Lectures on
The Theory of Algebraic Functions
# of One Variable

by

M. Deuring

Notes by

C.P. Ramanujam

Tata Institute of Fundamental Research
Bombay
1959

Contents

Lecture 1

1 Introduction

We shall be dealing in these lectures with the algebraic aspects of the theory of algebraic functions of one variable. Since an algebraic function $w(z)$ is defined implicitly by an equation of the form $f(z, w) = 0$, where f is a polynomial, it is understandable that the study of such functions should be possible by algebraic methods. Such methods also have the advantage that the theory can be developed in the most general setting, viz. over an arbitrary field, and not only over field of complex numbers (the classical case). 1

Definition . *Let k be a field. An* algebraic function field *K over k is a finitely generated extension over k of transcendence degree at least equal to one. If the transcendence degree of K/k is r, we say that it is a function field in r variables.*

We shall confine ourselves in these lectures to algebraic function fields of one variable, and shall refer to them shortly as 'function fields'.

If K/k is a function field, it follows from our definition that there exists an X in K transcendental over k, such that $K/k(X)$ is a finite algebraic extension. If Y is another transcendental element of k, it should satisfy a relation $F(X, Y) = 0$, where F is a polynomial over K which does not vanish identically. Since Y is transcendental by assumption, 2 the polynomial cannot be independent of X. Rearranging in powers of X, we see that X is algebraic over $k(Y)$. Moreover,

$$[K : k(Y)] = [K : k(X, Y)].[k(X, Y) : k(Y)] \\ \leq [K : k(X)].[k(X, Y) : k(Y)] < \infty$$

and thus Y also satisfies the same conditions as X. Thus, any transcendental element of K may be used as a variable in the place of X.

The set of all elements of K algebraic over k forms a subfield k' of K, which is called the *field of constants* of K. Hence forward, we shall always assume, unless otherwise stated, that $k = k'$, i.e., that k is algebraically closed in K.

2 Ordered Groups

Definition . *A multiplicative(additive) Abelian group W with a binary relation $<$ ($>$) between its elements is said to be an ordered group if*

0(1) for $\alpha,\beta \in W$, one and only one of the relations $\alpha < \beta, \alpha = \beta, \beta < \alpha$ $(\alpha > \beta, \alpha = \beta > \alpha)$ holds.

0(2) $\alpha < \beta, \beta < \gamma \Rightarrow \alpha < \gamma\,(\alpha > \beta, \beta > \gamma \Rightarrow \alpha > \gamma)$

0(3) $\alpha < \beta, \delta \in W \Rightarrow \alpha\delta < \beta\delta(\alpha > \beta, \delta \in W \Rightarrow \alpha + \delta > \beta + \delta)$

We shall denote the identity (zero) element by 1(0). In this and the following section, we shall express all our results in multiplicative notation. $\alpha > \beta$ shall mean the same thing as $\beta < \alpha$.

Let W_0 be the set $\{\alpha : \alpha \in W\alpha < 1\}$. W_0 is seen to be a semi group by
3 0(2) and 0(3). Moreover, $W = W_0 \cup \{1\} \cup W_0^{-1}$ is a disjoint partitioning of W (where W_0^{-1} means the set of inverses of elements of W_0). Conversely, if an Abelian group W can be partitioned as $W_0 \cup \{1\} \cup W_0^{-1}$, where W_0 is a semi-group, we can introduce an order in W by defining $\alpha < \beta$ to mean $\alpha\beta^{-1} \in W_0$; it is immediately verified that 0(1), 0(2) and 0(3) are fulfilled and that W_0 is precisely the set of elements < 1 in this order.

For an Abelian group W, the map $\alpha \to \alpha^n$ (n any positive integer) is in general only an endomorphism. But if W is ordered, the map is a monomorphism; for if α is greater than or less than 1, α^n also satisfies the same inequality.

3 Valuations, Places and Valuation Rings

We shall denote the non-zero elements of a field K by K^*.

Definition. *A* Valuation *of a field K is a mapping v of K^* onto an ordered multiplicative (additive) group W (called the* group of the valuation *or the* valuation group*) satisfying the following conditions:*

V(1) *For $a, b \in K^*, v(ab) = v(a)v(b)$ $(v(ab) = v(a) + v(b))$; i.e. v is homomorphism of the multiplicative group K^* onto W.*

V(2) *For $a, b, a+b \in K^*, v(a+b) \leq \max(v(a), v(b))$ $(v(a+b)) \geq \min(v(a)$ $v(b)))$*

V(3) *v is non-trivial; i.e., there exists an $a \in K^*$ with $v(a) \neq 1(v(a) \neq 0)$*

Let us add an element $0(\infty)$ to W satisfying the following

(1) $0.0 = \alpha.0 = 0.\alpha = 0$ for every $\alpha \in W(\infty+\infty = \alpha+\infty = \infty+\alpha = \infty)$,

(2) $\alpha > 0$ for every $\alpha \in W(\alpha < \infty)$. If we extend a valuation v to the whole of K by defining $v(0) = 0\,(v(0) = \infty$, the new mapping also satisfies $V(1), V(2)$ and $V(3)$. 4

The following are simple consequences of our definition.

(a) For $a \in K, \quad v(a) = v(-a)$. To prove this, it is enough by $V(1)$ to prove that $v(-1) = 1$. But $v(-1)$. $v(-1) = v(1) = 1$ by $V(1)$, and hence $v(-1) = 1$ by the remark at the end of §2.

(b) If $v(a) \neq v(b), v(a + b) = \max(v(a), v(b))$. For let $v(a) < v(b)$. Then, $v(a + b) \leq \max(v(a), v(b)) = v(b) = v(a + b - a) \leq \max(v(a + b), v(a)) = v(a + b)$

(c) Let $a_i \in K, (i = 1, \ldots n)$. Then an obvious induction on $V(2)$ gives $v(\sum\limits_1^n a_i) \leq \max\limits_{i=1}^{n} v(a_i)$, and equality holds if $v(a_i) \neq v(a_j)$ for $i \neq j$.

(d) If $a_i \in K, (i = 1, \ldots n)$ such that $\sum\limits_1^n a_i = 0$, then $v(a_i) = v(a_j)$ for at least one pair of unequal indices i and j. For let a_i be such that

$v(a_i) \geq v(a_k)$ for $k \neq i$. Then $v(a_i) = v(\sum\limits_{\substack{k=1\\k\neq i}}^{n} a_k) \leq \max\limits_{\substack{k=1\\k\neq i}}^{n}(v(a_k)) = v(a_j)$ for some $j \neq i$, which proves that $v(a_i) = v(a_j)$.

Let $\sum$ be a field. By $\sum(\infty)$, we shall mean the set of elements of $\sum$ together with an abstract element ∞ with the following properties.
$\alpha + \infty = \infty + \alpha = \infty$ for every $\alpha \in \sum$.
$\alpha \,.\, \infty = \infty.\alpha = \infty$ for every $\alpha \in \sum, \alpha \neq 0$.
$\infty + \infty$ and $0.\infty$ are not defined.

5 **Definition.** *A* place *of a field K is a mapping φ of K into $\sum U(\infty)$ (where $\sum$ may be any field) such that*

P(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$.

P(2) $\varphi(ab) = \varphi(a).\varphi(b)$.

P(3) *There exist $a, b \in K$ such that $\varphi(a) = \infty$ and $\varphi(b) \neq 0$ or ∞. $P(1) and P(2)$ are to hold whenever the right sides have a meaning.*

From this it follows, taking the b of $P(3)$, that $\varphi(1)\varphi(b) = \varphi(b)$, so that $\varphi(1) = 1$, and similarly $\varphi(0) = 0$.

Consider the set $\mathscr{O}_\varphi$ of elements $a \in K$ such that $\varphi(a) \neq \infty$. Then by P(1), P(2) and P(3), $\mathscr{O}_\varphi$ is a ring which is neither zero nor the whole of K, and φ is a homomorphism of this ring into $\sum$. Since $\sum$ is a field, the kernel of this homomorphism is a prime ideal $\mathscr{Y}$ of $\mathscr{O}_\varphi$

Let b be an element in K which is not in $\mathscr{O}_\varphi$. We contend that $\varphi(\frac{1}{b}) = 0$. For if this mere not true, we would get $1 = \varphi(1) = \varphi(b).\ \varphi(\frac{1}{b}) = \infty$, by $P(2)$. Thus $\frac{1}{b} \in \mathscr{Y}$, and thus $\mathscr{Y}$ is precisely the set of non-units of $\mathscr{O}_\varphi$. Since any ideal strictly containing $\mathscr{Y}$ should contain a unit, we see that $\mathscr{Y}$ is a maximal ideal and hence the image of $\mathscr{O}_\varphi$ in $\sum$ is again a field. We shall therefore always assume that $\sum$ is precisely the image of $\mathscr{O}_\varphi$ by φ, or that φ is a mapping onto $\sum U(\infty)$.

The above considerations motivate the

Definition. *Let K be a field. A* valuation ring *of K is a proper subring $\mathscr{O}$ of K such that if $a \in K^*$, at least one of the elements a $\dfrac{1}{a}$ is in $\mathscr{O}$.* 6

In particular, we deduce that $\mathscr{O}$ contains the unity element. Let $\mathscr{Y}$ be the set of non-units in $\mathscr{O}$. Then $\mathscr{Y}$ is a maximal ideal. For, let $a \in \mathscr{O}, b \in \mathscr{Y}$. If $ab \notin \mathscr{Y}$, ab would be a unit of $\mathscr{O}$, and hence $\dfrac{1}{ab} \in \mathscr{O}$. This implies that $a\dfrac{1}{ab} = \dfrac{1}{b} \in \mathscr{O}$, contradicting our assumption that b is a non-unit of $\mathscr{O}$. Suppose that c is another element of $\mathscr{Y}$. To show that $b - c \in \mathscr{Y}$, we may assume that neither of them is zero. Since $\mathscr{O}$ is a valuation ring, at least one of $\dfrac{b}{c}$ or $\dfrac{c}{b}$, say $\dfrac{b}{c}$, is in $\mathscr{O}$. Hence, $\dfrac{b}{c} - 1 = \dfrac{b-c}{c} \in \mathscr{O}$. If $b - c$ were not in $\mathscr{Y}$, $\dfrac{1}{b-c} \in \mathscr{O}$, and hence $\dfrac{1}{b-c} \cdot \dfrac{b-c}{c} = \dfrac{1}{c} \in \mathscr{O}$, contradicting our assumption that $c \in \mathscr{Y}$. Finally, since every element outside $\mathscr{Y}$ is a unit of $\mathscr{O}, \mathscr{Y}$ is a maximal ideal in $\mathscr{O}$.

Lecture 2

3 (Contd.)

In this lecture, we shall establish the equivalence of the concepts of valuation, place and valuation ring. 7

Two places $\varphi_1 : K \to \sum_1 \cup (\infty)$ and $\varphi_2 : K \to \sum_2 \cup (\infty)$ are said to be *equivalent* if there exists an isomorphism λ of $\sum_1$, onto $\sum_2$ such that $\varphi_2(a) = \lambda \circ \varphi_1(a)$ for every a, with the understanding that $\lambda(\infty) = \infty$.

This is clearly an equivalence relation, and thus, we can put the set of places of K into equivalence classes. Moreover, equivalent places φ_1 and φ_2 obviously define the same valuation rings $\mathscr{O}_{\varphi_1}$ and $\mathscr{O}_{\varphi_2}$. Thus, to every equivalence class of places is associated a unique valuation ring.

Conversely, let $\mathscr{O}$ be any valuation ring and $\mathscr{Y}$ its maximal ideal. Let $\sum$ be the quotient field $\mathscr{O}/\mathscr{Y}$ and η the natural homomorphism of $\mathscr{O}$ onto $\sum$. It is an easy matter to verify that the map $\varphi : K \to \sum U\{\infty\}$ defined by

$$\varphi(a) = \begin{cases} \eta(a) & \text{if } a \in \mathscr{O} \\ \infty & \text{if } a \notin \mathscr{O} \end{cases}$$

is a place, whose equivalence class corresponds to the given valuation ring $\mathscr{O}$.

Let v_1 and v_2 be two valuations of a field K in the ordered group W_1 and W_2. We shall denote the unit elements of both the groups by 1, 8 since it is not likely to cause confusion. We shall say that v_1 and v_2 are *equivalent* if $v_1(a) > 1$ if and only if $v_2(a) > 1$.

Let v_1 and v_2 be two equivalent valuations. From the definition, it follows, by taking reciprocals, that $v_1(a) < 1$ if and only if $v_2(a) < 1$, and hence (the only case left) $v_1(a) = 1$ if and only if $v_2(a) = 1$. Let α be any element of W_1. Choose $a \in K$ such that $v_1(a) = \alpha$ (this is possible since v_1 is onto W_1). Define $\sigma(\alpha) = v_2(a)$. The definition is independent of the choice of a since if b were another element with $v_1(b) = \alpha$, then $v_1(ab^{-1}) = 1$ so that $v_2(ab^{-1}) = 1$, i.e. $v_2(a) = v_2(b)$. Thus, σ is a mapping from W_1 onto W_2 (since v_2 is onto W_2). It is easy to see that σ is an order preserving isomorphism of W_1 onto W_2 and we have $v_2(a) = (\sigma.v_1)(a)$ for every $a \in K^*$. Thus, we see that the definition of equivalence of valuations can also be cast into a form similar to that for places.

Again, equivalence of valuations is an equivalence relation, and we shall that equivalence classes of valuations of a field K correspond canonically and biunivocally to valuation rings of the field K.

Let v be a valuation and $\mathscr{O}$ be the set of elements a in K such that $v(a) \leq 1$. It is an immediate consequence of the definition that $\mathscr{O}$ is a ring. Also, if $a \in K, v(a) > 1$, then $v\left(\dfrac{1}{a}\right) < 1$ and hence $\dfrac{1}{a} \in \mathscr{O}$. Thus, $\mathscr{O}$
9 is a valuation ring. Also, if v_1 and v_2 are equivalent, the corresponding rings are the same.

Suppose conversely that $\mathscr{O}$ is a valuation ring in K and $\mathscr{Y}$ its maximal ideal. The set difference $\mathscr{O} - \mathscr{Y}$ is the set of units of $\mathscr{O}$ and hence a subgroup of the multiplicative group K^*. Let $\eta : K^* \to K^*/\mathscr{O} - \mathscr{Y}$ be the natural group homomorphism. Then $\eta(\mathscr{O}^*)$ is obviously a semigroup and the decomposition $K^*/\mathscr{O} - \mathscr{Y} = \eta(\mathscr{O}^*) \cup \{1\}U \cup \eta(\mathscr{O}^*)^{-1}$ is disjoint, Hence, we can introduce an order in the group $K^*/\mathscr{O} - \mathscr{Y}$ and it is easy to verify that η is a valuation on K whose valuation ring is precisely $\mathscr{O}$.

Summarising, we have

Theorem. *The valuations and places of a field K are, upto equivalence, in canonical correspondence with the valuation rings of the field.*

Lecture 3

4 The Valuations of Rational Function Field

10 Let $K = k(X)$ be a rational function field over k ; i.e., K is got by adjoining to k a single transcendental element X over k. We seek for all the valuations v of K which are *trivial on k*, that is, $v(a) = 1$ for every $a \in K^*$. It is easily seen that these are the valuations which correspond to places whose restrictions to k are monomorphic.

We shall henceforward write all our ordered groups additively.

Let φ be a place of $K = k(X)$ onto $\sum \cup (\infty)$. We consider two cases

Case 1. *Let $\varphi(X) = \xi \neq \infty$. Then, the polynomial ring $k[X]$ is contained in $\mathscr{O}_\varphi$, and $\mathscr{Y} \cap k[X]$ is a prime ideal in $k[X]$. Hence, it should be of the form $(p(X))$, where $p(X)$ is an irreducible polynomial in X. Now, if $r(X) \in K$, it can be written in the form $r(X) = (p(X))^\rho \dfrac{g(X)}{h(X)}$, where $g(X)$ and $h(X)$ are coprime and prime to $p(X)$. Let us agree to denote the image in $\sum$ of an element c in k by $\overline{c}$, and that of a polynomial f over k by $\overline{f}$. Then,we clearly have*

$$\varphi(r(x)) = \begin{cases} 0 & if\, \rho > o \\ \frac{g(\xi)}{h(\xi)} & if\, \rho = 0 \\ \infty & if\, \rho < 0 \end{cases}$$

11 Conversely, suppose $p(X)$ is an irreducible polynomial in $k[X]$ and ξ a root of $p(X)$. The above equations then define a mapping of $k(X)$ onto $k(\xi) \cup \{\infty\}$, which is a place, as is verified easily. We have thus determined all places of $k(X)$ under case 1 (upto equivalence).

If Z is the additive group of integers with the natural order, the valuation v associated with the place φ above is given by $v(r(X)) = \rho$.

Case 2. *Suppose now that $\varphi(X) = \infty$. Then $\varphi(\frac{1}{X}) = 0$. Then since $K = k(X) = k(\frac{1}{X})$, we see that φ is determined by an irreducible polynomial $p(\frac{1}{X})$, and since $\varphi\frac{1}{X}) = 0$, $p(Y)$ should divide Y. Thus, $p(Y)$ must be Y (except for a constant in k), and if*

$$r(X) = \frac{a_0 + a_1 x + - + a_n x^n}{b_0 + b_1 x + - + b_m x^m}, a_n, b_m \neq 0,$$

$$\varphi(r(X)) = \varphi\left((\tfrac{1}{X})^{m-n} \frac{\frac{a_0}{x^n} + \frac{a_1}{x^{n-1}} + - + a_n}{\frac{b_0}{x^m} + \frac{b_1}{x^{m-1}} + - + b_m} \right) = \begin{cases} o & if\, m > n \\ \frac{a_n}{b_m} & if\, m = n \\ \infty & if\, m < n \end{cases}$$

The corresponding valuation with values in Z is given by $v(r(X)) = m - n = -\deg r(X)$, where the degree of a rational function is defined in the degree of the numerator-the degree of the denominator.

We shall say that a valuation is *discrete* if the valuation group may be taken to be Z. We have in particular proved that all valuations of a rational function field trivial over the constant field are discrete. We shall extend this result later to all algebraic function fields of one variable.

5 Extensions of Places

12 Given a field K, a subfield L and a place φ_L of L into $\sum$, we wish to prove in this section that there exists a place φ_K of K into $\sum^1$, where $\sum^1$ is a field containing $\sum$ and the restriction of φ_K to L is φ_L. Such a φ_K is called an extension of the place φ_L to K. For the proof of this theorem, we require the following

Lemma (*Chevalley*). *Let K be a field, $\mathscr{O}$ a subring and φ a homomorphism of $\mathscr{O}$ into a field Δ which we assume to be algebraically closed. Let q be any element of K^*, and $\mathscr{O}[q]$ the ring generated by $\mathscr{O}$ and q in*

K. Then φ can be extended into a homomorphism Φ of at least one of the rings $\mathscr{O}[q]$, $\mathscr{O}[\frac{1}{q}]$, such that Φ restricted to $\mathscr{O}$ coincides with φ.

Proof. We may assume that φ is not identically zero. Since the image of $\mathscr{O}$ is contained in a field, the kernel of φ is a prime ideal $\mathscr{Y}$ which is not the whole ring $\mathscr{O}$. Let $\mathscr{O}^1 = \mathscr{O} \cup \left\{\frac{a}{b}\ a, b \in \mathscr{O}, b \notin \mathscr{Y}\right\}$. Clearly, $\mathscr{O}^1$ is a ring with unit, and φ has a unique extension $\tilde{\varphi}$ to $\mathscr{O}^1$ as a homomorphism, give by $\tilde{\varphi}\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$. The image by $\tilde{\varphi}$ is then the quotient field $\sum$ of $\varphi(\mathscr{O})$. We shall denote $\tilde{\varphi}(a)$ by $\bar{a}$ for $a \in \mathscr{O}^1$. □

Let X and $\bar{X}$ be indeterminates over $\mathscr{O}^1$ and $\sum$ respectively. $\tilde{\varphi}$ can be extended uniquely to a homomorphism $\bar{\varphi}$ of $\mathscr{O}^1[X]$ onto $\sum[\bar{X}]$ which takes X to $\bar{X}$ by defining

$$\bar{\varphi}(a_0 + a_1X + - + a_nX^n) = \bar{a}_0 + \bar{a}_1\bar{X} + - + \bar{a}_n\bar{X}^n.$$

Let $\mathscr{U}$ be the ideal $\mathscr{O}^1[X]$ consisting of all polynomials which van- 13
ish for $X = q$, and let $\bar{\mathscr{U}}$ be the ideal $\bar{\varphi}(\mathscr{U})$ in $\sum[\bar{X}]$. We consider three cases.

Case 1. *Let $\bar{\mathscr{U}} = (0)$. In this case, we define $\Phi(q)$ to be any fixed element of Δ. Φ is uniquely determined on all other elements of $\mathscr{O}^1[q]$ by the requirement that it be a ring homomorphism which is an extension of $\tilde{\varphi}$. In order that it be well defined, it is enough to verify that if any polynomial over $\mathscr{O}^1$ vanishes for q, its image by $\bar{\varphi}$ vanishes for $\Phi(q)$. But this is implied by our assumption.*

Case 2. *Let $\bar{\mathscr{U}} \neq (0), \neq \sum[\bar{X}]$. Then $\bar{\mathscr{U}} = (f(\bar{X}))$, where f is a non-constant polynomial over $\sum$. Let α be any root $f(\bar{X})$ in Δ (there is a root in Δ since Δ is algebraically closed). Define $\Phi(q) = \alpha$. This can be extended uniquely to a homomorphism of $\mathscr{O}^1[q]$, since the image by $\bar{\varphi}$ of any polynomial vanishing for q is of the form $f(\bar{X})f(\bar{X})$, and therefore vanishes for $\bar{X} = \alpha$.*

Case 3. *Suppose $\bar{\mathscr{U}} = \sum[\bar{X}]$. Then the homomorphism clearly cannot be extended to $\mathscr{O}^1[q]$. Suppose now that it cannot be extended to $\mathscr{O}^1[\frac{1}{q}]$*

either. Then if δ denotes the ideal of all polynomials in $\mathscr{O}^1[X]$ which vanish for $\dfrac{1}{q}$, and if $\bar{\delta}$ is the ideal $\bar{\varphi}(\delta)$in $\sum[\bar{X}]$, we should have $\bar{\delta} = \sum[\bar{X}]$. Hence, there exist polynomials $f(X) = a_0 + a_1X + - + a_nX^n$ and $b_0+b_1X+-+b_mX^m$ such that $\bar{\varphi}(f(X)) = \bar{\varphi}(g(X)) = 1$, $f(q) = g\left(\dfrac{1}{q}\right) = 0$. We may assume that f and g are of minimal degree n and m satisfying
14 *the required conditions. Let us assume that $m \leq n$. Then, we have $\bar{a}_0 = \bar{b}_0 = 1, \bar{a}_i = \bar{b}_j = 1$ for i, $j > 0$. Let $g_0(X) = b_0X^m + \cdots + b_m$. Applying the division algorithm to the polynomials $b_0^n f(X)$ and $g_0(X)$, we obtain*

$$b_0^n f(X) = g_0(X)Q(X) + R(X), Q(X), R(X) \in \mathscr{O}^1[X], \deg R < m.$$

Substituting $X = q$, we obtain $R(q) = 0$. Also, acting with $\bar{\varphi}$, we have

$$1 = \bar{b}_0^n \bar{f}(\bar{X}) = \bar{g}_0(\bar{X})\bar{Q}(\bar{X}) + \bar{R}(\bar{X}) = \bar{Q}(\bar{X})\bar{X}^m + \bar{R}(\bar{X}),$$

and hence, we deduce that $\bar{Q}(\bar{X}) = 0$, $\bar{R}(\bar{X}) = 1$. Thus, $R(X)$ is a polynomial with $R(q) = 0, \bar{R}(\bar{X}) = 1$, and deg $F(X) < m \leq n$, which contradicts our assumption on the minimality of the degree of $f(X)$. Our lemma is thus prove.

We can now prove the

Theorem. *Let K be a field and $\mathscr{O}$ a subring of K. Let φ be a homomorphism of $\mathscr{O}$ in an algebraically closed field Δ. Then it can be extended either to a homomorphism of K in Δ or to a place of K in $\Delta \cup (\infty)$. In particular, any place of a subfield of K can be extended to a place of K.*

Proof. Consider the family of pairs $\{\varphi_\alpha, \mathscr{O}_\alpha\}$, where $\mathscr{O}_\alpha$ is a subring if K containing $\mathscr{O}$ and φ_α a homomorphism of $\mathscr{O}_\alpha$ in Δ extending φ on $\mathscr{O}$. The family is non-empty, since it contains $(\varphi, \mathscr{O})$. We introduce a partial order in this family by defining $(\varphi_\alpha, \mathscr{O}_\alpha) > (\varphi_\beta, \mathscr{O}_\beta)$ if $\mathscr{O}_\alpha \supset \mathscr{O}_\beta$ and φ_α is an extension of φ_β. □

15 The family clearly being inductive, it has a maximal element by Zorn's lemma. Let us denote it by $(\Phi, \mathscr{O})$. $\mathscr{O}$ is either the whole of K or

a valuation ring of K. For if not, there exists a $q \in K$ such that neither q nor $\dfrac{1}{q}$ belongs to $\mathscr{O}$. we may then extend Φ to a homomorphism of at least one of $\mathscr{O}[q]$ or $\mathscr{O}\left[\dfrac{1}{q}\right]$ in Δ. Since both these rings contain $\mathscr{O}$ strictly, this contradicts the maximality of $(\Phi, \mathscr{O})$.

If $\mathscr{O}$ were not the whole of K, Φ must vanish on every non - unit of $\mathscr{O}$; for if q were a non-unit and $\Phi(q) \neq 0$, we may define $\Phi\left(\dfrac{1}{q}\right) = \dfrac{1}{\Phi(q)}$ and extend this to a homomorphism of $\mathscr{O}\left[\dfrac{1}{q}\right]$, which again contradicts the maximality of $\mathscr{O}$. This proves that Φ can be extended to a place of K by defining it to be ∞ outside $\mathscr{O}$.

In particular, a place φ of a subfield L of K , when considered as a homomorphism of its valuation ring $\mathscr{O}_\varphi$ and extended to K, gives a place on K; for if φ where a homomorphism of the whole of K in Δ, it should be an isomorphism (since the kernel, being a proper ideal in K, should be the zero ideal). But Φ being an extension of φ, the kernel contains at least one non-zero element.

