 1/t$. We have $v_i(1/t) > 0$ for $0 \le i < n$ and $v_n(1/t) = -1$, so by the triangle equality, $v_i(z) = 0$ for $0 \le i < n$ and $v_n(z) = -1$. For $t_n = 1/z$ we then have $v_i(t_n) = 0$ for $0 \le i < n$ and $v_n(t_n) = 1$ as desired, and we are done. □

Corollary 20.4. *Let $\mathcal{O}_1, \dots, \mathcal{O}_n$ be distinct discrete valuation rings of a function field F/k. The ring $\mathcal{O} = \cap_i \mathcal{O}_i$ has exactly n nonzero prime ideals $(t_1), \dots, (t_n)$, each principal and generated by a uniformizer for $\mathcal{O}_i$. Every nonzero $f \in \mathcal{O}$ can be uniquely factored as $f = u t_1^{e_1} \cdots t_n^{e_n}$ with $u \in \mathcal{O}^\times$ and $e_i = \operatorname{ord}_{P_i}(f) \ge 0$.*

Proof. The elements $t_1, \dots, t_n$ given by Lemma 20.3 are uniformizers for $\mathcal{O}_1, \dots, \mathcal{O}_n$, and it follows that every $f \in F^\times$ can then be written uniquely in the form $x = u t_1^{e_1} \cdots t_n^{e_n}$ with $u \in \mathcal{O}^\times$ and $e_i = \operatorname{ord}_{P_i}(x)$. The nonzero elements of $\mathcal{O}$ are precisely those for which the e_i are all nonnegative, and the lemma is then clear. □

We now note a further corollary of the lemma, which is an analog of the weak approximation theorem we proved in Lecture 11.

Corollary 20.5 (Weak approximation for function fields)**.** *Let $P_1, \dots, P_n$ be distinct places of a function field F/k, and let $f_1, \dots, f_n \in F$ be given. For every positive integer N there exists $f \in F$ such that $\operatorname{ord}_{P_i}(f - f_i) > N$ for $0 \le i < n$.*

Proof. Let $t_1, \dots, t_n$ be as in Lemma 20.3. As in the proof of Theorem 20.1, we can construct Laurent polynomials $g_i \in k((t_i))$ such that $g_i \equiv f_i \bmod t_i^N$, where the first nonzero term of

g_i is $a_s t_i^s$ where $a_s = \operatorname{ord}_{P_i}(f)$. We then have $\operatorname{ord}_{P_i}(g_i - f_i) \geq N$, and $\operatorname{ord}_{P_j}(g_i) \geq 0$ for $j \neq i$ since $\operatorname{ord}_{P_j}(t_i) = 0$ for $j \neq i$, this follows from the triangle inequality. Multiplying each g_i by $(t_1 \cdots t_{i-1} t_{i+1} \cdots t_n)^N$ and summing the results yields the desired function f. □

Note that in terms of absolute values, making the valuation $\operatorname{ord}_{P_i}(f - f_i)$ large corresponds to making the corresponding absolute value $|f - f_i|_{P_i}$ small. To make the analogy with Theorem 11.7 more precise, we could construct the completions of F_{P_i} at each place P_i and then the f_i given in the theorem would lie in F_{P_i} but f would still lie in F. The relationship between F and its completions F_{P_i} is then exactly analogous to the relationship between $\mathbb{Q}$ and its completions $\mathbb{Q}_{p_i}$.

20.2 Divisors of degree zero

It follows from Theorem 20.1 that the group of principal divisors $\operatorname{Princ}_k C$ is a subgroup of the group of degree zero divisors $\operatorname{Div}_k^0 C$, the quotient $\operatorname{Div}_k^0 C / \operatorname{Princ}_k C$ is denoted $\operatorname{Pic}_k^0 C$. Equivalently, $\operatorname{Pic}_k^0 C$ is the kernel of the degree map $\operatorname{Pic} C \to \mathbb{Z}$. We then have the exact sequence

$$1 \to k^\times \to k(C)^\times \to \operatorname{Div}_k^0 C \to \operatorname{Pic}_k^0 C \to 0.$$

Up to now all the groups of divisors and divisor classes we have considered have been infinite, but this is not true of Pic_k^0. The case where Pic_k^0 is trivial is already an interesting result.