Corollary. *If K/k is an algebraic function field and X any element of K transcendental over k, there exists at least one valuation v for which $v(X) > 0$.*

Proof. We have already shown in the previous section that there exists a place $\mathscr{Y}_1$ in $k(X)$ such that $v_{\mathscr{Y}_1}(X) > 0$. If we extend this place $\mathscr{Y}_1$ to a place $\mathscr{Y}$ of K, we clearly have $v_{\mathscr{Y}}(X) > 0$. □

Lecture 4

6 Valuations of Algebraic Function Fields

It is our purpose in this paragraph to prove that all valuations of an algebraic function field K which are trivial on the constant field k are discrete. Henceforward, when we talk of valuations or places of an algebraic function field K, we shall only mean those which are trivial on k. Valuations will always be written additively. We require some lemmas. **16**

Lemma 1. *Let K/L be a finite algebraic extension of degree $[K : L] = n$ and let v be a valuation on K with valuation group V. If $V_\circ$ denotes the subgroup of V which is the image of L^* under v and m the index of $V_\circ$ in V, we have $m \leq n$.*

Proof. It is enough to prove that of any $n+1$ elements $\alpha_1, \ldots \alpha_{n+1}$ of V, at least two lie in the same coset modulo $V_\circ$. □

Choose $a_i \in K$ such that $v(a_i) = \alpha_i$ $(i = 1, \ldots n+1)$. Since there can be at most n linearly independent elements of K over L, we should have

$$\sum_{i=1}^{n+1} l_i a_i = 0, l_i \in L, \text{ not all } l_i \text{ being zero .}$$

This implies that $v(l_i a_i) = y(l_j a_j)$ for some i and $j, i \neq j$ (see Lecture 1, § 3). Hence, we deduce that

$$\begin{aligned} v(l_i) + v(a_i) = v(l_i a_i) = v(l_j a_j) = v(l_j) + v(a_j), \\ \alpha_i - \alpha_j = v(a_i) - v(a_j) = v(l_j) - v(l_i) \in V_\circ \end{aligned}$$

and α_i and α_j are in the same coset modulo $V_\circ$. Our lemma is proved. 17

Let V be an ordered abelian group. We shall say that V is *archimedean* if for any pair of elements α, β in V with $\alpha > 0$, there corresponds an integer n such that $n\alpha > \beta$. We shall call any valuation with value group archimedean an *archimedean valuation*.

Lemma 2. *An ordered group V is isomorphic to Z if and only if (i) it is archimedean and (ii) there exists an element $\xi > 0$ in V such that it is the least positive element; i.e., $\alpha > 0 \Rightarrow \alpha \geq \xi$.*

Proof. The necessity is evident. Now, let α be any element of V. □

Then by assumption, there exists a smallest integer n such that $n\xi \leq \alpha < (n+1)\xi$. Thus,

$$0 \leq \alpha - n\xi < (n+1)\xi - n\xi = \xi,$$

and since ξ is the least positive element, we have $\alpha = n\xi$. The mapping $\alpha \in V \to n \in Z$ is clearly an order preserving isomorphism, and the lemma is proved.

Lemma 3. *If a subgroup $V_\circ$ of finite index of an ordered group V is isomorphic to Z, V is itself isomorphic to Z.*

Proof. Let the index be $\left[V : V_\circ\right] = n$. Let α, β be any two elements of V, with $\alpha > 0$. Then $n\alpha$ and $n\beta$ are in $V_\circ$, $n\,\alpha > 0$. □

Since $V_\circ$ is archimedean, there exists an integer m such that $mn\alpha > n\beta$, from which it follows that $m\alpha > \beta$.

18 Again, consider the set of positive elements α in V. Then $n\alpha$ are in $V_\circ$ and are positive, and hence contain a least element $n\xi$ (since there is an order preserving isomorphism between $V_\circ$ and Z). Clearly, ξ is then the least positive element of V.

V is therefore isomorphic to Z, by Lemma 2.

We finally have the

Theorem. *All valuations of an algebraic function field K are discrete.*

Proof. If X is any transcendental element of $K/_k$, the degree $\left[K : k(X)\right]$ $< \infty$. Since we know that all valuations of $k(X)$ are discrete, our result by applying Lemma 1 and Lemma 3. □

7 The Degree of a Place

Let $\mathscr{Y}$ be a place of an algebraic function field K with constant field k onto the field $k_{\mathscr{Y}} \cup \infty$. Since $\mathscr{Y}$ is an isomorphism when restricted to k, we may assume that $k_{\mathscr{Y}}$ is an extension of k. We shall moreover assume that $k_{\mathscr{Y}}$ is the quotient $\mathscr{O}_{\mathscr{Y}}/\mathscr{M}_{\mathscr{Y}}$ where $\mathscr{O}_{\mathscr{Y}}$ is the ring of the place $\mathscr{Y}$ and $\mathscr{M}_{\mathscr{Y}}$ the maximal ideal. We now prove the

Theorem. *Let $\mathscr{Y}$ be a place of an algebraic function field. Then $k_{\mathscr{Y}/k}$ is an algebraic extension of finite degree.*

Proof. Choose an element $X \neq 0$ in K such that $\mathscr{Y}(X) = 0$. Then X should be transcendental, since $\mathscr{Y}$ is trivial on the field of constants. Let $\left[K : k(X)\right] = n < \infty$. Let $\alpha_1, \ldots \alpha_{n+1}$ be any $(n+1)$ elements of 19 $k_{\mathscr{Y}}$. Then, we should have $\alpha_i = \mathscr{Y}(a_i)$ for some $a_i \in K (i = 1, \ldots n+1)$. There therefore exist polynomials $f_i(X)$ in $k[X]$ such that

$\sum_{i=1}^{n+1} f_i(X) a_i = 0$, not all $f_i(X)$ having constant term zero. □

Writing $f_i(X) = l_i + X g_i(X)$, we have

$$\sum_{i=1}^{n+1} l_i a_i = -X \sum_{i=1}^{n+1} a_i g_i(X), \text{ and taking}$$

the $\mathscr{Y}$-image, $\sum_{i=1}^{n+1} l_i \alpha_i = -\mathscr{Y}(X) \sum_{i=1}^{n+1} a_i g_i(\mathscr{Y} X) = 0, l_i \in k$, not all l_i being zero.

Thus, we deduce that the degree of $k_{\mathscr{Y}}/_k$ is at most n.

The degree $f_{\mathscr{Y}}$ of $k_{\mathscr{Y}}$ over k is called the *degree of the place $\mathscr{Y}$*. Note that $f_{\mathscr{Y}}$ is always ≥ 1. If the constant field is algebraically closed (*e.g.* in the case of the complex number field), $f_{\mathscr{Y}} = 1$, since $k_{\mathscr{Y}}$, being an algebraic extension of k, should coincide with k.

Finally, we shall make a few remarks concerning notation.

If $\mathscr{Y}$ is a place of an algebraic function field, we shall denote the corresponding valuation with values in Z by $v_{\mathscr{Y}}$ ($v_{\mathscr{Y}}$ is said to be a normed valuation at the place $\mathscr{Y}$). The ring of the place shall be denoted by $\mathscr{O}_{\mathscr{Y}}$ and its unique maximal ideal by $\mathscr{Y}$. (This is not likely to cause any confusion).

8 Independence of Valuations

20 In this section, we shall prove certain extremely useful result on valuations of an arbitrary field K.

Theorem. *Let K be an arbitrary field and $v_i (i = 1, \ldots n)$ a set of valuations on K with valuation rings $\mathscr{O}_i$ such that $\mathscr{O}_i \not\subset \mathscr{O}_j$ if $i \neq j$. There is then an element $X \in K$ such that $v_1(X) \geq 0$, $v_i(X) < 0\,(i = 1, \ldots n)$.*

Proof. We shall use induction. If $n = 2$, since $\mathscr{O}_1 \not\subset \mathscr{O}_2$, there is an $X \in \mathscr{O}_1, X \notin \mathscr{O}_2$, and this X satisfies the required conditions. Suppose now that the theorem is true for $n - 1$ instead of n. Then there exists a $Y \in K$ such that

$$v_1(Y) \geq 0, v_i(Y) < 0\,(i = 2, \ldots n - 1).$$

□

Since $\mathscr{O}_1 nsubset \mathscr{O}_n$, we can find $a\,Z \in K$ such that

$$v_1(Z) \geq 0, v_n(Z) < 0$$

Let m be a positive integer. Put $X = Y + Z^m$. Then

$$v_1(Y + Z^m) \geq \min(v_1(Y), mv_1(Z)) \geq 0$$

Now suppose r is one of the integers $2, 3, \ldots n$. If $v_r(Z) \geq 0$, r cannot be n, and since $v_r(Y) < 0$, we have

$$v_r(Y + Z^m) = v_r(Y) < 0.$$

21 If $v_r(Z) < 0$ and $v_r(Y + Z^{m_r}) \geq 0$ for some m_r, for $m > m_r$ we have

$$v_r(Y + Z^m) = v_r(Y + Z^{mr} + Z^m - Z^{m_r}) = \min(v_r(Y + Z^{m_r}), v_r(Z^m - Z^{m_r})),$$

and $v_r(Z^m - Z^{m_r}) = v_r(Z^{m_r}) + v_r(1 - Z^{m-m_r}) = m_r v_r(Z) < 0$,

Since $v_r(1 - Z^{m-mr}) = v_r(1) = 0$

Thus, $v_r(Y + Z^m) < 0$ for large enough m in any case. Hence X satisfies the required conditions.

If we assume that the valuations v_i of the theorem are archimedean, then the hypothesis that $\mathscr{O}_i \not\subset \mathscr{O}_j$ for $i \neq j$ can be replaced by the weaker one that the valuations are inequivalent (which simply states that $\mathscr{O}_i \neq \mathscr{O}_j$ for $i \neq j$).

To prove this, we have only to show that if v and v^1 are two archimedean valuations such that the corresponding valuation rings $\mathscr{O}$ and $\mathscr{O}^1$ satisfy $\mathscr{O} \supset \mathscr{O}^1$, then v and v^1 are equivalent. For, consider an element $a \in K^*$ such that $v(a) > 0$. Then, $v\left(\dfrac{1}{a}\right) < 0$, and consequently $\dfrac{1}{a}$ is not in $\mathscr{O}$, and hence not in $\mathscr{O}^1$. Thus, $v^1\left(\dfrac{1}{a}\right) < 0, v^1(a) > 0$. Conversely, suppose $a \in K^*$ and $v^1(a) > 0$. Then by assumption, $v(a) \geq 0$. Suppose now that $v(a) = 0$. Find $b \in K^*$ such that $v(b) < 0$. If n is any positive integer, we have $v(a^n b) = nv(a) + v(b) < 0$, $a_n b \notin \mathscr{O}$.

But since v^1 is archimedean and $v^1(a) > 0$, for large enough n we have

$$v^1(a^n b) = nv^1(a) + v^1(b) > 0\,, a^n b \in \mathscr{O}^1.$$

22

This contradicts our assumption that $\mathscr{O}^1 \subset \mathscr{O}$, and thus, $v(a) > 0$. Hence v and v^1 are equivalent. Under the assumption that the v_i archimedean, we can replace in the theorem above the first inequality $V_1(X) \geq 0$ even by the strict inequality $v_1(X) > 0$. To prove this let $X_1 \in K^*$ satisfy $v_1(X_1) \geq 0$, $v_i(X_1) < 0, i > 1$. Let Y be an element in K^* with $v_1(Y) > 0$. Then, if $X = {X_1}^m Y$, where m is a sufficiently large positive integer, we have

$$v_1(X) = v_1(X_1^m Y) = mv_1(X_1) + v_1(Y) > 0,$$
$$v_i(X) = v_i(X_1^m Y) = mv_i(X_1) + v_i(Y) < 0, \; i = 2, \ldots, n.$$

We shall hence forward assume that all valuations considered are archimedean. To get the strongest form of our theorem, we need two lemmas.

Lemma 1. *If v_i $(i = 1, \ldots n)$ are inequivalent archimedean valuations, and ρ_i are elements of the corresponding valuations group, we can find $X_i (i = 1, \ldots n)$ in K such that $v_i(X_i - 1) > \rho_i, v_j(X_i) > \rho_j, i \neq j$*

Proof. Choose $Y_i \in K$ such that

$$v_i(Y_i) > 0, v_j(Y_i) < 0 \text{ for } j \neq i.$$

Put $X_i = \dfrac{1}{1 + Y_i^m}$. Then, if m is chosen large enough, we have (since the valuation are archimedean)

$$v_j(X_i) = -v_j(1 + Y_i^m) = -mv_j(Y_i) > \rho_j, \quad i \neq j$$

23 and $v_i(X_i - 1) = v_i(\dfrac{-Y_i^m}{1 + Y_i^m}) = mv_i(Y_i) - v_i(1 + Y_i^m) = mv_i(Y_i) > \rho_i$. since $v - i(1 + Y_i^m) = 0$. □

A set of valuations $v_i (i = 1, \ldots n)$ are said to be independent if given any set of elements $a_i \in K$ and any set of elements ρ_i in the respective valuation groups of v_i, we can find an $X \in K$ such that

$$v_i(X - a_i) > \rho_i.$$

We then have the following

Lemma 2. *Any finite set of inequivalent archimedean valuations are independent.*

Proof. Suppose $v_i (i = 1, \ldots n)$ is a given set of inequivalent archimedean valuations. If $a_i \in K$ and ρ_i are elements of the valuation group of the v_i, put $\sigma_i = \rho_i - \min\limits_{j=1}^{n} v_i(a_j)$. Choose X_i as in Lemma 1 for the v_i and σ_i. Put $X = \sum\limits_{1}^{n} a_i X_i$. Then

$$v_i(X - a_i) = v_i\left(\sum_{j \neq i} a_j X_j + a_i(X_i - 1)\right) > \sigma_i + \min_{j=1}^{n} v_i(a_j) = \rho_i,$$

and our lemma is proved. □

Finally, we have the following theorem, which we shall refer to in future as the theorem of independence of valuations.

Theorem . *If $v_i (i = 1, \ldots n)$ are inequivalent archimedean valuations, ρ_i is an element of the value group of v_i for every i, and a_i are given elements of the field, there exists an element X of the field such that* 24

$$v_i(X - a_i) = \rho_i$$

Proof. Choose Y by lemma 2 such that $v_i(Y - a_i) > \rho_i$. Find $b_i \in K$ such that $v_i(b_i) = \rho_i$ and an $Z \in K$ such that $v_i(Z - b_i) > \rho_i$. Then it follows that $v_i(Z) = \min(v_i(Z - b_i), v_i(b_i)) = \rho_i$. □

Put $X = Y + Z$. Then,

$$v_i(X - a_i) = v_i(Z + Y - a_i) = v_i(Z) = \rho_i,$$

and X satisfies the conditions of the theorem.

Corollary. *There are an infinity of places of any algebraic function field.*

Proof. Suppose there are only a finite number of places $\mathscr{Y}_1, \ldots, \mathscr{Y}_n$. □

Choose an X such that $v_{\mathscr{Y}_i}(X) > 0 (i = 1, \ldots n)$. Then, $v_{\mathscr{Y}_i}(X + 1) = v_{\mathscr{Y}_i}(1) = 0$ for all the places , $\mathscr{Y}_i$, which is impossible since X an consequently $X + 1$ is a transcendental element over k.

Lecture 5

9 Divisors

Let K be an algebraic function field with constant field k. We make the 25

Definition. *A* divisor *of K is an element of the free abelian group generated by the set of places of K. The places themselves are called* prime divisors.

The group ϑ of divisors shall be written multiplicatively. Any element $\mathscr{U}$ of the group ϑ of divisors can be written in the form

$$\mathscr{U} = \prod_{\mathscr{Y}} \mathscr{Y} v_{\mathscr{Y}(\mathscr{U})}$$

where the product is taken over all prime divisors $\mathscr{Y}$ of K, and the $v_{\mathscr{Y}}(\mathscr{U})$ are integers, all except a finite number of which are zero. The divisor is denoted by n.

We say that a divisor $\mathscr{U}$ is *integral* if $v_{\mathscr{Y}}(\mathscr{U}) \geq 0$, for every $\mathscr{Y}$, and that $\underline{\mathscr{U}}$ *divides* $\underline{\delta}$ if $\delta\mathscr{U}^{-1}$ is integral. Thus, $\mathscr{U}$ divides δ if and only if $v_{\mathscr{Y}}(\delta) \geq v_{\mathscr{Y}}(\mathscr{U})$ for every $\mathscr{Y}$.

Two divisors $\mathscr{U}$ and δ are said to be *coprime* if $v_{\mathscr{Y}}(\mathscr{U} \neq 0$ implies that $v_{\mathscr{Y}}(\delta) = 0$.

The *degree* $d(\mathscr{U})$ of a divisor $\mathscr{U}$ is the integer

$$d(\mathscr{U}) = \sum_{\mathscr{Y}} f_{\mathscr{Y}} v_{\mathscr{Y}}(\mathscr{U}),$$

where $f_{\mathscr{Y}}$ is the degree of the place $\mathscr{Y}$. 26

The map $\mathscr{U} \to d(\mathscr{U})$ is a homomorphism of the group of divisors ϑ into the additive group of integers. The kernel $\vartheta_\circ$ of this homomorphism is the subgroup of divisors of degree zero.

An element X of K is said to be *divisible* by the divisor $\mathscr{U}$ if $v_{\mathscr{Y}}(X) \geq v_{\mathscr{Y}}(\mathscr{U})$ for every $\mathscr{Y}$. Two elements $X, Y \in K$ are said to be *congruent modulo a divisor* $\mathscr{U}$ (written $X \equiv (\mod \mathscr{U})$) if $X - Y$ is divisible by $\mathscr{U}$.

Let S be a set prime divisors of K. Then we shall denote by $\Gamma(\mathscr{U}/S)$ the set of elements $X \in K$ such that $v_{\mathscr{Y}}(X) \geq v_{\mathscr{Y}}(\mathscr{U})$ for every $\mathscr{Y}$ in S. It is clear that $\Gamma(\mathscr{U}/S)$ is a vector space over the constant field k, and also that if $\mathscr{U}$ divides $\delta, \Gamma(\delta/S) \subset \Gamma(\mathscr{U}/S)$. Also, if S and S^1 are two sets of prime divisors such that $S \subset S^1$, then $\Gamma(\mathscr{U}/S^1) \subset \Gamma(\mathscr{U}/S))$. Finally, $\Gamma(\mathscr{U}/S) = \Gamma(\delta/S)$ if $\mathscr{U}\delta^{-1}$ contains no $\mathscr{Y}$ belonging to S with a non-zero exponent.

If S is a set of prime divisor which is fixed in a discussion and $\mathscr{U}$ a divisor, we shall denote by $\mathscr{U}_\circ$ the new divisor got from $\mathscr{U}$ by omitting all $\mathscr{Y}$ which do not occur in S: $\mathscr{U}_\circ = \prod\limits_{\mathscr{Y} \in S} \mathscr{Y}^{v_{\mathscr{Y}}(\mathscr{U})}$

Theorem. *Let S be a finite set of prime divisors and $\mathscr{U}, \delta$ two divisors such that $\mathscr{U}$ divides δ. Then,*

$$\dim_k \frac{\Gamma(\mathscr{U}/S)}{\Gamma(\delta/S)} = d(\delta_\circ) - d(\mathscr{U}_\circ) = d(\delta_\circ \mathscr{U}_\circ^{-1}).$$

27 *Proof.* By our remark above, we may assume that $\mathscr{U} = \mathscr{U}_\circ$ and $\delta = \delta_\circ$.

Moreover, it is clearly sufficient to prove the theorem when $\delta = \mathscr{U}\mathscr{Y}$, where $\mathscr{Y}$ is a prime divisor belonging to S. For, if $\delta = \mathscr{U}\mathscr{Y}_1..\mathscr{Y}_n$ we have

$$\dim_k \frac{\Gamma(\mathscr{U}/S)}{\Gamma(\delta/S)} = \dim_k \frac{\Gamma(\mathscr{U}/S)}{\Gamma(\mathscr{U}\mathscr{Y}_1/S)} + \dim_k \frac{\Gamma(\mathscr{U}\mathscr{Y}_1/S)}{\Gamma(\mathscr{U}\mathscr{Y}_1\mathscr{Y}_2/S)} + \cdots + \dim_k \frac{\Gamma(\mathscr{U}_{\mathscr{Y}_1 \cdots \mathscr{Y}_{n-1}}/S}{\Gamma(\delta/S)}$$

and $d(\delta) - d(\mathscr{U}) = d(\mathscr{Y}_1) + d(\mathscr{Y}_2) + \cdots + d(\mathscr{Y}_n)$. □

Hence, we have to prove that if $\mathscr{U}$ is a divisor such that all the prime divisors occurring in it with non-zero exponents are in S, and $\mathscr{Y}$

any prime divisor in S, we have

$$\dim_k \frac{\Gamma(\mathscr{U}/S)}{\Gamma(\mathscr{U}\mathscr{Y}/S)} = f_{\mathscr{Y}} = f.$$

By the theorem on independence of valuations, we may choose an element $u \in K$ such that 28

$$v_{\mathscr{U}}(u) = v_{\mathscr{U}}(\mathscr{U}) \text{ for all } \mathscr{U} \text{ in } S.$$

If $X_1, X_2, \ldots X_{f+1}$ are any $f+1$ elements of $\Gamma(\mathscr{U}/S)$, the elements $X_1 u^{-1}, \ldots X_{f+1} u^{-1}$ are all in $\mathscr{U}_{\mathscr{Y}}$. But since the degree of $k_{\mathscr{U}} = \mathscr{O}_{\mathscr{Y}/\mathscr{Y}}$ over k is f, we have

$$\sum_{i=1}^{f+1} a_i X_i u^{-1} \in \mathscr{Y}, a_i \in k, \text{ not all } a_i \text{ being zero .}$$

Hence, $\sum\limits_{i=1}^{f+1} a_i X_i \in \Gamma(\mathscr{U}\mathscr{Y}/S), a_i \in k$, not all a_i being zero, thus proving that the dimension over k of the quotient $\dfrac{\Gamma(\mathscr{U}/S)}{\Gamma(\mathscr{U}\mathscr{Y}/S)}$ is $\leq f$.

Now, suppose $Y_1, \ldots Y_f$ are f elements of $\mathscr{O}_{\mathscr{Y}}$such that they are linearly independent over k modulo $\mathscr{Y}$. Choose$Y_i^1 \in K$ such that

$$v_{\mathscr{Y}}(Y_i^1 - Y_i) > 0, v_{\mathscr{U}}(Y_i^1) \geq 0 \text{ for } \mathscr{U} \neq \mathscr{Y}, \mathscr{U} \in S.(i = 1, f).$$

By the first condition, $Y_i^1 \equiv Y_i(\mod \mathscr{Y})$, and hence Y_i and Y_i^1 determine the same element in $k_{\mathscr{Y}}$. But by the second condition, the elements uY_i^1 belong to $\Gamma(\mathscr{U}/S)$, and since $Y_1, \ldots Y_f$ are linearly independent $\mod \mathscr{Y}$, no linear combination of $uY_1^1, \ldots uY_f^1$ with coefficients in k- at least one of which is non-zero-can lie in $\Gamma(\mathscr{U}\mathscr{Y}/S)$. Thus, $\dim_k \dfrac{\Gamma(\mathscr{U}/S)}{\Gamma(\mathscr{U}\mathscr{Y}/S)} \geq f$.

This proves our theorem.

Lecture 6

10 The Space $L(\mathscr{U})$

Let $\mathscr{U}$ be any divisor of an algebraic function field K. 29

We shall denote by $L(\mathscr{U})$ the set of all elements of K which are divisible by $\mathscr{U}$. Clearly $L(\mathscr{U}) = \Gamma(\mathscr{U}/S)$ if S is the set of all prime divisors of K, and thus we deduce that $L(\mathscr{U})$ is a vector space over k and if $\mathscr{U}$ divides $\delta, L(\mathscr{U}) \supset L(\delta)$. We now prove the following important

Theorem. *For any divisor $\mathscr{U}$, the vector space $L(\mathscr{U})$ is finite dimensional over k. If we denote its dimension by $l(\mathscr{U})$, and if $\mathscr{U}$ divides δ, we have*

$$l(\mathscr{U}) + d(\mathscr{U}) \leq l(\delta) + d(\delta).$$

Proof. Let S be the set of prime divisors occurring in $\mathscr{U}$ or δ.

Then, it easy to see that

$$L(\delta) = L(\mathscr{U}) \cap \Gamma(\delta/S)$$

Hence, by Noether's isomorphism theorem,

$$\frac{L(\mathscr{U})}{L(\delta)} = \frac{L(\mathscr{U})}{L(\mathscr{U}) \cap \Gamma(\delta/S)} \simeq \frac{L(\mathscr{U}) + \Gamma(\delta/S)}{L(\delta/S)} \subset \frac{L(\mathscr{U}/S)}{\Gamma(\delta/S)},$$

and therefore, $\quad \dim_k \dfrac{L(\mathscr{U})}{L(\delta)} \leq \dim_k \dfrac{\Gamma(\mathscr{U}/S)}{\Gamma(\delta/S)} = d(\delta) - d(\mathscr{U})$

Now, choose for δ any integral divisor which is a multiple of $\mathscr{U}$ and is not the unit divisor $\mathfrak{n}$. Then, $L(\delta) = (0)$; for if X were a non-zero element of $L(\ \ )$, it cannot be a constant since $v_{\mathscr{Y}}(X) \geq v_{\mathscr{Y}}(\delta) > 0$ for

at least one $\mathscr{Y}$, and it cannot be transcendental over k since $v_{\mathscr{Y}}(X) \geq$ **30**
$v_{\mathscr{Y}}(\delta) \geq 0$ for all $\mathscr{Y}$. □

This is not possible. This together with the above inequality proves that $\dim_k L(\mathscr{U}) = l(\mathscr{U}) < \infty$, and our theorem is completely proved.

Since $L(\mathscr{N})$ clearly contains only the constants, $l(\mathscr{N}) = 1$.

11 The Principal Divisors

We shall now associate to every non-zero element of K a divisor. For this, we need the

Theorem. *Let $X \in K^*$. Then there are only a finite number of prime divisors $\mathscr{Y}$ with $v_{\mathscr{Y}}(X) \neq 0$.*

Proof. If $X \in k, v_{\mathscr{Y}}(X) = 0$ for all $\mathscr{Y}$ and the theorem is valid.

Hence assume that X is transcendental over k. Let $[K : k(X)] = N$. Suppose $\mathscr{Y}_1, \ldots \mathscr{Y}_n$ are prime divisors for which $v_{\mathscr{Y}_i}(X) > 0$. Let $\delta = \prod\limits_{i=1}^{n} \mathscr{Y}_i v_{\mathscr{Y}_i}(X)$, and $S = \{\mathscr{Y}_1, \ldots \mathscr{Y}_n\}$. □

Then, $\dim_k \frac{\Gamma(\mathscr{N}/S)}{\Gamma(\delta/S)} = (\delta) = \sum\limits_{i=1}^{n} f_{\mathscr{Y}_i} v_{\mathscr{Y}_i}(X)$. We shall show that this is at most equal to N.

Let in fact $Y_1, \ldots, Y_{N+1}$ be any $(N + 1)$ elements of $\Gamma(\mathscr{N}/S)$. Since $[K : k(X)] = N$, we should have $\sum\limits_{j=1}^{N+1} f_j(X)Y_j = 0$, $f_j(X) \in k[X]$, with at least one f_j having a non-zero constant term. Writing $f_j(X) = a_j + Xg_j(X)$, the above relation may be rewritten as $\sum\limits_{1}^{N+1} a_j Y_j = -X \sum\limits_{1}^{N+1} g_j$ $(X)Y_j$, not all aj being zero, and hence

$$v_{\mathscr{Y}_v}\left(\sum_{1}^{N+1} a_j Y_j\right) = v_{\mathscr{Y}_v}(X) + v_{\mathscr{Y}_v}\left(\sum_{1}^{N+1} g_j(X)Y_j\right) \geq v_{\mathscr{Y}_v}(X)$$

31

This proves that $\sum\limits_{1}^{N+1} a_j Y_j \in \Gamma(\delta/S)$, and therefore

$$n \leq \sum_{i=1}^{n} f_{\mathscr{Y}_i} v_{\mathscr{Y}_i}(X) = d(\delta) = \dim_k \frac{\Gamma(\mathscr{N}/S)}{\Gamma(\delta/S)} \leq N,$$

By considering $\dfrac{1}{X}$ instead of X, we deduce that the number of prime divisors $\mathscr{Y}$ for which $v_{\mathscr{Y}}(X) < 0$ is also finite, and our theorem follows.

The method of defining *the divisor* (X) corresponding to an element $X \in K^*$ is now dear. We define the *numerator* $\mathfrak{z}_X$ of X to be the divisor $\prod\limits_{v_{\mathscr{Y}}(X)>0} \mathscr{Y} v_{\mathscr{Y}}(X)$ (the product being taken over all $\mathscr{Y}$ for which $v_{\mathscr{Y}}(X) > 0$), the *denominator* $\mathscr{N}_X$ of X to be the divisor $\prod\limits_{v_{\mathscr{Y}}(X)<0} \mathscr{Y}^{-v_{\mathscr{Y}}(X)}$, and the *principal divisor* (X) *of* X to be $\prod\limits_{v_y(X)\neq 0} \mathscr{Y}^{v_{\mathscr{Y}}(X)} = \dfrac{\mathfrak{z}_X}{\mathscr{N}_X}$.

If $X, Y \in K^*$, clearly $(XY) = (X)(Y)$ and $(X^{-1}) = (X)^{-1}$. Thus, the principal divisors form a subgroup $\mathscr{Z}$ of the group of divisors ϑ. The quotient group $\Re = \dfrac{\vartheta}{\mathscr{Z}}$ is called *the group of divisor classes*. The following sequence of homomorphisms is easily seen to be exact (i.e., the image of a homomorphism is equal to the kernel of the next).

$$1 \to k^* \to K^* \to \vartheta \to \Re \to 1.$$

In the course of the proof of the above theorem, we proved the inequalities $d(\mathscr{N}_x) \leq N, d(\mathfrak{z}_x) \leq N$, for a transcendental X, where $[K : k(X)] = N$.

We will now show that equality holds 32

Theorem . *Let X be a transcendental element of K, and put $N = [K : k(X)]$. Then,*

$$d(\mathfrak{z}_X) = d(\mathscr{N}_X) = N.$$

In order to prove the theorem, we shall first prove a lemma. We shall say that $Y \in K$ is an *integral algebraic function* of X, if it satisfies a relation

$$Y^m + f_{m-1}(X)Y^{m-1} + - + f_o(X) = o,\ f_i(X) \in k[X].$$

We then have the

Lemma. *If Y is an integral algebraic function of X, and a prime divisor $\mathscr{Y}$ does not divide $\mathscr{N}_X$, it does not divide $\mathscr{N}_Y$.*

Proof. Since $\mathscr{Y}$ does not divide $\mathscr{N}_X, v_{\mathscr{Y}}(X) \geq 0$, and hence

$$mv_{\mathscr{Y}}(Y) = v_{\mathscr{Y}}(Y^m) = v_{\mathscr{Y}}(f_{m-1}(X)Y^{m-1} + \cdots + f_0(X)) \geq \min_{\nu=0}^{m-1}(\gamma v_{\mathscr{Y}}(Y)) = \nu_0 v_{\mathscr{Y}}(Y),$$

for some ν_0 such that $0 \leq \nu_0 \leq m-1$. This proves that $(m-\nu_0)v_{\mathscr{Y}}(Y) \geq 0, v_{\mathscr{Y}}(Y) \geq 0$, and therefore $\mathscr{Y}$ does not divide $\mathscr{N}_Y$. Now, let Y be any element of K satisfying the equation

$$f_m(X)Y^m + \cdots + f_0(X) = 0$$

Then, the element $Z = f_m(X)Y$ satisfying the equation

$$Z^m + g_{m-1}(X)Z^{m-1} + \cdots + g_o(X) = 0,$$

33 where $g_k(X) = f_k(X)f_m^{m-k-1}(x)$, and hence Z is an integral function of X □

Suppose then that $Y_1, \ldots Y_N$ is a basis of $K/k(X)$. By the above remark, we any assume that the Y_i are integral functions of X. The elements $X^iY_j(i = 0, \ldots t; j = 1, \ldots N)$ are then linearly independent over k, for any non-negative integer t. By the above lemma, we can find integer s such that $\mathscr{N}_X^s(Y_j)$ are integral divisors. Hence, $\mathscr{N}_X^{s+t}(X^i)(Y_j)$ is an integral divisor for $(i = 0, \ldots t, j = 1, \ldots N)$, which implies that X^iY_j are elements of $L(\mathscr{N}_X^{-s-t})$. Since these are linearly independent and $N(t+1)$ in number, we obtain

$$N(t+1) \leq 1(\mathscr{N}_X^{-s-t}) \leq l(\mathscr{N}) + d(\mathscr{N}) - d(\mathscr{N}_X^{-s-t}) = 1 + (s+t)d(\mathscr{N}_x),$$

the latter inequality holding because $\mathscr{N}_X^{-s-t}$ divides $\mathscr{N}$.

Thus, $d(\mathscr{N}_X) \geq \dfrac{Nt+N-1}{s+t} \to N$ as $t \to \infty$, which taken together with the opposite inequality we proved earlier shows that $d(\mathscr{N}_X) = N$.

It is clearly sufficient to show that $d(\mathscr{N}_X) = N$, since the other follows on replacing X by $\dfrac{1}{X}$ and observing that $k(X) = k(1/X)$.

Corollary 1. *If $X \in K^*$, $d((X)) = 0$. This is clear when X is a constant. If X be a variable, $d((X)) = d(\mathfrak{z}_X) - d(\mathscr{N}_X) = N - N = 0$. Hence we get the exact sequence*

$$1 \to k^* \to K^* \to \vartheta \to \mathfrak{R}_0 \to 1,$$

where ϑ_0 is the group of divisor of degree zero and $\mathfrak{R}_0 = \dfrac{\vartheta_0}{\mathscr{Z}}$ is the group of divisor classes of degree zero.

Corollary 2. *Suppose $C \in \mathfrak{R}$ is a class of divisors. IF $\mathscr{U}, \delta$ are two divisors of this class, there exists an $X \in K^*$ such that $\mathscr{U} = (X)\delta$. Hence, $d(\mathscr{U}) = d((X)) + d(\delta) = d(\delta)$, and therefore we may define the degree $d(C)$ of the class C to be the degree of any one of its divisors.* 34

Corollary 3. *If X is any transcendental element, there exists an integer Q dependent only on X such that for all integral m, we have*

$$l(\mathscr{N}_X^{-m}) + d(\mathscr{N}_X^{-m}) \geq -Q.$$

Proof. We saw in the course of the proof of the theorem that for $t \geq 0$,

$$l(\mathscr{N}_X^{-s-t}) \geq N(t+1) = d(\mathscr{N}_X)(t+1),$$

and writing $m = s + t$, we obtain for $m \geq s$,

$$l(\mathscr{N}_X^{-m}) + d(\mathscr{N}_X^{-m}) \geq (1-s)d(\mathscr{N}_X) = -Q.$$

For $m < s$, since $\mathscr{N}_X^{-s}$ divides $\mathscr{N}_X^{-m}$, we have

$$l(\mathscr{N}_X^{-m}) + d(\mathscr{N}_X^{-m}) \geq l(\mathscr{N}_X^{-s}) + d(\mathscr{N}_X^{-s}) \geq -Q.$$

□

Lecture 7

12 The Riemann Theorem

In the last lecture, we saw that if X is any element of K, the integer 35 $l(\mathscr{N}^{-m}) + d(\mathscr{N}_X^{-m})$ remains bounded below as m runs through all integral values. We now prove the following stronger result, known as Riemann's theorem.

Theorem. *Let X be any transcendental element of K and $(1-g)$ the lower bound of $l(\mathscr{N}_X^{-m}) + d(\mathscr{N}_X^{-m})$. Then, for any divisor $\mathscr{U}$,*

$$l(\mathscr{U}) + d(\mathscr{U}) \geq 1 - g.$$

Proof. Let $\mathscr{U} = \mathscr{U}_1 \mathscr{U}_2^{-1}$, where $\mathscr{U}_1$ and $\mathscr{U}_2$ are integral divisors. Then clearly $\mathscr{U}_2^{-1}$ divides $\mathscr{U}$, and we have

$$l(\mathscr{U}) + D(\mathscr{U}) \geq l(\mathscr{U}_2^{-1}) + d(\mathscr{U}_2^{-1}).$$

It is therefore enough to prove the inequality with $\mathscr{U}_2^{-1}$ in the place of $\mathscr{U}$. □

The key to the proof lies in the statement that $l(\delta) + d(\delta)$ is unaltered when we replace δ by $\delta(Z)$, where (Z) is a principal divisor. To prove this, consider the map defined on $L(\delta)$ by

$$Y \in L(\delta) \to YZ$$

This is clearly a k-isomorphism of the vector space $L(\delta)$ onto the vector space $L(\delta(Z))$. This proves that $l(\delta) = l(\delta(Z))$, and since we already know that $d(\delta) = d(\delta(Z))$, our statement follows.

36 Observe now that for any non-negative integer m, we have $l(\mathscr{N}_X^{-m}\mathscr{U}_2) + d(\mathscr{N}_X^{-m}\mathscr{U}_2) \geq l(\mathscr{N}_X^{-m}) + d(\mathscr{N}_X^{-m}) \geq l - g$. Since X is transcendental, $d(\mathscr{N}_X) > 0$ and it follows that for large enough m,

$$l(\mathscr{N}_X^{-m}\mathscr{U}_2) \geq md(\mathscr{N}_X - d(\mathscr{U}_2) + l - g > 0$$

For such an m therefore, there exists a non-zero element Z in $L(\mathscr{N}_X^{-m}\mathscr{U})$. This clearly means that the divisor $(Z)\mathscr{N}_X^{m}\ \mathscr{U}_2^{-1}$ is integral, or that $\mathscr{N}_X^{-m}$ divides $(Z)\mathscr{U}_2^{-1}$. Hence, we deduce that

$$\begin{aligned} l(\mathscr{U}_2^{-1}) + d(\mathscr{U}_2^{-1}) &= l((Z)\mathscr{U}_2^{-1}) + d((Z)\mathscr{U}_2^{-1}) \\ &\geq 1(\mathscr{N}_X^{-m}) + d(\mathscr{N}_X^{-m}) \geq l - g \end{aligned}$$

which proves our theorem.

The integer g is called the *genus* of the field. Since

$$1 + 0 = l(\mathscr{N}) + d(\mathscr{N}) \geq 1 - g,$$

it follows that g is always non-negative. The integer $\delta(\mathscr{U}^{-1}) = l(\mathscr{U}) + d(\mathscr{U}) + g - 1$, which is non-negative by the above theorem, is called the *degree of speciality* of the divisor $\mathscr{U}$. We say that $\mathscr{U}$ is a *non-special* or *special* divisor according as $\delta(\mathscr{U}^{-1})$ is or is not equal to zero. We shall interpret $\delta(\mathscr{U}^{-1})$ later. Incidentally, we have proved that if $\mathscr{U}$ is any divisor and $X \in K^*$, the dimensions of the spaces $L(\mathscr{U}(X))$ and $L(\mathscr{U})$ are the same.

This enables us to define the *dimension of a divisor classC*. Choose any element $\mathscr{U}^{-1}$ in C and define the dimension $N(C)$ of C to be $l(\mathscr{U})$. By the remark, this is independent of the choice of $\mathscr{U}^{-1}$ in C.

13 Repartitions

37 We now consider the following question, to which we are led naturally by the theorem of §7. If for every place $\mathscr{Y}$ of K, we are given an element $X_{\mathscr{Y}}$ of K, can we find an X in K such that $v_{\mathscr{Y}}(X - X_{\mathscr{Y}}) \geq 0$ holds for every $\mathscr{Y}$? A necessary condition for such an X to exist is that $v_{\mathscr{Y}}(X_{\mathscr{Y}}) \geq 0$ for all but a finite number of $\mathscr{Y}$. For, suppose $v_{\mathscr{Y}}(X_{\mathscr{Y}}) < 0$ for some $\mathscr{Y}$. Then, since $v_{\mathscr{Y}}(X - X_{\mathscr{Y}}) \geq 0$,

$$v_{\mathscr{Y}}(X) = v_{\mathscr{Y}}(X - X_{\mathscr{Y}} + X_{\mathscr{Y}}) = \min(v_{\mathscr{Y}}(X - X_{\mathscr{Y}}), v_{\mathscr{Y}}(X_{\mathscr{Y}})) = v_{\mathscr{Y}}(X_{\mathscr{Y}}) < O,$$

and this can hold for at most a finite number of $\mathscr{Y}$. We now make the following

Definition. *A* repartition $\mathscr{C}$ *is a mapping* $\mathscr{Y} \to \mathscr{G}_{\mathscr{Y}}$ *of the set of prime divisors* $\mathscr{Y}$ *of K into the field K such that* $v_{\mathscr{Y}}(\mathscr{C}_{\mathscr{Y}}) \geq o$ *for all but a finite number of* $\mathscr{Y}$.

We can define the operations of addition and multiplication in the space $\mathfrak{X}$ of repartitions in an obvious manner. If $\mathscr{C}$ and $\mathscr{G}$ are two repartitions, and a an element of the constant field k,

$$(\mathscr{C} + \mathscr{G})_{\mathscr{Y}} = \mathscr{C}_{\mathscr{Y}} + \mathscr{G}_{\mathscr{Y}}, (\mathscr{C}\mathscr{G})_{\mathscr{Y}} = \mathscr{C}_{\mathscr{Y}}\mathscr{G}_{\mathscr{Y}}, (a\mathscr{C})_{\mathscr{Y}} = a\mathscr{C}_{\mathscr{Y}}.$$

The newly defined mappings are immediately verified to be repartitions. Thus, $\mathfrak{X}$ becomes an algebra over the field k. We can imbed the field K in $\mathfrak{X}$ by defining for every $X \in K$ the repartition $\mathscr{C}_X$ by the equations $(\mathscr{C}_X)_{\mathscr{Y}} = X$ for every $\mathscr{Y}$. The condition for this to be a repartition clearly holds, and one can easily verify that this is an isomorphic **38** imbedding of K in the algebra $\mathfrak{X}$.

We can now extend to repartitions the valuations of the field K by defining for every place $\mathscr{Y}$,

$$v_{\mathscr{Y}}(\mathscr{C}) = v_{\mathscr{Y}}(\mathscr{C}_{\mathscr{Y}}).$$

Clearly, we have the following relations

$$v_{\mathscr{Y}}(\mathscr{C}\mathscr{G}) = v_{\mathscr{Y}}(\mathscr{C}) + v_{\mathscr{Y}}(\mathscr{G})$$
$$v_{\mathscr{Y}}(\mathscr{C} + \mathscr{G}) \geq \min(v_{\mathscr{Y}}(\mathscr{C}), v_{\mathscr{Y}}(\mathscr{G})),$$

and $v_{\mathscr{Y}}(\mathscr{C}_X) = v_{\mathscr{Y}}(X)$

This leads to the notion of the divisibility of a repartition $\mathscr{C}$ by a divisor $\mathscr{U}$. We shall say that $\mathscr{C}$ is *divisible* by $\mathscr{U}$ if $v_{\mathscr{Y}}(\mathscr{C}) \geq v_{\mathscr{Y}}(\mathscr{U})$ for every $\mathscr{Y}$, and that $\mathscr{C}$ and $\mathscr{G}$ are congruent modulo $\mathscr{U}(\mathscr{C} \equiv \mathscr{G}(\mathscr{U})$ in symbols) if $\mathscr{C} - \mathscr{G}$ is divisible by $\mathscr{U}$.

The problem posed at the beginning of this article may be restated in the following generalised form. Given a repartition $\mathscr{C}$ and a divisor $\mathscr{U}$, to find an element X of the field such that $X \equiv \mathscr{C}(\mathscr{U})$. (The original problem is the case $\mathscr{U} = \mathscr{N}$).

If $\mathscr{U}$ is a divisor, let us denote by $\wedge(\mathscr{U})$ the vector space (over k) of all repartitions divisible by $\mathscr{U}$. Then we have the following

Theorem . *If $\mathscr{U}$ and δ are two divisors such that $\mathscr{U}$ divides δ, then $\wedge(\mathscr{U}) \supset \wedge(\delta)$ and*

$$\dim_k \frac{\wedge(\mathscr{U})}{\wedge(\delta)} = d(\delta) - d(\mathscr{U}).$$

39 *Proof.* Let S denote the set of prime divisors occurring in either $\mathscr{U}$ or δ with a non-zero exponent. Since $\dim_k \dfrac{\Gamma(\mathscr{U}/S)}{\Gamma(\delta/S)} = d(\delta) - d(\mathscr{U})$, it is enough to set up an isomorphism of $\dfrac{\Gamma(\mathscr{U}/S)}{\Gamma(\delta/S)}$ onto the space $\dfrac{\wedge(\mathscr{U})}{\wedge(\delta)}$. □

If $x \in \Gamma(\mathscr{U}, /S)$, define a repartition $\mathscr{G}_x$ as follows:

$$(\mathscr{G}_X)_{\mathscr{Y}} = \begin{cases} X & \text{if } \mathscr{Y} \in S \\ 0 & \text{if } \mathscr{Y} \notin S \end{cases}$$

Clearly, $\mathscr{G}_X \in \wedge(\mathscr{U})$, and $X \to \mathscr{G}_X$ is a k-homomorphism of $\Gamma(\mathscr{U}/S)$ into $\wedge(\mathscr{U})$. The image of an element $X \in \Gamma(\mathscr{U}/S)$ lies in $\wedge(\delta)$ if and only if $v_{\mathscr{Y}}(X) \geq v_{\mathscr{Y}}(\delta)$ for every $\mathscr{Y} \in S$, i.e., if and only if $X \in \Gamma(\delta/S)$. Thus, we have an isomorphism of $\dfrac{\Gamma(\mathscr{U}/S)}{\Gamma(\delta/S)}$ into $\dfrac{\wedge(\mathscr{U})}{\wedge(\delta)}$. We shall show that this is onto. Given any repartition $\mathscr{C} \in \wedge(\mathscr{U})$, find $X \in K$ such that

$$v_{\mathscr{Y}}(X - \mathscr{C}) \geq v_{\mathscr{Y}}(\delta) \text{ for every } \mathscr{Y} \in S.$$

This means that the repartition $\mathscr{G}_X - \mathscr{C}$ is an element of $\wedge(\delta)$. Also, the above condition implies that for $\mathscr{Y} \in S$, $v_{\mathscr{Y}}(X) \geq \min(v_{\mathscr{Y}}(\mathscr{C}), v_{\mathscr{Y}}(\delta)) \geq v_{\mathscr{Y}}(\mathscr{U})$. Thus, X is an element of $\Gamma(\mathscr{U}/S)$ and its image in $\dfrac{\wedge(\mathscr{U})}{\wedge(\delta)}$ is the coset $\mathscr{C} + \wedge(\delta)$. Our theorem is thus proved.

Lecture 8

14 Differentials

In this article, we wish to introduce the important notion of a differential 40
of an algebraic function field. As a preparation, we prove the

Theorem. *If $\mathscr{U}$ and δ are two divisors and $\mathscr{U}$ divides δ, then*

$$\dim_k \frac{\wedge(\mathscr{U})+K}{\wedge(\delta)+K} = (l(\delta)+d(\delta)) - (l(\mathscr{U})+d(\mathscr{U}))$$

and
$$\dim_k \frac{\mathfrak{X}}{\wedge(\mathscr{U})+K} = \delta(\mathscr{U}^{-1}) = l(\mathscr{U})+d(\mathscr{U})+g-1.$$

Proof. We have

$$\frac{\wedge(\mathscr{U})+K}{\wedge(\delta)+K} = \frac{\wedge(\mathscr{U})+(\wedge(\delta)+K)}{\wedge(\delta)+K} \simeq \frac{\wedge(\mathscr{U})}{(\wedge(\delta)+K)\cap\wedge(\mathscr{U})}$$

But it is easily verified that $(\wedge(\delta)+K)\cap\wedge(\mathscr{U}) = \wedge(\delta)+L(\mathscr{U})$. Hence, we obtain

$$\frac{\wedge(\mathscr{U})+K}{\wedge(\delta)+K} \simeq \frac{\wedge(\mathscr{U})}{\wedge(\delta)+L(\mathscr{U})} \ \frac{\wedge(\mathscr{U})/\wedge(\delta)}{\wedge(\delta)+L(\mathscr{U})/\wedge(\delta)}$$
$$\frac{\wedge(\mathscr{U})/\wedge(\delta)}{L(\mathscr{U})/L(\mathscr{U})\cap\wedge(\delta)} = \frac{\wedge(\mathscr{U})/\wedge(\delta)}{L(\mathscr{U})/L(\delta)}$$

Thus,

$$\dim_k \frac{\wedge(\mathscr{U})+K}{\wedge(\delta)+K} = \dim_k \frac{\wedge(\mathscr{U})}{\wedge(\delta)} - \dim_k \frac{L(\mathscr{U})}{L(\delta)}$$

$$= (d(\delta) - d(\mathscr{U})) - (l(\mathscr{U}) - l(\delta)) = (l(\delta) + d(\delta)) - (l(\mathscr{U}) + d(\mathscr{U})),$$

41 which is the first part of the theorem. □

Now, choose a divisor $\mathfrak{L}$ such that

$$l(\mathfrak{L}) + d(\mathfrak{L}) = 1 - g.$$

Putting $\mu_{\mathscr{Y}} = \min(v_{\mathscr{Y}}(\delta), v_{\mathscr{Y}})$, and $\mathscr{U} = \prod\limits_{\mathscr{Y}} \mathscr{Y}^{\mu_{\mathscr{Y}}}$, we see that $\mathscr{U}$ divides both δ and $\mathfrak{L}$. Hence

$$1 - g \leq l(\mathscr{U}) + d(\mathscr{U}) \leq l(\mathfrak{L}) + d(\mathfrak{L}) = 1 - g,$$

and hence

$$l(\mathscr{U}) + d(\mathscr{U}) = 1 - g.$$

Moreover, we have

$$\dim_k \frac{\mathfrak{X}}{\wedge(\delta) + K} \geq \dim_k \frac{\wedge(\mathscr{U}) + K}{\wedge(\delta) + K} = l(\delta) + d(\delta) - 1 + g = \delta(\delta^{-1}).$$

To prove the opposite inequality, suppose $\mathscr{C}_1, \ldots \mathscr{C}_m$ are m linearly independent elements of $\mathfrak{X}$ over k module $\wedge(\delta) + K$. If we put $v_{\mathscr{Y}} = \min\limits_i(v_{\mathscr{Y}}(\mathscr{C}_i), v_{\mathscr{Y}}(\delta))$ and $\mathscr{U} = \prod\limits_{\mathscr{Y}} \mathscr{Y}^{\gamma_{\mathscr{Y}}}$, clearly all the $\mathscr{C}_i$ lie in $\wedge(\mathscr{U})$. We deduce that

$$m \leq \dim_k \frac{\wedge(\mathscr{U}) + K}{\wedge(\delta) + K} = (l(\delta) + d(\delta)) - (l(\mathscr{U}) + d(\mathscr{U})) \leq l(\delta) + d(\delta) - 1 + g,$$

which proves that $\dim_k \dfrac{\mathfrak{X}}{\wedge(\delta) + K}$ is finite and $\leq \delta(\delta^{-1})$. The second part of the theorem is therefore proved.

Definition. *A* differential ω *is a linear mapping of* $\mathfrak{X}$ *into* k *which vanishes on some sub space of the form* $\wedge(\mathscr{U} + K)$.

In this case, ω is said to be *divisible* by $\mathscr{U}^{-1}.\omega$ is said to be of the *first kind* if it is divisible by $\mathscr{N}$

42 If δ divides $\mathscr{U}$, clearly $\wedge(\delta^{-1}) + K \subset \wedge(\mathscr{U}^{-1}) + K$, and therefore every differential divisible by $\mathscr{U}$ is also divisible by δ.