Theorem 20.6. *Assume $k = \bar{k}$. Then $C \simeq \mathbb{P}^1$ if and only if $\operatorname{Pic}_k^0 C = \{0\}$.*

Proof. The forward implication is easy. Each point $P = (a_0, a_1) \in \mathbb{P}^1$ is the zero locus of the polynomial $f_P(x_0, x_1) = a_1 x_0 - a_0 x_1$, and if we have a divisor $D = \sum n_P P$ we can construct a corresponding homogeneous rational function $f = \prod f_P^{n_P}$. If D has degree zero then the numerator and denominator of f have the same degree and f is an element of $k(\mathbb{P}^1) \simeq k(C)$, so $D = \operatorname{div} f$. Thus $\operatorname{Div}_k C = \operatorname{Princ}_k C$ and $\operatorname{Pic}_k^0 C = 0$.

Now let P and Q be distinct points in $C(k)$; such P and Q exist because k is algebraically closed. Then $f = f_P / f_Q$ is a non-constant function in $C(k)$ that defines a morphism $(f_P : f_Q)$ from C to $\mathbb{P}^1$. The polynomials f_P and f_Q have degree one, and this implies that the morphism f has degree one and is an isomorphism. To check this, we can use Theorem 20.1 with $Q = 0$ and $t_0 = x/y$ to compute

$$\deg f = \deg f^*(0) = e_f(P) = \operatorname{ord}_P(f^* t_0) = \operatorname{ord}_P(t_0 \circ f) = \operatorname{ord}_P(f_P / f_Q) = 1. \qquad \square$$

Now let us consider the general case, where k is not necessarily algebraically closed. We then need to work with closed points, but the forward implication still holds: if C/k is isomorphic to $\mathbb{P}^1/k$ then $\operatorname{Pic}_k^0 C$ is trivial; the polynomials f_P in the proof are now irreducible polynomials that may have degree greater than one, but that doesn't change the argument.

But the converse is more interesting. We can always find closed points P and Q on C/k, but for the above proof to work we need them to have degree one, otherwise the function f_P/f_Q will not be an isomorphism. Equivalently, we need C/k to have two distinct rational points P and Q; these are closed points of degree one. We already know from earlier in the course that if C/k has genus 0 and even one rational point then it is isomorphic to $\mathbb{P}^1/k$ (and then it has more than two rational points). But if C/k has positive genus it can happen that C/k has one rational point and $\operatorname{Pic}_k^0 C = \{0\}$, but C cannot be isomorphic to $\mathbb{P}^1$, because $\mathbb{P}^1$ has genus zero. Indeed, this is exactly what happens for the elliptic curve

$y^2 = x^3 + 7$ over $\mathbb{Q}$, whose only rational point is ∞. So we need to add the hypothesis that C/k have two distinct rational points in order to get a theorem that works for general k.

Corollary 20.7. *Let C/k be a curve with at least two distinct rational points. Then C/k is isomorphic to $\mathbb{P}^1/k$ (with the isomorphism defined over k) if and only if* $\operatorname{Pic}^0_k C = \{0\}$.

As an interesting consequence, if C has genus greater than zero and at least two rational points, then $\operatorname{Pic}^0_k C$ cannot be trivial. The elliptic curve $C\colon y^2 = x^3 - 1$ over $k = \mathbb{Q}$ is such an example, with $\operatorname{Pic}^0_k C$ of order 2.

References

[1] I. R. Shafarevich, *Basic algebraic geometry*, 2nd edition, Springer-Verlag, 1994.

[2] H. Stichtenoth, *Algebraic function fields and codes*, Springer, 2009.