Consider now the set $D(\mathscr{U})$ of differentials ω of K which are divisible by $\mathscr{U}$. This is the dual of the finite dimensional vector space $\mathfrak{X}/_{\wedge(\mathscr{U}^{-1})+K}$, and therefore becomes a vector space over k of dimension

$$\dim_k D(\mathscr{U}) = \dim_k \frac{\mathfrak{X}}{\wedge(\mathscr{U}^{-1}) + K} = \delta(\mathscr{U}).$$

If ω_1 and ω_2 are two differentials divisible by $\mathscr{U}_1$ and $\mathscr{U}_2$ respectively, their sum is a linear function on $\mathfrak{X}$ which clearly vanishes on $\wedge(\mathscr{U}^{-1})+K$, where $\mathscr{U}$ is $(\mathscr{U}_1, \mathscr{U}_2)$. (The *greatest common divisor* (g.c.d.) of two divisors $\mathscr{U}_1$ and $\mathscr{U}_2$ is the divisor $\mathscr{U} = \prod\limits_{\mathscr{Y}} \mathscr{Y}^{\min(v_{\mathscr{Y}}(\mathscr{U}_1), v_{\mathscr{Y}}(\mathscr{U}_2))}$.) Thus, $\omega_1 + \omega_2$ is a differential divisible by $\mathscr{U}$. Similarly, for a differential ω divisible by $\mathscr{U}$ and an element $X \in K$, we define the differential $X\omega$ by

$$X\omega(\mathscr{C}) = \omega(X\mathscr{C}).$$

$X\omega$ is seen to be divisible by $(X)\mathscr{U}$. We then obtain

$$\begin{aligned} (XY)\omega &= X(Y\omega) \\ (X + Y)\omega &= X\omega + Y\omega \\ X(\omega_1+\omega_2) &= X\omega_1 + X\omega_2 \end{aligned}$$

It follows that the differentials form a vector space over K. We now prove the

Theorem. *If ω_0 is a non-zero differential, every differential can be written uniquely in the form $\omega = X\omega_0$ for some $X \in K$. In other words, the dimension over K of the space of differentials of K is one.* 43

Proof. Let ω_0 be divisible by δ_0^{-1} and ω by δ^{-1}. Let $\mathscr{U}$ be an integral divisor, to be chosen suitably later. The two mappings

$$X_0 \in L(\mathscr{U}^{-1}\delta_0) \to X_0\omega_0 \in D(\mathscr{U}^{-1})$$

and

$$X \in L(\mathscr{U}^{-1}\delta) \to X\omega \in D(\mathscr{U}^{-1})$$

are clearly k-isomorphisms of $L(\mathscr{U}^{-1}\delta_0)$ and $L(\mathscr{U}^{-1}\delta)$ respectively into $D(\mathscr{U}^{-1})$. Hence, the sum of the dimensions of the images in $D(\mathscr{U}^{-1})$. is

$$l(\mathscr{U}^{-1}\delta_0) + l(\mathscr{U}^{-1}\delta) \geq 2d(\mathscr{U}) - d(\delta) - d(\delta_0) + 2 - 2g,$$

and is therefore $> \dim D(\mathscr{U}^{-1}) = \delta(\mathscr{U}^{-1}) = d(\mathscr{U})+g-1$ if $\mathscr{U}$ is chosen so that $d(\mathscr{U})$ is sufficiently large. With such a choice of $\mathscr{U}$, therefore, we see that the images must have a non-zero intersection in $D(\mathscr{U}^{-1})$. Hence, for some X_0 and X different from zero, we must have

$$X_0\omega_0 = X\omega, \omega = X_0X^{-1}\omega_0 = Y\omega_0, Y \in K.$$

The uniqueness is trivial. □

We shall now associate with every differential ω a divisor. We require a preliminary

Lemma. *If a differential ω is divisible by two divisors $\mathscr{U}$ and δ, it is* 44 *also divisible by the least common multiple $\mathscr{L}$ of $\mathscr{U}$ and δ (Definition of l.c.m. obvious).*

Proof. Suppose $\mathscr{C} \in \wedge(\mathfrak{L}^{-1})$. Then,

$$v_{\mathscr{Y}}(\mathscr{C}) \geq -v_{\mathscr{Y}}(\mathfrak{L}) = -\max(v_{\mathscr{Y}}(\mathscr{U}), v_{\mathscr{Y}}(\mathfrak{z})).$$

Define two repartitions $\mathscr{C}^1$ and $\mathscr{C}''$ by the equations

$$\begin{aligned}
\mathscr{C}^1_{\mathscr{Y}_1} &= \mathscr{C}_{\mathscr{Y}}, \mathscr{C}''_{\mathscr{Y}} = 0 \text{ for all } \mathscr{C} \text{ such that } v_{\mathscr{Y}}(\mathscr{U}) \geq v_{\mathscr{Y}}(\delta)\\
\mathscr{C}^1_{\mathscr{Y}} &= 0, \mathscr{C}''_{\mathscr{Y}} = \mathscr{C}_{\mathscr{Y}} \text{ for all } \mathscr{Y} \text{ such that } v_{\mathscr{Y}}(\mathscr{U}) < v_{\mathscr{Y}}(\delta).
\end{aligned}$$

$\mathscr{C}^1$ and $\mathscr{C}''$ are by the above definition divisible by $\mathscr{U}^{-1}$ and $\mathscr{Y}^{-1}$ respectively, and $\mathscr{C} = \mathscr{C}^1 + \mathscr{C}''$. Hence,

$$\omega(\mathscr{C}) = \omega(\mathscr{C}^1) + \omega(\mathscr{C}'') = 0.$$

Since ω must vanish on K, ω must vanish on $\wedge(\mathfrak{L}^{-1})+K$. Our lemma follows □

Theorem. *To any differential $\omega \neq 0$, there corresponds a unique divisor (ω) such that ω is divisible by $\mathscr{U}$ if and only if (ω) is divisible by $\mathscr{U}$.*

Proof. Suppose ω is divisible by a divisor $\mathscr{U}$. Then, the mapping $X \in L(\mathscr{U}^{-1}) \to X\omega \in D(\mathscr{N})$ is clearly a k-isomorphism of $L(\mathscr{U}^{-1})$ into $D(\mathscr{N})$. Hence, we deduce that

$$l(\mathscr{U}^{-1}) \leq \dim D(\mathscr{N}) = \delta(\mathscr{N}) = l(\mathscr{N}) + d(\mathscr{N}) + g - 1 = g.$$

On other hand, we have

$$l(\mathscr{U}^{-1}) + d(\mathscr{U}^{-1}) = 1 - g + \delta(\mathscr{U}) \geq 2 - g,$$

since $\delta(\mathscr{U}) \geq 1$. Combining these two inequalities, we deduce that

$$d(\mathscr{U}) \leq 2g - 2.$$

45

This proves that the degrees of all divisors dividing a certain differential ω are bounded by $2g - 2$. □

Now, choose a divisor (ω) dividing ω and of maximal degree. If $\mathscr{U}$ were any another divisor of ω, the least common multiple δ of $\mathscr{U}$ and (ω) would have degree at least that of (ω), and would divide ω by the above lemma. Hence, we deduce that $\delta = (\omega)$ or that $\mathscr{U}$ divides (ω).

The uniqueness of (ω) also follows from this. Our theorem is proved.

Corollary 1. *If $X \in K^*, (X\omega) = (X)(\omega)$. This follows from the easily verified fact that $\mathscr{U}$ divides ω if and only if $(X)\mathscr{U}$ divides $X\omega$.*

This corollary, together with the theorem that the space of differentials is one dimensional over K, proves that the divisors of all differentials form a class W. This class is called the *canonical class*

15 The Riemann-Roch theorem

Let C be a class and $\mathscr{U}$ any divisor of C. If $\mathscr{U}_i (i = 1, \ldots, n)$ are elements of $C, \mathscr{U}_i\mathscr{U}^{-1} = (X_i)$ are principal divisors. We shall say that the divisors $\mathscr{U}_i$, are linearly independent if $X_i (i = 1, \ldots, n)$ are linearly independent over k. This does not depend on the choice of $\mathscr{U}$ or of the respectively X_i of $\mathscr{U}_i\mathscr{U}^{-1}$, as is easy to verify. We now prove the

Lemma. *The dimension $N(C)$ of a class C is the maximum number of linearly independent integral divisors of C.* 46

Proof. Let $\mathscr{U}$ be any divisor of C. Then, the divisors $(X_1)\mathscr{U}, (X_2)\mathscr{U}, \ldots$, $(X_n)\mathscr{U}$ are linearly independent integral divisors of C if and only if $X_1, \ldots, X_n$ are linearly independent elements of $L(\mathscr{U}^{-1})$. Our lemma follows. □

We now prove the celebrated theorem of Riemann-Roch.

Theorem. *If C is any divisor class,*

$$N(C) = d(C) - g + 1 + N(WC^{-1}).$$

Proof. Let $\mathscr{U} \in C$. Then,

$$N(C) = l(\mathscr{U}^{-1}) = d(\mathscr{U}) - g + 1 + \delta(\mathscr{U}) = d(C) - g + 1 + \delta(\mathscr{U}).$$

□

But $\delta(\mathscr{U})$ being the dimension of $D(\mathscr{U})$ is the maximum number of linearly independent differentials divisible by $\mathscr{U}$. Hence, it is the maximum number of linearly independent differentials $\omega_1, \ldots, \omega_n$ such that $(\omega_1)\mathscr{U}^{-1}, (\omega_2)\mathscr{U}^{-1}, \ldots, (\omega_n)\mathscr{U}^{-1}$ are integral. By the above lemma, we conclude that $\delta(\mathscr{U}) = N(WC^{-1})$, and our theorem is proved.

Corollaries E and W shall denote principal and canonical classes respectively.

(a) $N(E) = l(n) = 1, d(E) = d(N) = 0.$

$1 = N(E) = d(E) - g + 1 + N(W) \Longrightarrow N(W) = g.$

$g = N(W) = d(W) - g + 1 + N(E) \Longrightarrow d(W) = 2g - 2.$

(b) If $d(C) < 0$, or if $d(C) = 0$ and $C \neq E, N(C) = 0$.

47 If $d(C) > 2g - 2$ or if $d(C) = 2g - 2$ and $C \neq W$,

$$N(C) = d(C) - g + 1$$

Proof. Suppose $N(C) > 0$. Then there exists an integral divisor $\mathscr{U}$ in C, and hence $d(C) = d(\mathscr{U}) \geq 0$, equality holding if and only if $\mathscr{U} = N$ or $C = E$. □

The second part follows immediately on applying that first part to the divisor WC^{-1}.

(c) If W^1 is a class and g^1 an integer such that

$$N(C) = d(C) - g^1 + 1 + N(W^1C^{-1}),$$

We must have $W = W^1$ and $g = g^1$.

Proof. Exactly as in (a), we deduce that $N(W^1) = g^1, d(W^1) = 2g^1 - 2$. Again as in the second part of (b), we deduce that if $d(C) > 2g^1 - 2, N(C) = d(C) - g^1 + 1$. Hence, for $d(C) > \max(2g - 2, 2g^1 - 2)$,

$$N(C) = d(C) - g + 1 = d(C) - g^1 + 1, g = g^1.$$

Hence $N(W^1) = g$ and $d(W^1) = 2g - 2$, and it follows from the second part of (b) that $W = W^1$. □

This shows that the class W and integer g are uniquely determined by the Riemann-Roch theorem.

Let us give another application of the Riemann-Roch theorem. We shall say that a *divisor $\mathscr{U}$ divides a class C* if it divides every integral divisor of C. We then have the following

Theorem. *If C is any class and $\mathscr{U}$ an integral divisor,*

$$N(C) \geq N(C\mathscr{U}) \leq N(C) + d(\mathscr{U})$$

The first inequality becomes an equality if and only if $\mathscr{U}$ divides the class $C\mathscr{U}$, and the second if and only if $\mathscr{U}$ divides the class WC^{-1}.

Proof. Since the maximum number of linearly independent integral divisors in $C\mathscr{U}$ is clearly greater than or equal to the number of such divisors in C, the first part of the inequality follows. Suppose now that 48 equality prevails. Then there exists a maximal set $\delta_1, \ldots \delta_n$ of linearly independent integral divisors in C, such that $\mathscr{U}\delta_1, \ldots \mathscr{U}\delta_n$ forms such a set in $C\mathscr{U}$. But since every integral divisor in $C\mathscr{U}$ is 'linear combination of divisors of such a set' with coefficients in k (in an obvious sense), every integral divisor of $C\mathscr{U}$ is divisible by $\mathscr{U}$. □

Now, by the theorem of Riemann-Roch,

$$N(C\mathscr{U}) = d(C) + d(\mathscr{U}) + 1 - g + N(WC^{-1}\mathscr{U}^{-1}),$$

and the second inequality together with the condition of equality follows by applying the first to $WC^{-1}\mathscr{U}^{-1}$ instead of C.

Corollary. *For any class $C, N(C) \geq$* $\max(0, d(C) + 1)$.

Proof. If N(C) = 0, there is nothing to prove, if $N(C) > 0$, there exists an integral divisor $\mathscr{U}$ in C. Hence we obtain

$$N(C) = N(E\mathscr{U}) \leq N(E) + d(\mathscr{U}) = d(\mathscr{U}) + 1 = d(C) + 1,$$

and our corollay is proved. □

Lecture 9

16 Rational Function Fields

In this lecture, we shall consider some particular function fields and find their canonical class, genus, etc. as illustrations of the general theory. Let us first consider the rational function fields. 49

Let $K = k(X)$ be a rational function field in one variable over k. We shall first show that k is precisely the field of constants of K. For later use, we formulate this in a more general form.

Lemma. *Let K be a purely transcendental extension of a field k. Then k is algebraically closed in K.*

Proof. Let $(x_i)_{i \in I}$ be any transcendence basis of K over k such that $K = k(x_i)$. Since any element of K is a rational combination of a finite number of x_i, we may assume that I is a finite set of integers $(1, \ldots n)$. □

We proceed by induction. Assume first that $n = 1$. Let α be any element of $k(x_1)$ algebraic over k. α may be written in the form $\dfrac{f(x_1)}{g(x_1)}$, where f and g are polynomials over k prime to each other.

We then have

$$f(x_1) - \alpha g(x_1) = 0$$

This proves that if α were not in k, x_1 is algebraic over $k(\alpha)$, (since the above polynomial for x_1 over $K(\alpha)$ cannot vanish identically) and hence over k which is a contradiction. Hence α is in k. 50

Suppose now that the lemma holds for $n - 1$ instead on n. If α were an element of $k(x_1, \ldots x_n)$ algebraic over k, it is algebraic over $k(x_1, \ldots x_{n-1})$. By the first part, it should be the $k(x_1, \ldots x_{n-1})$, and hence by induction hypothesis in k. Our lemma is proved.

Let us return to the rational function field K. We have already seen that the prime divisors are $(i) N_X$, the prime divisor corresponding to $\frac{1}{X}$, and $(ii) \mathscr{Y}_{p(X)}$, the prime divisors corresponding to irreducible polynomials $p(X)$ in $k[X]$. If $f(X)$ is a rational function of X over k having the unique decomposition $p_1^{e_1}(X) \cdots p_r^{e_n}(X)$, the principal divisor $(f(X))$ is clearly given by

$$(f(X)) = \prod_{\nu=1}^{r} \mathscr{Y}_{p_\gamma}^{e_\gamma}(X) N_X^{-\deg f}$$

It follows that the space $L(N_X^{-t})$ for $t \geq 0$ consists precisely of all polynomials of degree $\leq t$, and since there are $t + 1$ such polynomials independent over k, and generating all polynomials of degree $\leq t, (1, X, \ldots X^t$ for example), we deduce that

$$N(N_X^t E) = t + 1.$$

But by the corollary to the Riemann - Roch theorem, if $d(N_X^t E) = td(N_X) = t > 2g - 2$, we should have

$$N(N_X^t E) = d(N_X^t E) + 1 - g = t + 1 - g,$$

51 and hence, $g = 0$. Thus, there are no non-zero differentials of the first kind.

Since $d(N_X^{-2} E) = -2 = 2g - 2 < 0$, it follows that $N(N_X^{-2} E) = 0 = g$. and hence $W = n_X^{-2} E$.

17 Function Fields of Degree Two Over a Rational Function Field

We start with a lemma which will be useful for later calculations.

Lemma. *Let $K/_k$ be any algebraic function field and $X \in K$ any transcendental element. If $R(X) = \dfrac{f_1(X)}{f_2(X)}$ is any rational function of X, then f_1 and f_2 being prime to each other $(R(X)) = \dfrac{\mathfrak{z}f_1}{\mathfrak{z}f_2} N_X^{-\deg R(X)}$ and $\mathfrak{z}_{f_1}$ and $\mathfrak{z}_{f_2}$ are prime to each other and both are prime to N_X. Moreover,* $[k(X) : k(R(X))] = \max(\deg f_1, \deg f_2)$.

Proof. Let $f(X)$ be any polynomial over k of the form

$$f(X) = a_o + a_1 X + \cdots + a_t X^t.$$

If $\mathscr{Y}$ is a prime divisor not dividing N_X, i.e., if $v_{\mathscr{Y}}(X) \geq 0$, we have $v_{\mathscr{Y}}(f(X)) \geq \min\limits_{\nu=o}(\gamma v_{\mathscr{Y}}(X)) \geq o)$. If on the other hand, $\mathscr{Y}$ does occur in N_X, we have $v_{\mathscr{Y}}(X) < o$, and hence

$$v_{\mathscr{Y}}(f(X)) = \min_{\nu=o-t}(\nu v_{\mathscr{Y}}(X)) = t v_{\mathscr{Y}}(X)$$

Thus, we see that $\mathfrak{z}_f$ is prime to N_X and $N_{f(x)} = N_X^t$. □

Hence, if $R(X) = \dfrac{f_1(X)}{f_2(X)}$, where $(f_1, f_2) = 1$, we have

$$(R(X)) = \frac{\mathfrak{z}f_1}{\mathfrak{z}f_2} N_X^{-\deg R(X)}$$

We assert that $\mathfrak{z}_{f_1}$ and $\mathfrak{z}_{f_2}$ are prime to each other. For if not, let $\mathfrak{z}_{f_1}$ 52
and $\mathfrak{z}_{f_2}$ have a prime divisor $\mathscr{Y}$ in common. Then $v_{\mathscr{Y}}(X) \geq o$. Find polynomials g_1 and g_2 such that

$$f_1 g_1 + f_2 g_2 = 1.$$

$$\begin{aligned}\text{Then,}\quad 0 &= v_{\mathscr{Y}}(1) = v_{\mathscr{Y}}(f_1 g_1 + f_2 g_2)\\ &\geq \min(v_{\mathscr{Y}}(f_1) + v_{\mathscr{Y}}(g_1), v_{\mathscr{Y}}(f_2) + v_{\mathscr{Y}}(g_2)) > 0,\end{aligned}$$

a contradiction. Thus, $\mathfrak{z}_{f_1}$ and $\mathfrak{z}_{f_2}$ are prime to each other.

To prove the last part of the lemma, we may assume without loss of generality that $\deg f_1 \geq \deg f_2$ or that $\deg R(X) \geq 0$ (otherwise consider $\dfrac{1}{R(X)}$). It then follows that

$$\mathfrak{z}_{R(X)} = \mathfrak{z}_{f_1(X)}, [k(X) : k(R(X))] = [K : k(R(X))]/[K : k(X)]$$

$$= \frac{d(\mathfrak{z}_{R(X)})}{d(N_X)} = \frac{d(\mathfrak{z}_{f_1(X)})}{d(N_X)} = \frac{d(\mathfrak{z}_{f_1(X)})}{d(N_X)} = \deg f_1.$$

Our lemma is proved.

It follows in particular that $k(x) = k(R(X))$ if and only if $\max(\deg f_1, \deg f_2) = 1$, or $R(X) = \dfrac{\alpha X + \beta}{\gamma X + \delta}, \alpha, \beta, \gamma, \delta \in k$ and $\alpha\delta - \beta\gamma \neq 0$.

Now, let k be a field of characteristic different from 2, X a transcendental element over k and K a field of degree two over $k(X)$ which is not got from an algebraic extension of k (viz., K should not be got by the adjunction to $k(X)$ of elements algebraic over k). Then k is the constant field of K, for if it were not, there exists an element α of K 53 which is algebraic over k but not in k. α cannot lie in $k(X)$, since k is algebraically closed in $k(X)$. Hence, $k(X, \alpha)$ should be an extension of degree at least two over $k(X)$, and should therefore coincide with K. But this contradicts our assumption regarding K.

Now, K can be get the adjunctions to $k(X)$ of an element Y which satisfies a quadratic equation

$$Y^2 + bY + c = 0, b, c \in k(X)$$

Completing the square (note that characteristic $k \neq 2$), we get

$$\left(Y + \frac{b}{2}\right)^2 + \left(c - \frac{b}{4}^2\right) = 0,$$

and hence $k(X, Y) = k(X, Y^1)$ where $Y^1 = Y + \dfrac{b}{2}$ satisfies equation of the form $\gamma^{1^2} = R(X), R(X)$ being a rational function of X. Let $R(X) = \prod\limits_{\nu-1}^{r} p_{\gamma}^{e\gamma}(X)$, where $p_\nu(X)$ are irreducible polynomials in $k[X]$ and e_ν are integers. Putting $e_\nu = 2g_\nu + \epsilon_\gamma$, where g_ν are integers and $\epsilon_\nu = 0$ or 1, and $Y'' = \dfrac{Y^1}{\prod\limits_{\nu} p^{\gamma} g_g amma(X)}$, we see that $k(X, Y) = k(X, Y^{''})$, and $Y^{''}$ satisfies an equation of the form

$$Y''^2 = \prod_{1}^{r} p_{\gamma}^{\epsilon\nu}(X) = D(X),$$

where $D(X)$ is a polynomial which is a product of different irreducible polynomials.

We shall therefore assume without loss in generality that $K = k(X, Y)$ with $Y^2 = D(X)$ of the above form. Let us assume that m is the degree of D.

Now, let σ be the automorphism of K over $k(X)$ which is not the 54 identity. If $Z = R_1(X) + YR_2(X)$ is any element of $K, Z^\sigma = R_1(X) - YR_2(X)$. To every prime divisor $\mathscr{Y}$ of K, let us associate a prime divisor $\mathscr{Y}^\sigma$ by the definition

$$v_{\mathscr{Y}^\sigma}(Z) = v_{\mathscr{Y}}(\sigma^{-1}Z)$$

This can be extended to an automorphism of the group ϑ of divisors (see Lecture 19). We shall denote this automorphism again by σ, and the image of a divisor $\mathscr{U}$ by $\mathscr{U}^\sigma$. Since $X^\sigma = X, N_X^\sigma = N_X$.

Suppose now that $Z = R_1(X) + YR_2(X)$ is any element of $L(N_X^{-t})$ (t any integer). Applying σ, we deduce that $R_1(X) - YR_2(X)$ should also be an element of $L(N_X^{-t})$. Adding, $2R_1(X) \in L(N_X^{-t}), R_1(X) \in L(N_X^{-t})$. If $R_1(X) = \dfrac{f_1(X)}{g_1(X)}$, where f_1 and g_1 are coprime polynomials, we have $(R_1(X)) = \dfrac{\mathfrak{z}_{f_1}}{\mathfrak{z}_{g_1}} N_X^{-\deg R_1}$ divisible by N_X^{-t}, and hence we deduce that $\mathfrak{z}_{g_1} = n$, and $g_1(X)$ is a constant. Hence $R_1(X)$ is a polynomial of degree $\leq t$ (if $t < o, R_1(X) = 0$).

Also, since both Z and Z^σ are in $L(N_X^{-t})$. This implies as before that $R_1^2 - DR_2^2$ is a polynomial of degree $\leq 2t$. Hence DR_2^2 is a polynomial of degree $\leq 2t$, and since D is square free, R_2 is a polynomial of degree $\leq t - \dfrac{m}{2}$.

Conversely, by working back, we see that if R_1 is a polynomial of degree $\leq t$ and R_2 a polynomial of degree $\leq t = \frac{m}{2}$, $Z = R_1 + YR_2 \in$

$L(N_X^{-t})$. Hence, we obtain

$$N(EN_X^t) = l(N_X^{-t}) = \begin{cases} 0 & \text{if } t < 0 \\ t+1 & \text{if } 0 \leq t \leq \frac{m}{2} - 1 \text{ and } m \text{ even} \\ t+1 & \text{if } m \text{ and } 0 \leq t \leq \frac{m-1}{2} \\ 2t+2-\frac{m}{2} & \text{if } m \text{ even and } t \geq \frac{m}{2} \\ 2t+2-\frac{m+1}{2} & \text{if } m \text{ odd and } t \geq \frac{m+1}{2}. \end{cases}$$

55 Since $d(N_X) = [K : k(X)] = 2$, for $t > g-1$, we have $d(EN_X^t) = 2t > 2g-2$ and hence

$$N(EN_X^t) = d(N_X^t) - g + 1 = 2t - g + 1$$

Comparing with the above equations, we deduce that g is $\dfrac{m}{2} - 1$ if m is even and $\dfrac{m-1}{2}$ if m is odd.

Thus, we obtain examples of fields of arbitrary genus over any constant field.

The canonical class of K is EN_X^{g-1}. For,

$$d(N_X^{g-1}E) = 2g - 2,$$

and
$$N(N_X^{g-1}E) = \begin{cases} g-1+1 = g & \text{if } g > 0 \\ 0 = g & \text{if } g = 0. \end{cases}$$

If $gg > o$, there exists a differential ω of the first kind with $(\omega) = N_X^{g-1}$. Then clearly the differentials $\omega, X\omega, \ldots, X^{g-1}\omega$ are all of the first kind and are linearly independent over k, and as they are g in number, they form a base over k for all differentials of the first kind.

18 Fields of Genus Zero

56 We shall find all fields of genus zero over a constant field k.

First, notice that any divisor of degree zero of a field of genus zero is a principal divisor. For let C be a class of degree 0. Then since $d(C) > -2 = 2g-2, N(C) = d(C) - g + 1 = 1$ and therefore $C = E$.

Now,

$$d(W^{-1}) = 2 > 2g - 2, N(W^{-1}) = 2 - g + 1 = 3,$$

and therefore there exists three linearly independent integral divisors $\mathscr{U}_1, \mathscr{U}_2, \mathscr{U}_3$ in the class W^{-1} (incidentally, this proves there exists integral divisors, and consequently prime divisors of degree at most two). Let $\dfrac{\mathscr{U}_1}{\mathscr{U}_2} = (X)$. Then clearly $\mathscr{N}_X$ divides $\mathscr{U}_2$, and hence we obtain

$$[K : k(X)] = d(N_X) \leq d(\mathscr{U}_2) = 2.$$

Thus, any field of genus zero should be either a rational function field or a quadratic extension of a rational function field. We have the following

Theorem . *The necessary and sufficient condition for a field of genus zero to be a rational function field is that it possess a prime divisor of degree* 1.

Proof. If $K = k(X)$, the prime divisor n_X satisfies the requisite condition.

Conversely, let $\mathscr{Y}$ be a prime divisor of degree 1 of K. Then, $N(\mathscr{Y}E) = d(\mathscr{Y}) + 1 = 2$, and therefore there are elements X_1, X_2 in 57
K linearly independent over k such that $X_1\mathscr{Y} = \mathscr{U}_1$ and $X_2\mathscr{Y} = \mathscr{U}_2$ are integral divisors. Thus if $X = \dfrac{X_1}{X_2}, (X) = (\dfrac{X_1}{X_2}) = \dfrac{\mathscr{U}_1}{\mathscr{U}_2}$, and $d(N_X) \leq d(\mathscr{U}_2) = d(\mathscr{Y}) = 1$. But X is not in k, and hence $d(N_X) = 1 = [K : k(X)]$, from which it follows that $K = k(X)$. The theorem is proved. □

19 Fields of Genus One

Let K/k be an algebraic function field of genus 1. Then, since $N(W) = g = 1$ and $d(W) = 2g - 2 = 0$, the canonical class W coincides with the principal class E.

A function field of genus one which contains at least one prime divisor of degree one is called an *elliptic function field.* (The genus being one does not imply that there exists a prime divisor of degree one. In fact, it can be proved easily that the field $R(X, Y)$, where R is the field of real numbers and X, Y transcendental over R and connected by the relation $Y^2 + X^4 + 1 = 0$ has every prime divisor of degree two). Let us investigate the structure of elliptic function fields.

Let $\mathscr{Y}$ be a prime divisor of degree one. Then, since $d(\mathscr{Y}^2) = 2 > 2g - 2 = 0$, we have $l(\mathscr{Y}^{-2}) = 2$. Let $1, X$ be a basis of $L(\mathscr{Y}^{-2})$ over k. Since $X\mathscr{Y}^2$ is integral, N_X divides $\mathscr{Y}^2 . N_X$ cannot be $\mathscr{Y}$, since if it were, we obtain $[K : k(X)] = d(N_X) = d(\mathscr{Y}) = 1, K = k(X)$ and hence $g = 0$. Thus, N_X should be equal to $\mathscr{Y}^2$.

Again, since $l(\mathscr{Y}^{-3}) = 3$, we may complete (l, X) to a basis $(1, X, Y)$ 58 of $L(\mathscr{Y}^{-3})$ over k. N_γ should divide $\mathscr{Y}^3$, and since Y is not an element of $L(\mathscr{Y}^{-2}), N_\gamma$ does not divide $\mathscr{Y}^2$. Thus, $N_\gamma = \mathscr{Y}^3$.

The denominators of $1, X, Y, X^2, XY, X^3$ and Y^2 are respectively N, $\mathscr{Y}^2$, $\mathscr{Y}^3$, $\mathscr{Y}^4, \mathscr{Y}^5, \mathscr{Y}^6$ and $\mathscr{Y}^6$. Since the first six elements have different powers of $\mathscr{Y}$ in the denominator, they are linearly independent elements of $L(\mathscr{Y}^{-6})$. But $l(\mathscr{Y}^{-6}) = 6$, and the seventh element, being in $L(\mathscr{Y}^{-6})$ should therefore be a linear combination of the first six. We thus obtain

$$Y^2 + \gamma XY + \delta Y = \alpha_3 X^3 + \alpha_2 X^2 + \alpha_2 X^2 + \alpha_1 X + \alpha_o, \gamma, \delta, \alpha_i \in k.$$

Now, if Y where a rational function of X, writing $Y = \dfrac{f(X)}{g(X)}$, $f(X)$, $g(X) \in k[X]$, $(f(X), g(X)) = 1$, and substituting in the above equation, we easily deduce that $g(X)$ should be a constant, and that Y should be a polynomial in X of degree ≤ 1. But this would mean that Y is divisible by $\mathscr{Y}^2$, which we have already ruled out. Hence, $[k(X, Y) : k(X)] = 2 = d(N_X) = [K : k(X)]$, and consequently, $K = k(X, Y)$.

If the characteristic of k is different from 2, we may as in §16 find a Z such that $K = k(X, Y)$, with

$$Z^2 = f(X)$$

where $f(X)$ is a cubic polynomial in X with non-repeating irreducible factors.

A partial converse of the above result is valid. Suppose that $K =$ 59 $k(X, Z)$, where X is transcendental over k and Z satisfies an equation of the form $Z^2 = f(X)$, where $f(X)$ is a cubic polynomial which we assume to be irreducible. Let $ch(k) \neq 2$. Then, the genus of K is one, by §16. Also, since $\deg f(X) = 3, Z^2 \in L(N_X^{-3})$, and N_z^2 divides N_X^3. But since X is of degree 3 over $k(Z)$, we have $d(N_z^2) = 2d(N_z) = 2.[K : k(Z)] = 6 = 3.[K : k(X)] = 3d(N_X)$, and therefore $N_z = N_X^3$. From this, it is clear that there exists a prime divisor $\mathscr{Y}$ with $d(\mathscr{Y}) = 1$ such that $N_z = \mathscr{Y}^3, N_X = \mathscr{Y}^2$.

Finally, suppose a field K is of genus greater than 1. Then, $N(W) = g > o$ and $d(W) = 2g - 2 > o$, and hence we deduce the existence of an integral divisor $\neq N$ of degree $2g - 2$. Thus, we have proved that if $g > 1$, there always exists prime divisors of degree $\leq 2g - 2$. The minimal degree of prime divisors for a field of genus one is not known.

Lecture 10

20 The Greatest Common Divisor of a Class

We wish to find when the greatest common divisor of all integral divisors 60 of a class is different from the unit divisor N. We assert that this is impossible when $d(C) \geq 2g$. In fact, let $\mathscr{U}$ be an integral divisor of the class C. Then we obtain

$$d(C) - g + 1 = N(C) = N(C\mathscr{U}^{-1}) = d(C) - d(\mathscr{U}) + 1 - g + N(WC^{-1}\mathscr{U}),$$
$$d(\mathscr{U}) = N(WC^{-1}\mathscr{U}) \leq \max(0, d(WC^{-1}\mathscr{U}) + 1)$$

and since $1 + d(WC^{-1}\mathscr{U}) \leq 2g - 2 - 2g + 1 + d(\mathscr{U}) = d(\mathscr{U}) - 1$, we should have $d(\mathscr{U}) = 0$ and $\mathscr{U} = N$.

This is in a sense the best possible result. In fact, if there exists a prime divisor $\mathscr{Y}$ of degree 1 in the field, we have $d(W\mathscr{Y}) = 2g - 2$, and hence.

$$N(W\mathscr{Y}) = d(W) + d(\mathscr{Y}) - g + 1 = g = N(W),$$

which proves that $\mathscr{Y}$ divides all integral divisor of the class $W\mathscr{Y}$. Nevertheless, if $g > 0$, we can prove that the greatest common divisor of the canonical class W is N. For, suppose $\mathscr{U} \neq N$ is an integral divisor of W. Then,

$$\begin{aligned}\dim L(\mathscr{U}^{-1}) &= N(E\mathscr{U}) = d(\mathscr{U}) + 1 - g + N(W\mathscr{U}^{-1})\\ &= d(\mathscr{U}) + 1 - g + N(W) = d(\mathscr{U}) + 1 \geq 2.\end{aligned}$$

Thus, there exists a transcendental element $X \in L(\mathscr{U}^{-1})$. The divisor $(X)\mathscr{U}$ is then integral. Also, since $N(W) = g > o$, we can choose a differential ω of the first kind. Then, $(X\omega) = ((X)\mathscr{U}).((\omega)\mathscr{U}^{-1})$ is **61** also integral and therefore $X\omega$ is also first kind. By repetition of the argument, we obtain that $X^n\omega$ is of the first kind for all positive integers n. But since X is transcendental, $\mathscr{N}_X \neq \mathscr{N}$, and hence $X^n\omega$ cannot be an integral divisor for large n. This is a contradiction. Our assertion is therefore proved.

For fields of genus $g > o$, we shall improve the inequality $N(C) \leq \max(o, d(C) + 1)$.

Lemma. *If $g > o$ and $d(C) \geq o, C \neq E$, we have*

$$N(C) \leq d(C)$$

Proof. We may obviously assume that $N(C) > o$. Then there exists an integral divisor $\mathscr{U}$ in C, and since $C \neq E, \mathscr{U} \neq \mathscr{N}$, and therefore $d(C) = d(\mathscr{U}) > o$. Since $G > o$, $\mathscr{U}$ cannot be a divisor of the class W,and therefore

$$g = N(W) > N(W\mathscr{U}^{-1}) = N(WC^{-1})$$
$$N(C) = d(C) - g + 1 + N(WC^{-1}) \leq d(C) - g + 1 + g - 1 = d(C).$$

Our lemma is proved □

21 The Zeta Function of Algebraic Function Fields Over Finite Constant Fields

In the rest of this lecture and the following two lectures, we shall always assume that k is a finite field of characteristic $p > o$ and with $q = p^t$ **62** elements,and that K is an algebraic function field with constant field k.

If $\mathscr{Y}$ is any prime divisor of K, we shall call the number of elements in the class field $k_{\mathscr{Y}}$ the *norm of* $\mathscr{Y}$. Since $[k_{\mathscr{Y}} : k] = d(\mathscr{Y})$, we see that norm of $\mathscr{Y}$ (which we shall denote by $N_{\mathscr{Y}}$) is given by

$$N_{\mathscr{Y}} = q^{d(\mathscr{Y})}$$

We may extend this definition to all divisors, by putting

$$N\mathscr{U} = \prod_{\mathscr{Y}} (N\mathscr{Y})^{v_{\mathscr{Y}}(\mathscr{U})} = q^{d(\mathscr{U})}$$

Clearly we have for two divisors $\mathscr{U}$ and δ

$$N\mathscr{U}\delta = N\mathscr{U}.N\delta.$$

Before introduction the zeta function, we shall prove an important

Lemma. *For any positive integer m, the number of prime divisors of degree $\leq m$ is finite. The number of classes of degree zero is finite. (The latter is called* the class number *of K and is denoted by h).*

Proof. To prove the first part of the lemma, choose any transcendental element X of K. Let $\mathscr{Y}$ be any prime divisor of K with $d(\mathscr{Y}) \leq m$ and which does not divide $\mathscr{N}_X$. (We may neglect those $\mathscr{U}$ which divide $\mathscr{N}_X$, since they are finite in number.) Let $\mathscr{Y}^1$ be the restriction of $\mathscr{Y}$ to $k(X)$. $\mathscr{Y}^1$ must be a place on $k(X)$. Since $\mathscr{Y}^1(X) \neq \infty$, there corresponds a unique polynomial $(p(X))$ which gives rise to $\mathscr{Y}^1$.

Now, since $k_{\mathscr{Y}'} \subset k_{\mathscr{Y}}$, we obtain 63

$$\deg(p(X)) = d(\mathscr{Y}') \leq d(\mathscr{Y}) \leq m.$$

□

Since the number of polynomials of degree $\leq m$ over a finite field is finite, and since there the are only a finite number of prime divisors $\mathscr{Y}$ of K which divide $\mathfrak{z}_{p(X)}$ for a fixed $p(X)$, the first part of our theorem is proved.

To prove the second part, choose and fix an integral divisor $\mathscr{U}_o$ such that $d(\mathscr{U}_o) \geq g$. If C is any class of degree zero, we have

$$N(C\mathscr{U}_o) \geq d(C) + d(\mathscr{U}_o) - g + 1 \geq 1,$$

and hence there exists an integral divisor $\mathscr{U}$ in $C\mathscr{U}_o$ such that $d(\mathscr{U}) = d(C\mathscr{U}_o) = d(\mathscr{U}_o)$. But since

$$d(\mathscr{U}) = \sum d(\mathscr{Y})v_{\mathscr{Y}}(\mathscr{U}), d(\mathscr{Y}) \geq 1, v_{\mathscr{Y}}(\mathscr{U}) \geq 0,$$

and there are only a finite number of $\mathscr{Y}$ with $d(\mathscr{Y}) \leq d(\mathscr{U}_o)$, there are only a finite of integral $\mathscr{U}$ with $d(\mathscr{U}) = d(\mathscr{U}_o)$ and consequently only a finite number of C with $d(C) = 0$.

The lemma is completely proved.

Remark 1. Let ρ denote the least positive integer which is the degree of a class. since $C \to d(C)$ is a homomorphism of the group $\mathfrak{R}$ of divisor classes into the additive group Z of integers, we see that the degree of any class of the from $\nu\rho$ where ν is an integer, and that to any ν, there correspond precisely h classes $C_1^{(\gamma\rho)}, \ldots, C_h^{(\nu\rho)}$ of degree $\nu\rho$. 64

Remark 2. The number of integral divisors in any C is precisely $\dfrac{q^{N(C)}-1}{q-1}$. This is clear if $N(C) = 0$. If $N(C) > 0$, let $\mathscr{U}$ be any integral divisor of C. Then all integral divisors of C are of the from $(X)\mathscr{U}$, where $X \in L(\mathscr{U}^{-1}), X \neq 0$. Also $(X)\mathscr{U} = (Y)\mathscr{U}$ if and only if $\left(\dfrac{X}{Y}\right) = \mathscr{N}$ or $X = a\gamma, a \in k^*$. Since the number of non zero elements of $L(\mathscr{U}^{-1})$ is $q^{N(C)} - 1$ and the number of non zero elements of k is $q-1$ our assertion follows.

Now, let $s = \sigma + it$ be a complex variable. For $\sigma > 1$, we define *the zeta function* of the algebraic function field K by the series

$$\zeta(s, K) = \sum_{\mathscr{U}} \frac{1}{(N\mathscr{U})^s}, s = \sigma + it, \sigma > 1$$

the summation being extended over all integral divisors of the field K. Since $\left|\dfrac{1}{(N\mathscr{U})^s}\right| = \dfrac{1}{(N\mathscr{U})^\sigma}$, and all the terms of the series are positive when s is real, the following calculations are valid first for $s > 1$ and the for complex s with $\sigma > 1$. In particular, they prove the absolute convergence of the series

$$\tau(s, K)$$

$= \sum\limits_C$ (number of integral divisors in C). $q^{-sd(C)}$, the last summation being over all classes,

$$= \frac{1}{q-1} \sum_C (q^{N(C)} - 1) q^{-sd(C)};$$

65 writing $d(C) = \nu\rho$, and noticing that $q^{N(C)} - 1 = 0$ if $d(C) < 0$, the above

expression becomes

$$\frac{1}{q-1}\sum_{\nu=o}^{\infty} q^{-\nu\rho s}\sum_{l=1}^{h} q^{N(C_l^{(\nu\rho)})} - \frac{h}{q-1}\sum_{\nu=o}^{\infty} q^{-\nu\rho s}$$

Let us now put $U = q^{-s}$. Then $|U| = |q^{-s}| = q^{-\sigma} < 1$ since $\sigma > 1$, and we can sum the second geometric series. Suppose now that $g > o$. We may then split the first sum into two parts, the ranging over $o \leq \nu \leq \dfrac{2g-2}{\rho}$ and the second over $\nu > \dfrac{2g-2}{\rho}$. (Since $d(w) = 2g-2, \rho$) divides $2g-2$; or $\dfrac{2g-2}{\rho}$ is an integer). In the second summation since $d(C_l^{(\nu\rho)}) = \nu\rho > 2g-2$, we may substitute $N(C_l^{(\nu\rho)}) = \nu\rho - g + 1$. We obtain the expression

$$\frac{1}{q-1}\sum_{\nu=o}^{\frac{2g-2}{\rho}} q^{-\nu\rho s}\sum_{l=1}^{h} q^{N(C_l^{(\nu\rho)})} + \frac{h}{q-1}\sum_{\nu>\frac{2g-2}{\rho}} q^{-\nu\rho s}q^{\nu\rho-g+1} - \frac{h}{q-1}\cdot\frac{1}{1-q^{s\rho}}$$

$$= \tau(s,K) = \frac{1}{q-1}\sum_{\nu=o}^{\frac{2g-2}{\rho}} U^{\nu\rho}\sum_{l=1}^{h} q^{N(C_l^{(\nu\rho)})}$$

$$+ \frac{hq^{1-g}}{q-1}\frac{(Ug)^{2g-2+\rho}}{1-(Uq)^{\rho}} - \frac{h}{q-1}\frac{1}{1-U^{\rho}} \tag{1}$$

If $g = o, N(C) = d(C) - g + 1$ for all C with $d(C) > o$, and a similar computation gives

$$\tau(S,K) = \frac{hq}{q-1}\frac{1}{1-(Uq)^{\rho}} - \frac{h}{q-1}\frac{1}{1-U^{\rho}} \tag{2}$$

(1) and (2) may be combined as follows

$$(q-1)\tau(s,K) = F(U) + R(U), \tag{3}$$

where $F(U)$ is the polynomial 66

$$F(U) = \sum_{o \leq d(C) \leq 2g-2} q^{N(C)}U^{d(C)} \tag{4}$$

and $R(U)$ the rational function

$$R(U) = hq^{1-g}\frac{(Uq)^{\max(o,2g-2+\rho)}}{1-(Uq)^{\rho}} - \frac{h}{1-U^{\rho}} \tag{5}$$

These formulae provide the analytic continuation of $\tau(s, K)$ to the whole plane. The only possible poles are the values of s for which $U^{\rho} = 1$ or $(q^{U})^{\rho} = 1$.

For a rational function field $K = k(X)$, since $g = o, h = 1$ and $\rho = 1$, we obtain

$$(q-1)\tau(s, K) = \frac{q}{1-Uq} - \frac{1}{1-U} = \frac{q-1}{(1-Uq)(1-U)}$$

Lecture 11

22 The Infinite Product for $\zeta(s, K)$

Let K be an algebraic function field over a finite constant field k. Then, 67
the ζ function of K can be expressed as an infinite product taken over all prime divisors of K.

Theorem. *For $s = \sigma + it$, and $\sigma > 1$, we have*

$$\zeta(s, K) = \prod_{\mathscr{Y}} \frac{1}{1 - (N\mathscr{Y})^{-s}},$$

where the product is taken over all prime divisors $\mathscr{Y}$ of K. The product is absolutely convergent, and hence does not depend on the order of the factors.

Proof. Since $\sigma > 1$, we have for any integer $m > o$,

$$\prod_{N\mathscr{Y} \le m} \frac{1}{1 - N\mathscr{Y}^{-s}} = \prod_{N\mathscr{Y} \le m} \left(1 + \frac{1}{(N\mathscr{Y})^{s}} + \frac{1}{(N\mathscr{Y})^{2s}} + \cdots\right),$$

and since there are only a finite number of factors in the product, each factor being an absolutely convergent series, we may multiply these to obtain

$$\prod_{N\mathscr{Y} \le m} \frac{1}{1 - (N\mathscr{Y})^{-s}} = \sum_{n\mathscr{U} \le m} \frac{1}{(N\mathscr{U})^{s}} + \sum_{N\mathscr{U} > m} \frac{1}{(N\mathscr{U})^{s}},$$

where the first summation is over all integral divisors $\mathscr{U}$ with $N\mathscr{U} \le m$, and the second over all integral divisors $\mathscr{U}$ which do not contain any prime divisor $\mathscr{U}$ with $N\mathscr{U} > m$ and which satisfy the inequality $N\mathscr{U} > m$. □

68 Hence

$$\left|\prod_{N\mathscr{Y}\leq m}\frac{1}{1-(N\mathscr{Y})}-s-\sum_{N\mathscr{U}\leq m}\frac{1}{N\mathscr{U}}s\right| = \left|\sum_{N\mathscr{U}>m}^{1}\frac{1}{(N\mathscr{U})^{s}}\right|$$
$$\leq \sum_{N\mathscr{U}>m}\frac{1}{(N\mathscr{U})^{\sigma}}$$

and letting $m \to \infty$, we obtain the asserted equality, since $\sum_{N\mathscr{U}>m}(\frac{1}{N\mathscr{U}})^{\sigma}$, being the remainder of the convergent series for $\zeta(\sigma, K)$, tends to zero as $m \to \infty$.

The absolute convergence of the product is deduced from the inequality

$$\left|\frac{1}{(N\mathscr{Y})^{s}}+\frac{1}{(N\mathscr{Y})^{2s}}+-\right| \leq \frac{1}{(N\mathscr{Y})^{\sigma}}+\frac{1}{(N\mathscr{Y})^{2\sigma}}$$

As a corollary to this theorem, we see that $\zeta(s, K)$ has no zero for $\sigma > 1$.

23 The Functional Equation

In the last lecture, we obtained the following formula:

$$(q-1)^{\xi}(s, K) = F(U) + R(U), \quad \text{where} \quad U = q^{-s},$$
$$F(U) = \sum_{o\leq d(c)\leq 2g-2} q^{N(C)}U^{d(C)}$$

and
$$R(U) = hq^{1-g}\frac{(Uq)^{\max(o,2g-2+\rho)}}{1-(Uq)\rho} - \frac{h}{1-U\rho}.$$

Substituting for $N(C)$ in $F(U)$ from the theorem of Riemann-Roch, we obtain 69

$$F(U) = \sum_{o\leq d(C)\leq 2g-2} q^{d(C)-g+1+N(WC^{-1})}\mathscr{V}^{d(C)}$$

$$= q^{1-g} \sum_{o \le d(C) \le 2g-2} \left(\frac{1}{q^U}\right)^{d(WC^{-1})-2g+2} q^{N(WC^{-1})}$$

Writing $WC^{-1} = C^1$, and noticing that C^1 runs through the same set of classes as C in the summation, we have

$$F(U) = q^{q-1} U^{2g-2} \sum_{o \le d(C^1) \le 2g-2} \left(\frac{1}{qU}\right)^{d(C^1)} q^{N(C^1)} = q^{g-1} U^{2g-2} F\left(\frac{1}{qU}\right).$$

We shall prove that a similar functional equation holds for $R(U)$. First suppose that $g > o$. Then,

$$\begin{aligned} R(U) &= hg^{1-g} \frac{(qU)^{2g-2+\rho}}{1-(qU)^\rho} - \frac{h}{1-U^\rho} \\ &= -hg^{1-g} \frac{\left(\frac{1}{qU}\right)^{2g+2}}{1-\left(\frac{1}{qU}\right)\rho} + \frac{h.(q.\frac{1}{Uq})^\rho}{1-\left(q.\frac{1}{Uq}\right)^\rho} \\ &= U^{2g-2} q^{g-1} \left[hq^{1-g} \frac{\left(q\frac{1}{qU}\right)^{2g-2+\rho}}{1-\left(g.\frac{1}{U}q\right)^\rho} - \frac{h}{1-\left(\frac{1}{Uq}\right)^\rho} \right] \\ &= q^{g-1} U^{2g-2} R\left(\frac{1}{qU}\right). \end{aligned}$$

If $g = o$, the only divisor class of degree zero is E and hence $h = 1$. Also, since ρ divides $2g-2 = -2, \rho = 1$ or $\rho = 2$. If $\rho = 1$, we obtain

$$\begin{aligned} R(U) &= \frac{q}{1-qU} - \frac{1}{1-U} = \frac{q-1}{(1-U)(1-qU)} \\ &= q^{-1} U^{-2} \frac{q-1}{\left(1-\frac{1}{qU}\right)\left(1-q.\frac{1}{qU}\right)} \\ &= q^{-1} U^{-2} R\left(\frac{1}{qU}\right). \end{aligned}$$

If $\rho = 2$, we get 70

$$R(U) = \frac{q}{1-(qU)^2} - \frac{1}{1-U^2} = \frac{-q.\left(\frac{1}{qU}\right)^2}{1-\left(\frac{1}{qU}\right)^2} + \frac{U^{-2}}{1-\left(q.\frac{1}{qU}\right)^2}$$

$$= q^{-1}U^{-2}R\left(\frac{1}{qU}\right).$$

Thus, in any case, we have the functional equation

$$R(U) = q^{g-1}U^{2g-2}R\left(\frac{1}{qU}\right).$$

Adding the equation for $F(U)$ and $R(U)$, we see that $\zeta(s, K)$ satisfies the functional equation

$$(q-1)\zeta(s, K) = q^{g-1}q^{s(2-2g)}(q-1)\zeta(1-s, K), \text{ or}$$
$$\zeta(s, K) = q^{g-1}q^{s(2-2g)}\zeta(1-s.K)$$

We may also rewrite this in the from

$$q^{s(q-1)}\zeta(s, K) = q^{(1-s)(g-1)}\zeta(1-s, K).$$

Thus, the function on the left is unaltered by the transformation $s \to 1-s$.

24 L-series

We wish to study the L-series associated to characters of the class group of an algebraic function with a finite constant field.

71 **Definition.** *A* character $\mathcal{X}$ of finite order *on the class group* $\mathfrak{R}$ *is a homomorphism of* $\mathfrak{R}$ *into the multiplicative group* C^* *of non zero complex numbers such that there exists in integer* N *with* $\mathcal{X}^N(C) = 1$ *for all* C *in* $\mathfrak{R}$.

$\mathcal{X}(C)$ *is therefore an* N^{th} *root of unity for all* C. *We may define* $\mathcal{X}$ *on the group* v *of divisors by comparing with the natural homomorphism* $v \to \mathfrak{R}$, *i.e., by putting* $\mathcal{X}(\mathscr{U}) = \mathcal{X}(\mathscr{U}E)$ *for any divisor* $\mathscr{U}$.

The L-function $L(s, \mathcal{X}, K)$ associated to a character $\mathcal{X}$ (which we shall always assume to be of finite order) is then defined for $s = \sigma + it$, $\sigma > 1$ by the series

$$L(s, \mathfrak{X}, K) = \sum_{\mathscr{U}} \mathcal{X}(\mathscr{U})(N\mathscr{U})^{-s}$$

where the summation is over all integral divisors $\mathscr{U}$ of the field. The absolute value of the terms of this series is majorised by the corresponding term of the series $\sum \frac{1}{(N\mathscr{U})^{\sigma}} = \zeta(\sigma, K)$ and is therefore absolutely convergent for $\sigma > 1$. We may prove along exactly the same lines as in the case of the ζ -function the following product formula:

$$L(s, \mathfrak{X}, K) = \prod_{\mathscr{Y}} \frac{1}{1 - X(\mathscr{Y})(N\mathscr{Y})^{-s}}$$

where $\mathscr{Y}$ runs through all prime divisors and $\sigma > 1$.

Lecture 12

25 The Functional Equation for the L-functions

Let $\mathcal{X}$ be a character of finite order on the class group of an algebraic field K over a constant field k with $q = p^f$ elements. We consider two cases. 72

Case 1. *$\mathcal{X}$ when restricted to the subgroup $\Re_o$ of $\Re$ of all classes of degree zero, is trivial; i.e., $\mathcal{X}(C_o) = 1$ for $C_o \in \mathscr{R}_o$.*

Let ρ be as before the smallest positive integer which is the degree of a class, and let $C^{(\rho)}$ be a class of degree ρ. Then $\Re$ is clearly the direct product of $\Re_o$ and the cyclic group generated by $C^{(\rho)}$. Set $\mathcal{X}(C^{(\rho)}) = e^{2\pi i\xi}$. We then have

$$\begin{aligned} L(s, \mathcal{X}, K) &= \sum_{\mathscr{U}} \mathcal{X}(\mathscr{U})(N\mathscr{U})^{-s} = \sum_{C_o \in \Re_o} \sum_{\substack{n=-\infty \\ \mathscr{U} \in C^o C^{(\rho)^n}}}^{\infty} e^{2\pi i\xi n} q^{-n\rho s} \\ &= \sum_{\mathscr{U}} (N\mathscr{U})^{-\left(s - \frac{2\pi i\xi}{\rho \log q}\right)} = \zeta\left(s - \frac{2\pi i\xi}{\rho \log q}\right). \end{aligned}$$

Thus, the L-function reduces to a ζ- function in this case. We can therefore deduce a functional equation for $L(s, \mathcal{X}, K)$ from the functional equation for $\zeta(s, K)$. Define the character $\overline{\mathcal{X}}$ conjugate to $\mathcal{X}$ by putting $\overline{\mathcal{X}}(C) = \overline{\mathcal{X}(C)}$. Clearly, $\overline{\mathcal{X}}$ is a character of finite order on the class group and is trivial on $\Re_o$, also $\overline{\mathcal{X}}C^{(\rho)} = e^{-2\pi i\xi}$. Then, we obtain the following relation for $L(s, \mathcal{X}, K)$ by substituting from the functional equation for the ζ function.

$$\begin{aligned} q^{s(g-1)}L(s,\mathcal{X},K) &= q^{s(g-1)}\zeta\left(s-\frac{2\pi i\xi}{\rho\log q}\right)\\ &= q^{2(q-1)}\frac{2\pi i\xi}{\rho\log q}\zeta\left(1-s+\frac{2\pi i\xi}{\rho\log q}\right)q^{(1-s)(g-1)}\\ &= \mathcal{X}(W)_q{}^{(1-s)(g-1)}L(1-s,\bar{\mathcal{X}},K)\end{aligned}$$

73 since $\mathcal{X}(W) = (\mathcal{X}(C^{(\rho)}))\dfrac{2g-2}{\rho} = e\dfrac{2\pi i\xi}{\rho}(2g-2)$

Case 2. *Suppose now that $\mathcal{X}$ when restricted to $\Re_o$ is not identically 1. Let C_o^1 be a fixed class with $\mathcal{X}(C_o^1) \neq 1$. Then,*

$$\mathcal{X}(C_o^1)\sum_{C_o\in\Re_o}\mathcal{X}(C_o) = \sum_{C_o\in\Re_o}\mathcal{X}(C_o^1C_o) = \sum_{C_o\in\Re_o}\mathcal{X}(C_o),$$

and therefore $\sum\limits_{C_o\in\Re}\mathcal{X}(C_o) =$

Again, using the fact that $N(C) = 0$ if $d(C) < 0$, we obtain

$$\begin{aligned}(q-1)L(s,\mathcal{X},K) &= \sum_{C_o\in\Re_o}\mathcal{X}(C_o)\sum_{n=0}^{\infty}\mathcal{X}^n(C^{(\rho)})(q^{N(C_oC^{(\rho)})^n}-1)q^{-n\rho s}\\ &= \sum_{C_o\in\Re_o}\mathcal{X}(C_o)\sum_{n=o}^{\frac{2g-2}{\rho}}\mathcal{X}^n(C^{(\rho)})(q^{N(C_oC^{(\rho)^n})}-1)\\ &\quad+\sum_{C_o\in\Re_o}\mathcal{X}(C_o)\sum_{n>\frac{2g-2}{\rho}}\mathcal{X}^n(C^{(\rho)})(q^{n\rho-g+1}-1)q^{-n\rho s}\end{aligned}$$

The second sum vanishes, since $\sum\limits_{C_o\in\Re_o}\mathcal{X}(C_o) = 0$.

Thus, we obtain

$$(q-1)L(s,\mathcal{X},K) = \sum_{o\leq d(C)\leq 2g-2}\mathcal{X}(C)q^{N(C)}U^{d(C)}$$

74 The coefficient of U^{2g-2} is given by

$$\sum_{d(C)=2g-2} \mathcal{X}(C)q^{N(C)} = \mathcal{X}(W) \sum_{C_o \in \Re_o} \mathcal{X}(C_o)q^{N(C_oW)}$$

$$= \mathcal{X}(W)\left\{\sum_{C_o \neq E} \mathcal{X}(C_o)q^{g-1} + q^g\right\},$$

since $\quad N(C_oW) = d(C_oW) - g + 1 = g - 1$ if $C_o \neq E$ and $N(W) = g$,

$$= \mathcal{X}(W)\left\{\sum_{C_o \in \Re_o} \mathcal{X}(C_o)q^{g-1} + (q^g - q^{g-1})\right\}$$

$$= (q-1)\mathcal{X}(W)q^{g-1} \neq 0.$$

Thus, $L(s, \mathcal{X}, K)$ is a polynomial in $U = q^s$ of degree $2g - 2$ and leading coefficient $q^{g-1}\mathcal{X}(W)$

Again, by substituting from the Riemann-Roch theorem, we have

$$(q-1)L(s, \mathcal{X}, K) = \sum_{o \leq d(C) \leq 2g-2} \mathcal{X}(C)q^{N(C)}U^{d(C)}$$

$$= \sum_{o \leq d(C) \leq 2g-2} \mathcal{X}(C)q^{d(C)-g+1+N(WC^{-1})}U^{d(C)}$$

$$= q^{g-1}U^{2g-2}\mathcal{X}(W) \sum_{o \leq d(C) \leq 2g-2} \overline{\mathcal{X}(WC^{-1})}q^{N(WC-1)} \left(\frac{1}{qU}\right)^{d(WC^{-1})}$$

Writing C^1 for WC^{-1} and noting that C^1 runs through exactly the same range of summation as does C, we obtain

$$(q-1)L(s, \mathcal{X}, K) = (q-1)q^{g-1}U^{2g-2}\mathcal{X}(W)L(1-s, \overline{\mathcal{X}}, K),$$

which is again the same functional equation that we got in Case 1. We have therefore proved the

Theorem. *For any character $\mathcal{X}$ of finite order,*

$$q^{s(g-1)}L(s, \mathcal{X}, K) = \mathcal{X}(W)q^{(1-s)(g-1)}L(1 - s\overline{\mathcal{X}}, K).$$

Lecture 13

26 The Components of a Repartition

Our next aim is to introduce the L-functions modulo an integral divisor of an algebraic function field over a finite constant filed and to obtain their functional equation. We shall develop the necessary results for this in this and the next two lectures. 75

Let K be an algebraic function field over an arbitrary (not necessarily finite) constant field k. For a repartition $\mathscr{C} \in \mathscr{X}$ and a prime divisor $\mathscr{Y}$, we define the component $\mathscr{C}^{\mathscr{Z}}$ of $\mathscr{C}$ at $\mathscr{Z}$ to be the repartition defined by

$$\mathscr{C}^{\mathscr{Z}}(\mathscr{U}) = \begin{cases} \mathscr{C}_{\mathscr{Z}} & \text{if } \mathscr{U}\ \mathscr{Y} \\ 0 & \text{if } \mathscr{Y} \text{is a prime divisor other than } \mathscr{Y}. \end{cases}$$

The mapping is clearly a k-linear mapping of $\mathscr{X}$ into itself. This induces a linear mapping of the dual of $\mathscr{X}$ into itself, by which a differential ω is taken to a liner map $\omega\mathscr{Z} : \mathscr{X} \to \mathscr{X}$ given by

$$\omega^{\mathscr{Y}}(\mathscr{C}) = \omega(\mathscr{C}^{\mathscr{Z}})$$

$\omega^{\mathscr{Z}}$ is called the component of the differential ω at $\mathscr{Y}.\omega^{\mathscr{Z}}$ is not, in general, a differential. For $X \in K$, we have

$$(X\omega)^{\mathscr{Y}}(\mathscr{C}) = (X\omega)(\mathscr{C}^{\mathscr{Z}}) = \omega(X\mathscr{C}^{\mathscr{Z}}) = \omega((X\mathscr{C})^{\mathscr{Y}}) = \omega^{\mathscr{Z}}(X\mathscr{C})$$

We shall now prove a lemma which expresses a differential in terms of its components.

Lemma. *If ω is a differential and $\mathscr{C}$ a repartition, $\omega^{\mathscr{Y}}(\mathscr{C}) = 0$ for all but a finite number of prime divisors $\mathscr{Y}$, and we have* 76

$$\omega(\mathscr{C}) = \sum_{\mathscr{Y}} \omega^{\mathscr{Y}}(\mathscr{C}).$$

Proof. Let $\mathscr{U}$ be a divisor which divides the differential ω. Let $\mathscr{Y}_1, \ldots, \mathscr{Y}_n$ be the finite number of prime divisors for which either $v_{\mathscr{Y}_i}(\mathscr{U}) \neq 0$ or $v_{\mathscr{Y}_i}(\mathscr{C}) < 0$. For $\mathscr{U} \neq$ any of the $\mathscr{Y}_i$, and any prime divisor $\mathscr{Y}$, we have

$$\begin{aligned} v_{\mathscr{Y}(\mathscr{C}^{\mathscr{U}})} &= v_{\mathscr{Y}}(\mathscr{C}^{\mathscr{U}}(\mathscr{Y})) \\ &= \begin{Bmatrix} v_{\mathscr{C}}(\mathscr{Y}_{\mathscr{U}}) & \text{if } \mathscr{U} = \mathscr{Y} \\ v_{\mathscr{Y}}(0) & \text{if } \neq \mathscr{Y}\mathscr{U} \end{Bmatrix} = \begin{Bmatrix} v_{\mathscr{U}}(\mathscr{C}) & \text{if } \mathscr{Y} = \mathscr{U} \\ \infty & \text{if } \mathscr{Y} \neq \mathscr{U} \end{Bmatrix} \geq v_{\mathscr{Y}}(\mathscr{U}), \end{aligned}$$

and therefore $\mathscr{C}^{\mathscr{U}} \in \Lambda(\mathscr{U})$, $\omega^{\mathscr{U}}(\mathscr{C}) = \omega(\mathscr{C}^{\mathscr{U}}) = 0$. □

Also, if we put $\mathscr{Y} = \mathscr{C} - \sum\limits_{i=1}^{n} \mathscr{C}^{\mathscr{Y}_i}$, we have for any $\mathscr{Y}$,

$$v_{\mathscr{Y}}(\mathscr{Y}) = \begin{Bmatrix} v_{\mathscr{Y}}(\mathscr{C}_{\mathscr{Y}}) & \text{if } \mathscr{Y} \text{ is not any of the} \mathscr{Y}_1 \\ v_{\mathscr{Y}}(0) = \infty & \text{if } \mathscr{Y} \text{ is a certain } \mathscr{Y}_i \end{Bmatrix} \geq v_{\mathscr{Y}}(\mathscr{U}),$$

and therefore $\mathscr{Y} \in \Lambda(\mathscr{U})$. Hence,

$$\begin{aligned} \omega(\mathscr{C}) &= \omega\left(\mathscr{C} - \sum_{i=1}^{n} \mathscr{C}^{\mathscr{Y}_i}\right) + \omega\left(\sum_{i=1}^{n} \mathscr{C}^{\mathscr{Y}_i}\right) = \omega\left(\sum_{i=1}^{n} \mathscr{C}^{\mathscr{Y}_i}\right) \\ &= \sum_{i=1}^{n} \omega\left(\mathscr{C}^{\mathscr{Y}_i}\right) = \sum_{i=1}^{n} \omega^{\mathscr{Y}_i} = \sum_{\mathscr{Y}} \omega\mathscr{Y}(\mathscr{C}). \end{aligned}$$

Our lemma is proved.

We shall now prove another useful

77 **Lemma.** *Let ω be a differential and $\mathscr{C}$ a prime divisor. Then $v_{\mathscr{Y}}((\omega))$ is the largest integer m such that whenever $X \in K$ and $v_{\mathscr{Y}}(X) \geq -m$, we have $\omega^{\mathscr{Y}}(X) = 0$.*

Proof. Suppose first that $X \in K$ with $v_{\mathscr{Y}}(X) \geq -v_{\mathscr{Y}}((\omega))$. Then clearly the repartitions $x^{\mathscr{Y}}$ is in $\Lambda((\omega)^{-1})$ and therefore $\omega^{\mathscr{Y}}(X) = \omega(X^{\mathscr{Y}}) = 0$. □

Now, by the definition of (ω), ω does not vanish on the space $\Lambda((\omega)^{-1}\mathscr{Y}^{-1})$. Hence there exists a repartition $\mathscr{C} \in \Lambda((\omega)^{-1}\mathscr{Y}^{-1})$ such that $\omega(\mathscr{C}) \neq 0$. It is evident that for $\mathscr{U} \neq \mathscr{Y}$, $\mathscr{C}^{\mathscr{U}} \in \Lambda((\omega)^{-1})$ and therefore $\omega(\mathscr{C}) \neq 0$. Hence,

$$0 \neq \omega(\mathscr{C}) = \sum_{\mathscr{U}} \omega(\mathscr{C}^{\mathscr{U}}) = \omega(\mathscr{C}^{\mathscr{Y}})$$

Put $X = \mathscr{C}^{\mathscr{Y}}$. Then,

$$\omega^{\mathscr{Y}}(X) = \omega(X^{\mathscr{Y}}) = \omega(\mathscr{C}^{\mathscr{Y}}) \neq 0$$

and $$v_{\mathscr{Y}}(X) = v_{\mathscr{Y}}(\mathscr{C}) \geq -v_{\mathscr{Y}}((\omega)) - 1.$$

Thus, $v_{\mathscr{Y}}((\omega))$ is the largest m for which $v_{\mathscr{Y}}(X) \geq -m$ implies that $\omega^{\mathscr{Y}}(X) = 0$.

Lecture 14

27 A Consequence of the Riemann-Roch Theorem

In this lecture, we shall prove a theorem which will be crucial in the proof of the functional equation of the L-functions modulo an integral divisor. 78

Let $\mathscr{F}$ be an integral divisor and $\mathscr{U}_1, \ldots, \mathscr{U}_r$ the distinct prime divisors occurring in it. We prove a series of lemmas leading upto the proof of the theorem we mentioned above.

Lemma 1. *In any class C, there exists a divisor $\mathscr{U}$ such that $v_{\mathscr{U}_\nu}(\mathscr{U}) = 0 (\nu = 1, \cdots r)$.*

Proof. Let $\mathscr{U}_\circ$ be any divisor of C. By the independence theorem for valuations, we may find $X \in K$ with

$$v_{\mathscr{U}_\nu}(X) = -v_{\mathscr{U}_\nu}(\mathscr{U}_\circ)$$

Then $\mathscr{U} = (X)\mathscr{U}_\circ \in C$ satisfies the required conditions. □

Let us denote by R the vector space $\Gamma(n/\mathscr{U}_1, \mathscr{U}_r)$ and by i the subspace $\Gamma(\mathscr{F}/\mathscr{U}_1, \ldots \mathscr{U}_r)$. R is not only a vector space over k, but also an algebra. In fact, if $X, Y \in R$,

$v_{\mathscr{U}_i}(XY) = v_{\mathscr{U}_i}(X) + v_{\mathscr{U}_i}(Y) \geq 0$, $XY \in R$. $(i = 1, \ldots r)$ i is an ideal of R, since $X \in R$, $Y \in i$ implies that

$$v_{\mathscr{U}_i}(XY) = v_{\mathscr{U}_i}(X) + v_{\mathscr{U}_i}(Y) \geq v_{\mathscr{U}_i}(\mathscr{F}), XY \in i.$$

Thus, the quotient $\overline{R} = R/i$ is an algebra of 79

$$\text{rank}\dim_k = \frac{\Gamma(n/\mathscr{U}r)\,\mathscr{U}r)}{\Gamma(\mathscr{F}/\mathscr{U}_1\,\mathscr{U}_r)} = d(\mathscr{F})$$

over the field k.

Now, choose a differential ω such that the divisor $\mathscr{F}(\omega)$ is coprime to $\mathscr{F}$. This is possible by Lemma 1. We shall assume this ω to be chosen and fixed throughout the discussion. We define a linear function S on the algebra R by

$$S(X) = \sum_{\nu=1}^{r} \omega^{\mathscr{U}_\nu}(X),\ X \in R.$$

S vanishes on the ideal i, for if $X \in i$, $v_{\mathscr{U}_\nu}(X) \geq v_{\mathscr{U}_\nu}(\mathscr{F})$, and since $\mathscr{F}(\omega)$ is corprime to each $\mathscr{U}_\nu$, $v_{\mathscr{U}_\nu}(\mathscr{F}) + v_{\mathscr{U}_\nu}((\omega)) = 0$, $v_{\mathscr{U}_\nu}(\mathscr{F}) = -v_{\mathscr{U}_\nu}((\omega))$. By the last lemma of the previous lecture, we deduce that

$$S(X) = \sum_{\nu=1}^{r} \omega^{\mathscr{U}_\nu}(X) = 0.$$

Thus, S induces a linear map from the quotient $\overline{R}$ to the field k. This in turn gives rise to a bilinear form on $\overline{R}$ defined by $(\overline{X}, \overline{Y}) \to S(\overline{X}\,\overline{Y})$. Our next lemma states that this is non - degenerate.

Lemma 2. *If $\overline{X} \in \overline{R}$, $\overline{X} \neq 0$, there exist a $\overline{Y} \in \overline{R}$ such that $S(\overline{X}.\overline{Y}) = 1$.*

Proof. Let X be any element of the coset $\overline{X}$. Since $\overline{X} \neq 0$, we have $X \notin i$ and $v_{\mathscr{U}_\nu}(X) < v_{\mathscr{U}_\nu}(\mathscr{F}) = -v_{\mathscr{U}_\nu}((\omega))$ for some ν. Thus, $X\omega$ is a differential with $v_{\mathscr{U}_\nu}(X\omega) < 0$. By the last lemma of the previous lecture, we deduce that there exists an element $Y_1 \in K$ such that $v_{\mathscr{U}_\nu}(Y_1) \geq 0$ and $(X\omega)^{\mathscr{U}_\nu}(Y_1) \neq 0$. □

80 Find $Y_2 \in K$ such that

$$v_{\mathscr{U}_\nu}(Y_2 - Y_1) \geq \max(0, -v_{\mathscr{U}_\nu}((X\omega))),$$
$$v_{\mathscr{U}_\nu}(Y_2) \geq \max(0, -v_{\mathscr{U}_\mu}\ ((X\omega))).\ \text{for}\ \mu \neq \nu.$$

Since we also have

$$v_{\mathscr{U}_\nu}(Y_2) \geq \min(v_{\mathscr{U}_\nu}(Y_2 - Y_1), v_{\mathscr{U}_\nu}(Y_1)) \geq 0,$$

it follows that $Y_2 \in \overline{R}$. Also, for any $\mu \neq \nu$, we have by the second condition, $(X\omega)^{\mathscr{U}_\mu}(Y_2) = 0$. Again, it follows from the first condition that

$$(X\omega)^{\mathscr{U}_\nu}(Y_2 - Y_1) = 0, (X\omega)^{\mathscr{U}_\nu}(Y_2) = (X\omega)^{\mathscr{U}_\nu}(Y_1) \neq 0$$

Thus,

$$S(\overline{X}\,\overline{Y}_2) = \sum_{\lambda=1}^{r} \omega^{\mathscr{U}_\lambda}(XY_2) = \sum_{\lambda=1}^{r}(X\omega)^{\mathscr{U}_\lambda}(Y_2) = (X\omega)^{\mathscr{U}_\nu}(Y_2) \; = \varrho \neq 0,$$

and $\overline{Y} = \overline{Y}_{2_{\bar{\varrho}}}$ satisfies the conditions of our lemma.

Now, let $\mathscr{U}$ be any divisor coprime to $\mathscr{F}$. Then, we assert that $L(\mathscr{U})$ is a subspace of R. In fact, we have for $X \in L(\mathscr{U})$, $v_{\mathscr{U}_\nu}(X) \geq v_{\mathscr{U}_\nu}(\mathscr{U}) = 0$. Also, we assert that $L(\mathscr{U}) \cap i = L(\mathscr{U}\mathscr{F})$. This follows from the following argument $X \in L(\mathscr{U}\mathscr{F}) \Longleftrightarrow v_{\mathscr{U}}(X) \geq \; v_{\mathscr{U}}(\mathscr{U}) + v_{\mathscr{U}}(\mathscr{F})$ for every $\mathscr{U} \Longleftrightarrow v_{\mathscr{U}}(X) \geq v_{\mathscr{U}}(\mathscr{U})$ for every $\mathscr{U}$ and $v_{\mathscr{U}_\nu}(X) \geq v_{\mathscr{U}_\nu}(\mathscr{F})$ for $(\nu = 1, \quad, r)$. Hence, if we denote by $\overline{L(\mathscr{U})}$ the image of $L(\mathscr{U})$ under the natural homomorphism form R to $\overline{R}$, we have

$$\begin{aligned} \dim_k(\overline{L(\mathscr{U})}) = \dim_k\left(\frac{L(\mathscr{U}) + i}{i}\right) &= \dim \frac{L(\mathscr{U})}{L(\mathscr{U}) \cap i} \\ &= \dim_k \frac{L(\mathscr{U})}{L(\mathscr{U}\mathscr{F})} = l(\mathscr{U}) - l(\mathscr{U}\mathscr{F}). \end{aligned}$$

81

This proves that the dimension of $\overline{L(\mathscr{U})}$ depends only on the class of $\mathscr{U}$. Since there are divisors in any class prime to $\mathscr{F}$, we may define $N_0(C)$ for a class C to be $\dim_k \overline{L(\mathscr{U})}$ for any $\mathscr{U} \in C^{-1}$ coprime to $\mathscr{F}$.

For any class C, we shall call the class $C^* = WC^{-1}\mathscr{F}$ the *complementary class* of C modulo $\mathscr{F}$. We then prove the following

Lemma 3. *For any class C, we have*

$$N_0(C) + N_0(C^*) = d(\mathscr{F}).$$

Proof. Let $\mathscr{U} \in C^{-1}$ and $\delta \in C^{*-1}$ be prime to $\mathscr{F}$. Then,

$$N_0(C) + N_0(C^*) = \dim \overline{L(\mathscr{U})} + \dim \overline{L(\delta)}$$

$$\begin{aligned}
&= (l(\mathscr{U}) - l(\mathscr{U}\mathscr{F})) + (l(\delta) - l(\delta\mathscr{F})\\
&= N(C) - N(C\mathscr{F}^{-1}) + N(WC^{-1}\mathscr{F}) - N(WC^{-1})\\
&= (d(C) - g + 1) - (d(C\mathscr{F}^{-1}) - g + 1) = d(\mathscr{F})
\end{aligned}$$

by the Riemann-Roch theorem. Our lemma is proved. □

Now, let V be a vector space on a field k and $B : VxV \to K$ a non-degenerate bilinear form on V. (A bilinear form is said to be non-degenerate if for every $X \neq 0$, there exist a $X_1 \in V$ such that $B(X, X_1) \neq 0$ and for every $Y \neq 0$ there exists a $Y_1 \in V$ such that $B(Y_1, Y) \neq 0$. Let V_1 be a subspace of V. Then we define *the complementary subspace of* V_1 with respect to the bilinear form B to the space $V_{1_{comp}}$ of all elements
82 $Y \in V$ such that $B(X, Y) = 0$ for every $X \in V_1$. We then have the

Lemma 4. *Let V be a finite dimensional vector space and B a; non-degenerate bilinear form on V. Then, if V_1 is a subspace of V, we have*

$$\dim_k V_1 + \dim_k V_{1_{comp.}} = \dim V.$$

Proof. Let V^* be the dual of V. We can define a homomorphism $\varphi : V \to V^*$ which takes an element $X \in V$ ot the linear map $\varphi(X) \in V^*$ defined by

$$\varphi(X)(Y) = B(Y, X)$$

Since B is non-degenerate, $\varphi(X) \neq 0$ if $X \neq 0$, and φ is a monomorphism. Since V is finite dimensional, $\dim V^* = \dim V = \dim \varphi(V)$. Thus, φ is also an epimorphism. □

Now, let V_2 be the complementary subspace of V_1. Then, every element of $\varphi(V_2)$ is a linear map of V into k which vanishes on the subspace V_1, and conversely every element of V^* which vanishes on V_1 should be of the form $\varphi(X)$, where $X \in V_2$. Hence, we deduce that $\varphi(V_2)$ is isomorphic to the dual of the quotient space V/V_1. Therefore,

$$\dim_k V_2 = \dim_k \varphi(V_2) = \dim_k (V/V_1)^* = \dim_k V - \dim_k V_1,$$
$$\dim_k V_1 + \dim_k V_2 = \dim_k V.$$

The lemma is proved.

83 Now, let $\mathscr{U}$ be a divisor prime to $\mathscr{F}$ and ω the (already chosen and fixed) differential such that $(\omega)\mathscr{F}$ is prime to $\mathscr{F}$. We define *the complementary divisor* $\mathscr{U}^*$ of $\mathscr{U}$ as the divisor $(\omega)^{-1}\mathscr{F}^{-1}\mathscr{U}^{-1}$. It is clear that $\mathscr{U}^*$ is also prime to $\mathscr{F}$ and that if $\mathscr{U}^{-1} \in C$, $\mathscr{U}^{*-1} \in C^*$. We may then state our theorem as follows.

Theorem. *The complementary space of $\overline{L(\mathscr{U})}$ in $\overline{R}$ with respect to the bilinear form $B(\overline{X}, \overline{Y}) = S(XY)$ defined on $\overline{R}$ is $\overline{L(\mathscr{U}^*)}$.*

Proof. Suppose $\overline{X} \in \overline{L(\mathscr{U})}$ and $\overline{Y} \in \overline{L(\mathscr{U}^*)}$. Then, for any prime divisor $\mathscr{Y} \neq$ any of the $\mathscr{U}_\nu$, we have

$$v_{\mathscr{Y}}(XY) \geq v_{\mathscr{Y}}(\mathscr{U}\mathscr{U}^*) = v_{\mathscr{Y}}((\omega)^{-1}\mathscr{F}^{-1}) = -v_{\mathscr{Y}}((\omega)),$$

and therefore by the lemma of the previous lecture,

$$\omega^{\mathscr{Y}}(XY) = 0$$

Hence, we obtain,

$$S(\overline{X}\overline{Y}) = S(XY) = \sum_{i=1}^{n} \omega^{\mathscr{U}}(XY) = \sum_{\mathscr{Y}} \omega^{\mathscr{Y}}(XY) = \omega(XY) = 0,$$

since $XY \in K$. Thus, we deduce that

$$\overline{L(\mathscr{U}^*)} \subset \overline{((L(\mathscr{U})}_{compl}.$$

□

Now, let C and C^* be the classes of $\mathscr{U}^{-1}$ and $\mathscr{U}^{*-1}$. We then have

$$\begin{aligned}\dim_k \overline{L(\mathscr{U}^*)} &= N_0(C^*) = d(\mathscr{F}) - N_0(C)\\ &= \dim_k \overline{R} - \dim_k \overline{L(\mathscr{U})}\\ &= \dim_k \overline{(L(\mathscr{U}))}_{compl.}\end{aligned}$$

since $B(\overline{X}, \overline{Y}) = S(\overline{X}\overline{Y})$ is non-degenerate by lemma 2. Hence, it follows that $\overline{(L(\mathscr{U})}_{comp.} = \overline{L(\mathscr{U}^*)}$. 84

Lecture 15

28 Classes Modulo $\mathcal{F}$

Let K be an algebraic function field over an arbitrary constant field k and 85 $\mathcal{F}$ an integral divisor of K. We shall denote the distinct prime divisors of $\mathcal{F}$ by $\mathscr{U}_1, \ldots, \mathscr{U}_r$. We now define some groups associated to the integral divisor $\mathcal{F}$. In all the cases, it is an easy matter to verify that the sets defined are closed under taking products or inverses.

$\vartheta^{\mathcal{F}}$ will be the group of divisors coprime to $\mathcal{F}$, and $\vartheta_0^{\mathcal{F}}$ the subgroup of all elements of $\vartheta^{\mathcal{F}}$ whose degree is zero. $K^{*\mathcal{F}}$ is the multiplicative group of elements of K^* which are coprime to $\mathcal{F}$. $E^{\mathcal{F}}$ is the group of principal divisors coprime to $\mathcal{F}$.

Clearly, $k^* \subset K^{*\mathcal{F}}$, and since two elements of $K^{*\mathcal{F}}$ define the same divisors if and only if their ratio is a constant, we have the isomorphism

$$E^{\mathcal{F}} \simeq K^{*\mathcal{F}}/_{k^*}$$

Moreover, since every class contains a divisor coprime to $\mathcal{F}$, the saturation of $\vartheta^{\mathcal{F}}$ by E is the whole of ϑ, and consequently

$$\vartheta^{\mathcal{F}}/_{E^{\mathcal{F}}} = \frac{\vartheta^{\mathcal{F}}}{E \cap \vartheta^{\mathcal{F}}} \simeq \frac{\vartheta^{\mathcal{F}} E}{E} = \frac{\vartheta}{E} = \Re,$$

and similarly $\vartheta_o^{\mathcal{F}}/_{E^{\mathcal{F}}} \simeq \vartheta_0$.

We shall say that $X \equiv Y(\mod {}^+\mathcal{F})$ if $v_{\mathscr{U}_i}(X - Y) \geq v_{\mathscr{U}_i}(\mathcal{F})$ $(i =$ 86 $1, r)$. The condition is evidently equivalent to saying that $X - Y \in \Gamma(\mathcal{F}/\mathscr{U}_{1,}\mathscr{U}_r)$. Let $K^*_{\mathcal{F}}$ be the set of elements X of K^* which satisfy $X \equiv 1(\mod {}^+\mathcal{F})$. If $X \in K^*_{\mathcal{F}}$, it follows that $v_{\mathscr{U}_i}(X) = \min(v_{\mathscr{U}_i}(X - 1),$

$v_{\mathscr{U}_i}(1)) = 0$. Hence, if $X, Y \in K^*$, we have $XY \equiv Y \equiv 1(\mod {}^+\mathscr{F})$ and therefore $XY \in K^*_{\mathscr{F}}$. Similarly, $\dfrac{1}{X}$ is also in $K^*_{\mathscr{F}}$. Since $X \in K^*_{\mathscr{F}} \Rightarrow_{\mathscr{U}i}$ $(X) = 0$, we deduce that $K^*_{\mathscr{F}}$. $E_{\mathscr{F}}$ shall denote the group of principal divisors of $K^*_{\mathscr{F}} \subset K^{*\mathscr{F}}$. $E_{\mathscr{F}}$ elements of $K^*_{\mathscr{F}}$. It follows from the above inclusion that $E_{\mathscr{F}} \subset E^{\mathscr{F}}$. $E_{\mathscr{F}}$ is called *the ray modulo $\mathscr{F}$*.

If $\mathscr{F} \neq N$, it is easy to see that $k^* \cap K^*_{\mathscr{F}} = \{1\}$. Hence, we deduce, in this case, that $E_{\mathscr{F}} = \dfrac{K^*_{\mathscr{F}} k^*}{k*} \simeq \dfrac{K*}{k^*_{\mathscr{F}} \cap k^*} \simeq K^*_{\mathscr{F}}$.

The *class group modulo $\mathscr{F}$* is by definition the quotient group $\mathfrak{R}_{\mathscr{F}} = \vartheta^{\mathscr{F}} /_{E_{\mathscr{F}}}$ and its elements are called *classes modulo $\mathscr{F}$*. The subgroup $\mathfrak{R}_{0_{\mathscr{F}}} = \vartheta^{\mathscr{F}}_0 /_{E_{\mathscr{F}}}$ of $\mathfrak{R}_{\mathscr{F}}$ is called the *group of classes modulo $\mathscr{F}$ of degree zero* and its order $h_{\mathscr{F}}$ is called the *class number modulo $\mathscr{F}$*. In the case of a finite field $k, h_{\mathscr{F}}$ can be expressed in terms of the class number h. We have the following theorem.

Theorem. *Let the constant field k be finite with q elements and let $\mathscr{F}$ be an integral divisor different from N. Then,*

$$h_{\mathscr{F}} = \frac{hN\mathscr{F}}{q-1} \prod_{\nu=1}^{r} \left(1 - \frac{1}{N\mathscr{U}_\nu}\right)$$

Proof. From the isomorphisms

$$\mathfrak{R}0 \simeq \vartheta^{\mathscr{F}}_0 / E^{\mathscr{F}} \simeq \frac{\vartheta^{\mathscr{F}}_0 / E_{\mathscr{F}}}{E^{\mathscr{F}} / E_{\mathscr{F}}},$$

87 it follows that

$$h = \frac{h_{\mathscr{F}}}{\left(\frac{E^{\mathscr{F}}}{E_{\mathscr{F}}} : 1\right)}$$

Again,

$$\frac{E^{\mathscr{F}}}{E_{\mathscr{F}}} \simeq \frac{K^{*\mathscr{F}} / k^*}{K^*_{\mathscr{F}} k^* / k^*} \simeq \frac{K^{*\mathscr{F}}}{K^*_{\mathscr{F}} k^*} \simeq \frac{K^{*\mathscr{F}} / K^*_{\mathscr{F}}}{K^*_{\mathscr{F}} k^* / K^*_{\mathscr{F}}},$$

and
$$\frac{K^*_{\mathscr{F}} k^*}{k^*_{\mathscr{F}}} \simeq \frac{k^*}{k^* \cap K^*_{\mathscr{F}}} \simeq k^*,$$

since $\mathscr{F} \neq N$ and therefore $k^* \cap K^*_{\mathscr{F}} = \{1\}$. Hence, we obtain

$$h_{\mathscr{F}} = \frac{h}{q-1}\left[K^{*\mathscr{F}} : K^{*}{}_{\mathscr{F}}\right].$$

□

Now , $K^{*\mathscr{F}}$ is precisely the set of elements of $\Gamma(N/\mathscr{U}_1, \ldots \mathscr{U}_r)$ which do not lie in any of the spaces $\Gamma(\mathscr{U}_i/\mathscr{U}_1, \ldots \mathscr{U}_r)$. Also, if $X, Y \in K^{*\mathscr{F}}$, they belong to the same coset modulo $K^*_{\mathscr{F}}$ if and only if $XY^{-1} \equiv 1$ (mod ${}^{+}\mathscr{F}$) $\Longleftrightarrow$ $X \equiv Y$ (mod ${}^{+}\mathscr{F}$) (since Y is coprime to $\mathscr{F}$) $\Longleftrightarrow$ $X - Y \in \Gamma(\mathscr{F}/\mathscr{U}_1 \cdots \mathscr{U}_r)$. We deduce from these facts that (with $S = (\mathscr{U}_1, \ldots \mathscr{U}_r)$)

$$\begin{aligned}\left[K^{*\mathscr{F}} : K^*_{\mathscr{F}}\right] &= q^{\dim \frac{\Gamma(n/s)}{\Gamma(\mathscr{F}/s)}} - \sum_i q^{\dim \frac{\Gamma(\mathscr{U}_i/s}{\Gamma(\mathscr{F}/s)}} + \sum_{i \neq j} q^{\dim \frac{\Gamma(\mathscr{U}_i\mathscr{U}_j/s)}{\Gamma(\mathscr{F}/s)} \cdots} \\ &= q^{d(\mathscr{F})} - \sum_i q^{d(\mathscr{F})-d(\mathscr{U}_i)} + \sum_{i \neq j} q^{d(\mathscr{F})-d(\mathscr{U}_i)-d(\mathscr{U}_j)} \ldots \\ &= N(\mathscr{F}) \prod_{\nu=1}^{r}\left(1 - \frac{1}{N\mathscr{U}_\nu}\right)\end{aligned}$$

Substituting this expression in the value of $h_{\mathscr{F}}$, we get the required result. 88

Note that the theorem is not valid when $\mathscr{F} = N$. In fact, we have $\Re_{0_N} = \Re_0$ and $h_N = h$.

We shall end this lecture with a simple lemma asserting the existence of sufficiently many divisors in any class modulo $\mathscr{F}$.

Lemma. *If $\mathscr{U}$ is any given divisor, any class $C_{\mathscr{F}}$ modulo $\mathscr{F}$ contains a divisor δ prime to $\mathscr{U}$.*

Proof. Let $\mathscr{U}_0$ be any divisor of $C_{\mathscr{F}}$. Find a $Y \in K$ such that

$$v_{\mathscr{U}_\nu}(Y-1) \geq v_{\mathscr{U}_\nu}(\mathscr{F}) \; (\nu = 1, \ldots, r)$$

and $$v_{\mathscr{U}}(Y) = -v_{\mathscr{U}}(\mathscr{Y}_0) \text{ if } v_{\mathscr{Y}}(\mathscr{U}) \neq 0 \text{ and } \mathscr{Y} \neq \mathscr{U}_\nu$$

Then it is easy to verify that $\delta = \mathscr{U}_0(Y)$ satisfies the conditions of the lemma. □

Lecture 16

29 Characters Modulo $\mathscr{F}$

We shall now introduce the characters of an algebraic function field K modulo an integral divisor $\mathscr{F}$ 89

Definition. *A chapter $\mathscr{X}$ modulo an integral divisor $\mathscr{F}$ is a homomorphism of $\Re_{\mathscr{F}}$ into the multiplicative group of complex numbers with absolute value one.*

If $\mathscr{U}$ is a divisor prime to $\mathscr{F}$, we put $\mathcal{X}(\mathscr{U}) = \mathcal{X}(\mathscr{U} E_{\mathscr{F}})$. If $\mathscr{U} = \delta/\mathscr{L}$, where δ and $\mathscr{L}$ are mutually coprime and integral and $\mathscr{L}$ coprime to $\mathscr{F}$ whereas δ is not, we define $\mathcal{X}(\mathscr{U}) = 0$. $\mathcal{X}$ is this defined as a complex valued function on a subset of $\mathscr{V}$, and is clearly multiplicative (i.e., if $\mathcal{X}(\mathscr{U})$) and $\mathcal{X}(\delta)$ are defined, $\mathcal{X}(\mathscr{U}\delta) = \mathcal{X}(\mathscr{U}\mathcal{X}(\delta))$. Note that $\mathcal{X}$ is defined in particular on all integral divisors of K.

Let $\mathcal{X}$ be a character $\mod \mathscr{F}$ of K. An integral divisor $\mathscr{F}^1$ is said to be a modulus of definition of $\mathcal{X}$ if for any $X \in K$ coprime to $\mathscr{F}$ and $X \equiv 1(\mod {}^{+}\mathscr{F}^{\infty})$ we have $\mathcal{X}((X)) = 1$. $\mathscr{F}$ itself is clearly a modulus of definition. The reason for our terminology is provided by the following

Theorem. *If $\mathcal{X}$ is a character $\mod \mathscr{F}$ and $\mathscr{F}^1$ a modulus of definition of $\mathcal{X}$, there exists a unique character $\mathcal{X}^1$ of $K \mod \mathscr{F}^1$ such that for any divisor $\mathscr{U}$ prime to $\mathscr{F}\mathscr{F}^1$,*

$$\mathcal{X}(\mathscr{U}) = \mathcal{X}^1(\mathscr{U})$$

Conversely, if $\mathcal{X}$ and $\mathcal{X}^1$ are two characters mod $\mathscr{F}$ and $\mathscr{F}^1$ respec- 90 tively such that whenever $\mathscr{U}$ is coprime to $\mathcal{F}\mathcal{F}^1$, we have $\mathcal{X}(\mathscr{U}) = \mathcal{X}^1(\mathscr{U})$, then $\mathcal{F}^\infty$ is a modulus of definition of $\mathcal{X}$ and $\mathcal{X}^1$ is the character associated to $\mathcal{X}$ by the first part of the theorem.

Proof. Suppose $\mathcal{F}^1$ is a modulus of definition of $\mathcal{X}$. If $C_{\mathcal{F}^1}$ is any class modulo $\mathcal{F}^1$, we can find a divisor $\mathscr{U}$ in $C_{\mathcal{F}^1}$ coprime to $\mathcal{F}$ and we define

$$\mathcal{X}^1(C_{\mathcal{F}^1}) = \mathcal{X}(\mathscr{U}).$$

□

The definition is independent of the choice of $\mathscr{U}$ in $C_{\mathcal{F}^1}$. For ,if $\delta \in C_{\mathcal{F}^1}$ and is coprime to $\mathcal{F}$, there exists an $X \in K$ such that $\mathscr{U}\delta^{-1} = (X), X \equiv 1(\mod {}^+\mathcal{F}^1)$ and X coprime to $\mathcal{F}$. Hence

$$\mathcal{X}(\mathscr{U}\delta^{-1}) = \mathcal{X}((X)) = 1,$$
$$\mathcal{X}(\mathscr{U}) = \mathcal{X}(\delta).$$

So defined, $\mathcal{X}^1$ is evidently a character modulo $\mathcal{F}^1$ which satisfies the condition

$$\mathcal{X}(\mathscr{U}) = \mathcal{X}^1(\mathscr{U})$$

if $\mathscr{U}$ is coprime to $\mathcal{F}\mathcal{F}'$. The uniqueness follows from the fact that this definition of $\mathcal{F}^1$ is forced upon us by the above condition.

The first of our theorem is proved.

91 To prove the second part, suppose $\mathcal{X}$ and $\mathcal{X}^1$ are two characters modulo $\mathcal{F}$ and $\mathcal{F}^1$ respectively satisfying the above condition. Then, if (X) is coprime to $\mathcal{F}$ and $X \equiv 1(\mathcal{F}^1), (X)$ is coprime to $\mathcal{F}\mathcal{F}^1$, and therefore

$$\mathcal{X}((X)) = \mathcal{X}^1((X)) = 1$$

This proves that $\mathcal{F}^1$ is a modules of definition of $\mathcal{X}$ and $\mathcal{X}^1$ the associated character $\mod \mathcal{F}^1$.

Corollary. *$\mathcal{F}$ is a modulus of definition of $\mathcal{X}^1$.*

Our next theorem states that to any given character, there exists a 'smallest' modulus of definition. To prove this, we require the following

Lemma. *If $\mathscr{F}^1$ and $\mathscr{F}''$ are two moduli of definition of a character modulo $\mathscr{F}$, their greatest common divisor $\mathscr{F}'''$ is also a modulus of definition.*

Proof. Let X be coprime to $\mathscr{F}$ and $X \equiv 1(\mod \mathscr{F}''')$. Find a $Y \in K$ such that

$$v_{\mathscr{Y}}(XY-1) \geq v_{\mathscr{Y}}(\mathscr{F}^1) + \left|v_{\mathscr{Y}}(X)\right| \text{ if } v_{\mathscr{Y}}(\mathscr{F}^1\mathscr{F}'''^{-1} > 0, \tag{1}$$

$$v_{\mathscr{Y}}(X(Y-1)) \geq v_{\mathscr{Y}}(\mathscr{F}'') + \left|v_{\mathscr{Y}}(X)\right| \text{ if } v_{\mathscr{F}}(\mathscr{F}''\mathscr{F}'''^{-1} > 0, \tag{2}$$

and $v_{\mathscr{Y}}(Y-1) \geq v_{\mathscr{Y}}(\mathscr{F}\mathscr{F}'\mathscr{F}") + \left|v_{\mathscr{Y}}(X)\right|$ if $\mathscr{Y}$ divides $\mathscr{F}\mathscr{F}'\mathscr{F}"$ but does not belong to the first two categories. (3)

Since $\mathscr{F}'''$ is the greatest common divisor of $\mathscr{F}'$ and $\mathscr{F}''$ the first two categories are mutually exclusive, and the third category is by definition exclusive of (1) or (2). □ 92

Now, one can easily verify that (Y) is coprime to $\mathscr{F}$. Hence, (XY) is also coprime to $\mathscr{F}$. We now assert that $Y \equiv 1 (\mod {}^+\mathscr{F}'')$ and $XY \equiv 1(\mod {}^+\mathscr{F}')$. To verify the first, suppose $\mathscr{Y}$ is a prime divisor dividing $\mathscr{F}''$. Then $\mathscr{Y}$ must occur in one of the three categories. If $\mathscr{Y}$ belongs to (1),

$$\begin{aligned} v_{\mathscr{Y}}(Y-1) &= v_{\mathscr{Y}}(XY-1+1-X) - v_{\mathscr{Y}}(X) \\ &\geq \min(v_{\mathscr{Y}}(XY-1), v_{\mathscr{Y}}(X-1)) - v_{\mathscr{Y}}(X), \end{aligned}$$

and since $v_{\mathscr{Y}}(X-1) \geq v_{\mathscr{Y}}(\mathscr{F}''') = v_{\mathscr{Y}}(\mathscr{F}'') > 0, v_{\mathscr{Y}}(X) = 0$, and the right hand side of the inequality becomes

$$\geq \min(v_{\mathscr{Y}}(\mathscr{F}'), v_{\mathscr{Y}}(\mathscr{F}'')) = v_{\mathscr{Y}}(\mathscr{F}'').$$

If $\mathscr{Y}$ belongs to category (2), we get

$$v_{\mathscr{Y}}(Y-1) \geq v_{\mathscr{Y}}(\mathscr{F}'') + \left|v_{\mathscr{Y}}(X)\right| - v_{\mathscr{Y}}(X) \geq v_{\mathscr{Y}}(\mathscr{F}'').$$

Finally, for $\mathscr{Y}$ in (3), we get again

$$v_{\mathscr{Y}}(Y-1) \geq v_{\mathscr{Y}}(\mathscr{F}'').$$

The second congruence $XY \equiv 1 \pmod{{}^{+}\mathcal{F}'}$ can be proved similarly. Since $\mathcal{F}'$ and $\mathcal{F}''$ are moduli of definition, we deduce that $\mathcal{X}(Y) = \mathcal{X}(XY) = 1$. Hence $\mathcal{X}(X) = 1$. This completes the proof of the fact that $\mathcal{F}'''$ is a modulus of definition.

93 The theorem we mentioned is a fairly easy consequence.

Theorem . *Let $\mathcal{X}$ be a character of $K \mod \mathcal{F}$. Then there exists a unique integral divisor m such that it divides every modulus of definition of $\mathscr{X}$ and every integral divisor which is divisible by it is a modulus of definition. m is called the conductor of $\mathcal{X}$.*

If $\mathcal{X}_1$, is the associated character to m, the conductor of $\mathcal{X}_1$ is m itself.

Proof. By the previous lemma, the g.c.d. of all moduli of definition of $\mathcal{X}$ is an integral divisor which satisfies all the conditions of the first part of the theorem. Let $\mathcal{X}_1$, be the associated character $\mod m$. If the conductor of $\mathcal{X}_1$, is m_1, it is clear that m_1 is also a modulus of definition of $\mathcal{X}$. Hence m divides m_1, and m_1 divides m since m_1 is the conductor of $\mathcal{X}_1$. Thus, $m = m_1$. Our theorem is proved. □

A character $\mathcal{F}$ modulo $\mathcal{F}$ is said to be *primitive* or *proper* if $\mathcal{F}$ is the conductor of $\mathcal{X}$.

Lecture 17

30 L-functions Modulo $\mathcal{F}$

Throughout this lecture, we shall assume that K is an algebraic function 94 field over a finite constant field k with $q = p^f$ elements. Let $\mathcal{F}$ be an integral divisor of K and $\mathcal{X}$ a character modulo $\mathcal{F}$. For a complex variable $s = \sigma +$ it $\sigma > 1$, we define the L-function w.r.t. the character $\mathcal{F}$ by the infinite series

$$L(s, \mathcal{X}) = \sum_{\mathscr{U}} \frac{\mathcal{X}(\mathscr{U})}{(N\mathscr{U})^s},$$

the summation being over all integral divisors. The absolute convergence, etc. of the series do not offer any difficulty to prove, and we may also get the following product formula:

$$L(s, \mathcal{X}, K) = \prod_{\mathscr{Y}} \left(1 - \frac{\mathcal{X}(\mathscr{Y})}{(N\mathscr{Y})^s}\right)^{-1} \text{ for } \sigma > 1.$$

31 The Functional Equations of the L-functions.

Before proceeding to the proof of the functional equation of the L-functions, we shall prove some essential lemmas. Since it is possible to prove these in a general setting, we shall do so.

Let A be a commutative algebra with unit element 1 of finite rank f over a finite k with q elements. We shall assume that a mapping $\mathcal{X}$ of A into the complex number is given with the following properties:

95 1) $\chi(X) = 0$ if and only if X is a zero divisor is A

2) $\chi(XY) = \chi(X)\chi(Y)$ for $X, Y \in A$

3) $\chi(\alpha X) = \chi(X)$ for $X \in A$ and $\alpha \in k^*$

4) If X is a zero divisor of A, there exists a Y in A such that $XY = X$ and $\chi(Y) \neq 0, \chi(Y) \neq 1$.

We shall also assume that a k-linear mapping S of A in k is given which is such that if $X \in A, X \neq 0$, There exists a $Y \in A$ such that $S(XY) = 1$. Lastly, we assume that a complex valued function ψ is given on k such that $(a)\,\psi(0) = 1$ and $(b) \sum\limits_{\alpha \in k} \psi(\alpha) = 0$. (e.g, $\psi(0)) = 1, \psi(\alpha) = -\dfrac{1}{q-1}$ for $\alpha \neq 0$ satisfies the required conditions). We then have the following lemmas.

Lemma 1. *Let V be a vector subspace of A. Then,*

$$\sum_{X \in V} \psi(S(XY)) = \begin{cases} q^{\dim V} & \text{if } Y \in V_{comp}. \\ 0 & \text{otherwise .} \end{cases}$$

Proof. If $Y \in V_{comp}, S(X, Y) = 0$ for every $X \in V$ and the first equality follows from condition (a) for ψ. □

If $Y \notin V_{comp}$, we can find $X_1 \in V$ such that $S(X_1 Y) = 1$. Complete X_1 to a basis $X_1, \ldots X_d$ of V over k. Then the sum on the left is

$$\sum_{\alpha_1,\ldots,\alpha_d \in K} \psi\left(S\left(\sum_{i=1}^{d} \alpha_i X_i Y\right)\right) = \sum_{\alpha_1,\ldots,\alpha_d \in K} \sum_{\alpha_1 \in K} \psi\left(\alpha_1 + S\left(\sum_{i=2}^{d} \alpha_1 X_i Y\right)\right) = 0,$$

since for fixed $\alpha_2, \ldots \alpha_d$, the sum $\alpha_1 + S(\sum_{i=2}^{d} \alpha_i X_i Y)$ runs through all elements of k when α_1 does. Our lemma is proved.

96 **Lemma 2.** *Define the generalised Gaussian sum $G(X, \chi)$ for $X \in A$ by*

$$G(X, \chi) = \sum_{Y \in A} \chi(Y) \psi(S(XY)).$$

Then we have

$$G(X,\chi) = \overline{\chi(X)}G(1,\chi)$$

Proof. Since A is a finite algebra every non-zero divisor is a unit. (In fact, if u is a non-zero divisor, $ua \neq ub$ if $a \neq b$, and since A is a finite set, $uA = A$. In particular, there exists and element $u^1 \in A$ with $uu^1 = 1$). □

Now, if X is a zero divisor, there exists an element $u \in A$ by 4) with $Xu = X$ and $\chi(u) \neq 0$ or 1; thus, u, is a non-zero divisor. Hence we obtain

$$G(X,\chi) = \sum_{Y\in A}\chi(Y)\psi(S(XuY)) = \sum_{Y\in A}\chi(Yu^{-1})\psi(S(XY))$$
$$= \chi(u^{-1})G(X,\chi),$$

and since $\chi(u^{-1}) = \chi^{-1}(u) \neq 1, G(X,\chi) = 0 = \overline{\chi(X)}G(1,\chi)$. If X is not a zero divisor,

$$G(X,\chi) = \sum_{Y\in A}\chi(Y)\psi(S(XY)) = \sum_{Y\in A}\chi(X^{-1}Y)\psi(S(Y)) = \chi^{-1}(X)G(1,\chi).$$

Now, the units of A form a finite group and therefore there exists an integer $n \neq 0$ with $X^n = 1$. Hence $\chi^n(X) = \chi(X^n) = \chi(1) = 1, |\chi(X)| = 1$ and $\chi^{-1}(X) = \overline{\chi(X)}$. The lemma is proved.

Lemma 3. *Let V be a subspace of A and* 97

$$M(V,\chi) = \sum_{X\in V}\chi(X).$$

Then,

$$M(V_{comp},\bar{\chi}) = q^{-\dim V}\Delta(\chi)M(V,\chi),$$

where $\Delta(\chi)$ depends only on χ and $|\Delta(\chi)| = q^{f/2}$

Proof. By the first two lemmas, we have

$$q^{-\dim V}M(V_{comp},\bar{\chi}) = \sum_{X\in V_{comp}}\bar{\chi}(X)q^{\dim V} = \sum_{X\in A}\bar{\chi}(X)\sum_{X\in V}\psi(S(XY))$$
$$= \sum_{Y\in V}\sum_{X\in A}\bar{\chi}(X)\psi(S(XY))\sum_{Y\in V}G(Y,\bar{\chi}) = \sum_{Y\in V}\chi(Y)G(1,\bar{\chi}) = G(1,\bar{X})M(V,\chi)$$

□

Put $\Delta(\chi) = G(1, \overline{\chi})$. It only remains to prove that $|G(1, \overline{\chi})| = q^{f/2}$.

Now, k can be imbedded in A by the mapping $\alpha \in k \to \alpha 1 \cdot \in A$. Also,

$$M(k, \chi) \sum_{\alpha \in k} \chi(\alpha) = \sum_{\alpha \in k^*} \chi(1) = q - 1 \neq 0.$$

Choose ψ to be real. Taking $V = k$ in the above formula, we obtain

$$G(1, \chi) G(1, \overline{\chi}) M(k, \chi) = G(1, \chi) q M(k_{comp} \overline{\chi}) = q^{\dim k_{comp} + 1} M(k, \chi),$$
$$G(1, \chi) G(1, \overline{\chi}) = q^f$$

But since ψ is real, $G(1, \overline{\chi}) = \overline{G(1, \chi)}$, and therefore

$$|\Delta(\chi)| = |G(1, \overline{\chi})| = q^{f/2}$$

98 Our lemma is proved.

Since we had $\Delta(\overline{\chi}) = G(1, \chi)$, we see that $G(1, \chi)$ does not depends on the function ψ. By lemma 2, it follows that $G(X, \chi)$ is independent of ψ. (This may also be proved directly.)

We now proceed to the functional equation

Theorem . *Let $\mathcal{F}$ be an integral divisor which is not the unit divisor and χ a proper character modulo $\mathcal{F}$. Then $L(s, \chi, K)$ is a polynomial in $U = q^{-s}$ of degree $2g - 2 + d(\mathcal{F})$ and satisfies the functional equation*

$$q^{s(g-1+\frac{1}{2}d(\mathcal{F}))} L(s, \chi, K) = \epsilon(\chi) q^{(1-s)(g-1+\frac{1}{2}d(\mathcal{F}))} L(1 - s, \overline{\chi}, K)$$

where $\epsilon(\chi)$ is a constant depending on χ, with $|\epsilon(\chi)| = 1$.

Proof. Let $\underline{R}$ be the algebra $\Gamma(\mathcal{N} / \mathcal{U}_1, \ldots \mathcal{U}_r)$, i the ideal $\Gamma(\mathcal{F} / \mathcal{U}_1, \ldots \mathcal{U}_r)$ and $\overline{R}$ the quotient algebra R/i. □

Now, if $X \in R, X \neq 0$, $\mathcal{N}_X$ is prime of $\mathcal{F}$ and $\chi((X))$ is meaningful. We shall show that $\chi((X))$ is constant on the cosets modulo the ideal i.

Let $X, Y \in R, X - Y \in i$. If (X) is not coprime to $\mathcal{F}, (Y)$ cannot be coprime to $\mathcal{F}$ and therefore $\chi((X)) = \chi((Y)) = 0$. If X is coprime to $\mathcal{F}$, we have

$$v_{\mathcal{U} i}\left(\frac{Y}{X} - 1\right) = v_{\mathcal{U} i}(Y - X) \geq v_{\mathcal{U} i}(\mathcal{F}),$$

and hence $\dfrac{Y}{X} \equiv 1(\mod {}^{+}\mathscr{F}), \chi(X) = \chi(Y)$.

Thus, we may define for $\bar{X} \in \bar{R}$ a mapping which again we shall denote by χ by the equation

$$\chi(\bar{X}) = \chi((X)).$$

99 Clearly we have $\chi(\bar{X})\chi(\bar{Y}) = \chi(\overline{XY})$ and $\chi(\alpha\bar{X}) = \chi(\bar{X})$ if $\alpha \in k^{*}$. Also, $\chi(\bar{X}) = 0$ if and only if $\nu_{\mathscr{U}_i}(X) > 0$ for some i. Find a $Y \in K$ such that

$$\nu_{\mathscr{U}_i}(Y) = \nu_{\mathscr{U}_i}(\mathscr{F}) - \nu_{\mathscr{U}_i}(X)$$
$$\nu_{\mathscr{U}_i}(Y) = \nu_{\mathscr{U}_i}(\mathscr{F}) \text{ for } j \neq i.$$

Then, $\bar{Y} \in \bar{R}, \bar{Y} \neq 0$ and $\bar{X}\bar{Y} = 0$. Thus $\chi(\bar{X}) = 0$ implies that $\bar{X}$ is a zero divisor. Conversely, if $\bar{X}$ is a zero divisor, we should have $\nu_{\mathscr{U}_i}(X) > 0$ for some i and therefore $\chi(\bar{X}) = 0$.

Now, suppose $\bar{Z}$ is a zero divisor in $\bar{R}$. Then $\nu_{\mathscr{U}_i}(Z) > 0$ for some i. Since χ is proper character modulo $\mathscr{F}, \mathscr{F}^{-1}_{\mathscr{U}_i}$ is not a modulus of definition of χ. Hence there exists an element $X \in K^{*}$, with (X) coprime to $\mathscr{F}, X \equiv 1(\mod {}^{+}\mathscr{F}\mathscr{U}_i^{-1})$, and $\chi((X)) \neq 1$. Then we have $(X-1)Z \equiv 0(\mod {}^{+}\mathscr{F}), \bar{X}\bar{Z} = \bar{Z}$, and $\chi(\bar{X}) \neq 0$ or 1.

Hence, the map χ on $\bar{R}$ satisfies the conditions 1), 2), 3) and 4) stipulated at the beginning of this lecture. We have already seen (Lecture 14) that if ω is a differential such that $\mathscr{F}(\omega)$ is coprime to $\mathscr{F}, S(\bar{X}) = S(X) = \sum\limits_{i=1}^{r} \omega^{\mathscr{U}_i}(X)$ has all the requisite properties. Now,

$$L(s, \chi, K) = \sum_{C} q^{-sd(c)} \sum_{\mathscr{U} \in C} \chi(\mathscr{U}),$$

where the first summation is over all classes C and the second over all integral divisors in the class C. Choose a divisor $\mathscr{U}_C$ in the class C 100
coprime to $\mathscr{F}$. We have

$$\sum_{\mathscr{U} \in C} \chi(\mathscr{U}) = \frac{\chi(\mathscr{U}_C)}{q-1} \sum_{X \in L^{*}(\mathscr{U}_C^{-1})} \chi((X)),$$

since every integral divisor $\mathscr{U} \in C$ can be written in precisely $(q-1)$ ways in the form $(X)\mathscr{U}_C$, where X is a non-zero element of $L(\mathscr{U}_C^{-1})$.

Again, since $\mathscr{U}_C$ is coprime to $\mathscr{F}, L(\mathscr{U}_C^{-1}) \subset R$ and two elements of $L(\mathscr{U}_C^{-1})$ go to the same coset modulo i if and only if their difference in $L(\mathscr{U}_C^{-1})\mathscr{F}$. We therefore have

$$\sum_{\mathscr{U} \in C} \chi(\mathscr{U}) = \frac{\chi(\mathscr{U}_C)}{q-1} q^{l(\mathscr{U}_C^{-1}\mathscr{F})} \frac{\sum \chi(\bar{X})}{\bar{X} \in L(\mathscr{U}_C^{-1})}$$

Applying lemma 3 with $V = \overline{L(\mathscr{U}_C^{-1})}$, we have

$$\sum_{\bar{X} \in L(\mathscr{U}_C^{-1})} \chi(\bar{X}) = M(V,\chi) = \Delta^{-1}(\chi) q^{\dim V} M(V_{comp}, \bar{\chi}).$$

But by the theorem of lecture 14, we have

$$\overline{L(\mathscr{U}_C^{-1})}_{compl.} = \overline{L(\mathscr{U}_C \mathscr{F}(\omega))}$$

Now, if $d(C) < 0, N(C) = l(\mathscr{U}_C^{-1}) = 0$ and hence $M(V,\chi) = 0$. Also, if $d(C) > 2g-2+d(\mathscr{F}), d(C^{-1}\mathscr{F}W) < 0$, and $N(C^*) = l(\mathscr{U}_C\mathscr{F}(\omega)) = 0$; hence again $M(V,\chi) = 0$. Substituting in the expression for $L(s,\chi,K)$, we see that it is a polynomial in $U = q^{-s}$ of degree at most $2g-2+d(\mathscr{F})$.

101 We have

$$(q-1)L(s,x,K) = \sum_C q^{-sd(C)} \chi(\mathscr{U}_C) q^{l(\mathscr{U}_C^{-1}\mathscr{F})} M(\overline{L(\mathscr{U}_C^{-1})}, \chi)$$

$$= \frac{1}{\Delta(\chi)} \sum_C q^{-sd(C)+N(C)} \chi(\mathscr{U}_C) M(\overline{L(\mathscr{U}_c^{-1})}_{comp} \bar{\chi}) \qquad \text{by lemma 3,}$$

$$= \frac{1}{\Delta(\chi)} \sum_C q^{-sd(C)+N(C)} \chi(\mathscr{U}_C) M(L((\mathscr{U}_c^{-1})^*)\bar{\chi})$$

by the theorem of lecture 14,

$$= \frac{1}{\Delta(\chi)} \sum q^{(1-s)d(C)-g+1+N(WC^{-1})} \bar{\chi}(\mathscr{U}_C^{-1}) M(L(\mathscr{U}_C^{-1})^*), \bar{\chi})$$

$$= \frac{\chi(\omega)\mathscr{F}}{\Delta(\chi)} q^{(2s-1)(1-g)+(1-s)d(\mathscr{F})}$$

$$\times \sum_{C} q^{(1-s)d(C^*)} \overline{\chi}((\mathscr{U}_C^{-1})^{*-1}) q^{l(\mathscr{U}_C^{-1})\mathcal{F}^*)} M(L((\mathscr{U}_C^{-1})^*), \chi)$$

$$= (q-1)\frac{\chi((\omega)\mathcal{F})}{\Delta(\chi)} q^{(2s-1)(1-g)+(1-s)d(\mathcal{F})} L(1-s, \overline{\chi}, K), \quad \text{since } C^*$$

runs through all classes as C does. This gives

$$q^{s(g-1+\frac{1}{2}d(\mathcal{F}))} L(s, \chi, K) = \epsilon(\chi) q^{(1-s)(g-1+\frac{1}{2}d(\mathcal{F}))} L(1-s, \overline{\chi}, K),$$

where $$\epsilon(\chi) = \frac{\chi((\omega)\mathcal{F}) q^{\frac{1}{2}d(\mathcal{F})}}{\Delta(\chi)}, |\epsilon(\chi)| = 1.$$

That the degree in U of $L(s, \chi, K)$ is exactly $2g - 2 + d(\mathcal{F})$ follows by comparing the coefficients of highest powers on both sides of the equation. Our theorem is proved.

Lecture 18

32 Extensions of Algebraic Function Fields

In the next five Lectures, we shall investigate the relations between an algebraic function field and an extension of it (see below for definition). In particular, we consider in the end the connection between the ζ-function of a function field and the ζ-function of a constant field extension. This gives in particular the interesting result that for algebraic function fields over a finite constant field, the smallest positive degree of a divisor is 1. 102

We start with the definition of an extension.

Definition . *Let K be an algebraic function field with constant field k. An extension of K an algebraic function field L with constant field l such that $L \supset K$ and $l \cap K = k$.*

Now let L/l be an extension of K/k and $\mathscr{K}$ a prime divisor of L. If $v_{\mathscr{K}}(X) = 0$ for all $X \in \mathscr{K}$ is said to be *variable over K* or *trivial* on K. If this were not true, the restriction of $v_{\mathscr{K}}$ to K defines a valuation of K trivial on k and should therefore correspond to a prime divisor $\mathscr{Y}$ of K. In this case, $\mathscr{K}$ is said to be *fixed on* K and is said to lie over the prime divisor $\mathscr{Y}$ of K. Also, since the restriction of $v_{\mathscr{K}}$ to K and $v_{\mathscr{Y}}$ are equivalent valuations with values in Z, the latter having the whole of Z for its value group, there exist a positive integer $e_{L/K}(\mathscr{K})$ such that

$$v_{\mathscr{K}}(X) = e_{L/K} v_{\mathscr{Y}}(X) \text{ for all } X \in K$$

$e_{L/K}(\mathscr{K})$ is called *ramification index* of $\mathscr{K}$ over K. 103

The relation between the residue fields of $\mathscr{K}$ and $\mathscr{Y}$ is given by the following

Lemma . *If L/l is an extension of K/k and a prime divisor $\mathscr{K}$ of L lies over a prime divisor $\mathscr{Y}$ of K, the residue field $K_{\mathscr{Y}}$ of $\mathscr{Y}$ can be canonically imbedded in the residue field $L_{\mathscr{K}}$ of $\mathscr{Y}$*

Proof. Let $\mathscr{O}, \mathscr{K}$ denote respectively the valuation ring and maximal ideal of $\mathscr{K}$ and $\mathscr{O}$ and $\mathscr{Y}$ those of $\mathscr{Y}$. Since $v_{\mathscr{K}}$ and $v_{\mathscr{Y}}$ are equivalent on K, we clearly have $\mathscr{O} \supset \mathscr{Y}$ and $\mathscr{Y} = \mathscr{O} \cap \mathscr{K}$. Hence we have monomorphism $\mathscr{Y} = \mathscr{O}/\mathscr{Y} \to \mathscr{O}/\mathscr{K} = L_{\mathscr{K}}$ and $K_{\mathscr{Y}}$ can be considered as imbedded as a subfield of $L_{\mathscr{K}}$. □

We now give condition for L/K to be a finite or an arbitrary algebraic extension.

Lemma . *Let L/l be an extension of K/k. Then among the following statements, (1), (2) and (3) are equivalent and so are* (1′), (2′) *and* (3′).

(1)	$[l : k] < \infty$	(1′)	l is algebraic over k.
(2)	$[L : K] < \infty$	(2′)	L is algebraic over K
(3)	If $\mathscr{K}$ is any prime divisor of L lying over the prime divisor $\mathscr{Y}$ of $K[L_{\mathscr{K}} : K_{\mathscr{Y}}] < \infty$	(3')	If $\mathscr{K}$ is any prime of L lying over the prime divisor $\mathscr{Y}$ of $K, L_{\mathscr{K}}$ is algebraic over $K_{\mathscr{Y}}$

Proof. We shall show that (1) ⇔ (2) ⇔ (3). The proof that (1)′ ⇔ (2)′ ⇔ (3)′ is similar, and even simpler □

The equation (valid even when either side is infinite)

$$[L_{\mathscr{K}} : k] = [L_{\mathscr{K}} : K_{\mathscr{Y}}][K_{\mathscr{Y}} : k] = [L_{\mathscr{K}} : l][l : k]$$

104 show that (1) ⇔ (3) since $[K_{\mathscr{Y}} : k]$ and $[L_{\mathscr{Y}} : l]$ are both finite.

We shall now prove that (1) ⇔ (2). Let X be any transcendental elements of K over k. Since $X \notin k$ and $L \cap k = l$, $X \notin l$ and is therefore transcendental over 1. It follows that $[K : k(X)] < \infty$ and $[L : l(X)] < \infty$, and from the equalities

$$[L : k(X)] = [L : K][K : k(X)] = [L : l(X)][l(X) : k(X)],$$

it follows that $[L : K] < \infty \Leftrightarrow [l(X) : k(X)] < \infty$.

We shall now prove that $[l(X) : k(X)] = [l : k]$, which would finish the proof of the theorem.

Suppose $\alpha_1, \ldots, \alpha_n$ are n linearly independent element of l over K. We assert that they are also linearly independent over $k(X)$. For it there were a linear relation among these with coefficients in $k(X)$ with at least one non-vanishing coefficient, we may clearly assume that it is of the form

$$\sum_{i=1}^{n} \alpha_i g_i(X) = 0$$

at least one $g_i(X)$ with a non-zero constant term. Since X is transcendental over l, we may put $X = 0$ in the above equation to obtain a linear relation among the α_1 over k with at least one non-zero co-efficient. But this is impossible since the α_i are linearly independent by a assumption. Hence, $[l(X); k(X)] \geq [l : k]$.

To prove the reverse inequality, we may assume that $[l : k] < \infty$. 105
Hence, there exists a finite set $\beta_1, \ldots \beta_r$ of element of l such that $l = k(\beta_1, \ldots \beta_r)$. Then

$$\begin{aligned}
[l(X) : k(X)] &= [k(X, \beta_1, \ldots, \beta_r) : k(X)] \\
&= [k(X), \beta_1, \ldots \beta_r] : k(X, \beta_1, \ldots, \beta_{r-1}).[k(X, \beta_1, \ldots, \beta_{r-1})] : \\
&\qquad k[X, \beta_1, \ldots, \beta_{r-2}] \ldots [k(X, \beta_1) : k(X)] \\
&\leq [k, \beta_1, \ldots \beta_r] : k(, \beta_1, \ldots, \beta_{r-1}).[k(, \beta_1, \ldots, \beta_{r-2})] : \\
&\qquad k[, \beta_1, \ldots, \beta_{r-2}] \ldots [k(\beta_1) : k(X)]
\end{aligned}$$

since the degree of β_1 over $k(X, \beta_1 \cdots \beta_{i-1})$ is less than or equal to its degree over the smaller field $k(\beta_1 \cdots \beta_{i-1})$, $[k(\beta_1 \cdots \beta_r) : k] = [l : k]$.

The proof of the lemma is completed.

We shall call an extension L/l over K/k satisfying any of the conditions (1), (2), (3) of lemma a finite extension. If $\mathscr{K}$ is a prime divisor of L lying over a prime divisor $\mathscr{Y}$ of K, the positive integer $[L_{\mathscr{K}} : K_{\mathscr{Y}}] = d_{L/K}(\mathscr{K})$ is called the relative degree of $\mathscr{K}$ over K. It follows from the proof of the above lemma that

$$d_{L/K}(\mathscr{K}) = \frac{[L_{\mathscr{K}} : l][l : k]}{[K_{\mathscr{Y}} : k]} = \frac{d_L(\mathscr{K})}{d_K(\mathscr{Y})}[l : k],$$

$$d_L(\mathscr{K})[l:k] = d_{L/K}(\mathscr{K})d_K(\mathscr{Y})$$

106 (The suffix to d indicated the field in which the degree is taken)

If L/l is an algebraic extension of K/k, there does not exist any prime divisor of L which is variable over K. For, suppose v is a valuation on L which is trivial on K. Any elements $\alpha \in L$ satisfies an irreducible equation

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, a_i \in K,$$

so that
$$0 = v(a_n) = v(\alpha) + v(\alpha^{n-1} + \quad + a_{n-1})$$

If $v(\alpha) > 0$, we have

$$v(\alpha^{n-1} + \cdots + a_{n-1}) = \min((n-1)v(\alpha), (n-2)v(\alpha), \quad 0) = 0,$$

and we obtain a contradiction by substituting in the previous equation. Thus, v cannot be positive for any element of L, which is impossible.

Now, let L/l be any extension of K/k. We shall prove that there are at most a finite number of prime divisors of L lying over a given prime divisor $\mathscr{Y}$ of K, and that there is at least one.

Let g be the genus of K and let C be the class of the divisor $\mathscr{Y}^{g+1}$. Since $d(C) = d(\mathscr{Y}^{g+1}), \geq g+1$, we have

$$N(C) \geq d(C) - g + 1 \geq 2,$$

and there exists at least one more integral divisor $\mathscr{U}$ in C. Then, $\mathscr{Y}^{g+1}$ $\mathscr{U}^{-1} = (X)_K$ where $X \in K$ and X transcendental over k. Hence X is also transcendental over l and the divisor $(X)_L$ has a decomposition $(X)_L = \dfrac{\mathscr{K}_1^{a_1} \mathscr{K}_h^{a_h}}{\mathscr{N}_X}$, where $h \geq 1$, and $a_i > 0$. We assert that 107 $\mathscr{K}_1, \ldots \mathscr{K}_n$ are precisely the divisors of L lying over $\mathscr{Y}$. For, if $\mathscr{K}$ lies over $\mathscr{Y}, v_{\mathscr{K}}(X) > 0$ and hence should be one of the $\mathscr{K}_i$; and since $v_{\mathscr{K}_i}(X) > 0$, the restriction of $v_{\mathscr{K}_i}$ to K should be a prime divisor occurring in the numerator of $(X)_K$, and the only such prime divisor is $\mathscr{Y}$. Our contention is proved.

We now have the

Theorem. *Suppose L/l is an algebraic extension of K/k. Let $\mathscr{Y}$ be a prime divisor of K and $\mathscr{K}_1, \ldots \mathscr{K}_h$ all the prime divisors of L lying over $\mathscr{Y}$. Then,*

$$[L : K] = \sum_{\nu=1}^{h} d_{L/K}(\mathscr{K}_\nu) e_{L/K}(\mathscr{K}_\nu)$$

Proof. Choose an element $X \in K$ as above. We have

$$(X)_k = \frac{\mathscr{Y}^t}{(\mathscr{N}_X)_K}$$

and
$$(X)_L = \frac{(\mathfrak{z}_X)_L}{(\mathscr{N}_X)_L} = \frac{\mathscr{K}_1^{v_{\mathscr{K}_1}(X)} \mathscr{K}_2^{v_{\mathscr{K}_2}(X)} \ldots \mathscr{K}_h^{v_{\mathscr{K}_h}(X)}}{(\mathscr{N}_X)_L}$$

Therefore we have

$$[L : l(X)] = d((\mathfrak{z}_X)_L) = \sum_{\nu=1}^{h} v_{\mathscr{K}_\nu}(X) d_L(\mathscr{K}_\nu) = v_{\mathscr{Y}}(X) \sum_{\nu=1}^{h} e_{L/K}(\mathscr{K}_\nu) d_L(\mathscr{K}_\nu)$$

and on the other hand

$$[K : k(X)] = d_K(\mathscr{Y}^t) = t d_K(\mathscr{Y}) = v_{\mathscr{Y}}(X) d_K(\mathscr{Y}).$$

□

Hence, 108

$$[L : K] = \frac{[L : l(X)][l(X) : k(X)]}{[K : k(X)]} = \frac{[l : k]}{d_K(\mathscr{Y})} \sum_{\nu=1}^{h} e_{L/K}(\mathscr{K}_\nu) d_L(\mathscr{K}_\nu)$$
$$= \sum_{\nu=1}^{h} e_{L/K}(\mathscr{K}_\nu) d_{L/k}(\mathscr{K}_\nu),$$

which is the formula we want.

As corollaries, we deduce the inequalities

$$h \leq [L : K],$$
$$d_{L/K}(\mathscr{K}_\nu) \leq [L : K]$$
and
$$e_{L/K}(\mathscr{K}_\nu) \leq [L : K].$$

Lecture 19

33 Application of Galois Theory

We shall now recall some basic facts of Galois theory which we shall use in the sequel. 109

Let A be a field and B a finite algebraic extension of $A.B_s$ shall denote the subfields of all separable elements over A of B. The *separable degree* $[B : A]_s$ is then define to be the degree of the field B_s over $A.B$ is a purely inseparable extension over B_s and its degree is called the *degree of inseparability* of B over A, and is denoted by $[B : A]_i$. We obtained the relation

$$[B : A] = [B : B_s].[B_s : A] = [B : A]_s.[B : A]_i$$

If B/A is a normal extension, we define the *Galois group* $G(B/A)$ to be the group of all automorphisms of B which leave all the elements of A fixed. The set A_1 of all elements left fixed by every automorphism belonging to $G(B/A)$ is clearly a field containing A. It is called the *fixed field* of $G(B/A)$. A_1 is a purely inseparable extension of A and B a separable extension of A_1, and we have

$$[B : A_1] = [B : B]_s, [A_1 : A] = [B : A]_i.$$

We shall now apply these facts to the theory of algebraic functions. Let L/l ba a extension of K/k. We define the *relative separable degree* $d_{L/K}(\mathscr{K})_s$ *and the relative inseparable degree* $d_{L/K}(\mathscr{K})_i$ of a prime divisor $\mathscr{K}$ of L lying over the prime divisor $\mathscr{Y}$ of K to be respectively $[L_{\mathscr{K}} : K_{\mathscr{Y}}]_s$ and $[L_{\mathscr{K}} : K_{\mathscr{Y}}]_i$. $\mathscr{K}$ is said to be *separable, inseparable* 110 *or purely inseparable* accordingly as $d_{L/_K}(\mathscr{K})_i$ is equal to one, greater than one or equal to $d_{L/_K}(\mathscr{K})$.

Suppose now that $L^1/_{l'} \supset L/l \supset K/_k$ is a tower of algebraic function fields. Let $\mathscr{K}^1$ be a prime divisor of L^1 lying over a prime divisor $\mathscr{K}$ of L, which again lies over a prime divisor $\mathscr{Y}$ of K. It is easy to see that the following relation between the ramification indices holds

$$e_{L'/K}(\mathscr{K}^1) = e_{L'}(\mathscr{K}^1).e_{L/K}(\mathscr{K})$$

If moreover we assume that $[L^1 : K] < \infty$, we have

$$d_{L^1/_K}(\mathscr{K}^1) = d_{L^1/_L}(\mathscr{K}^1) d_{L/_K}(\mathscr{K}),$$

and similar relations for the separable and inseparable degrees.

Now, suppose $L/_l$ and $L^1/_{l^1}$ are two extensions of $K/_k$ and σ is an isomorphism of L onto L^1 which maps l on l^1 and fixes every element of K. If $\mathscr{K}$ is any prime divisor of L, we define the prime divisor $\sigma\mathscr{K}$ in L^1 by the equation

$$v_{\sigma\mathscr{K}}(Y) = v_{\mathscr{K}}(\sigma^{-1}Y) \text{ for } Y \in L^1.$$

Clearly, $\mathscr{K} \to \sigma\mathscr{K}$ is a one-one and onto mapping of the set of prime divisors of L onto the prime divisors of L^1. It is also immediate 111 that the isomorphism σ maps the valuation ring and the maximal ideal of $\mathscr{K}$ onto those of $\sigma\mathscr{K}$. Hence we have an induced isomorphism $\bar{\sigma} : L_{\mathscr{K}} \to L^1_{\sigma\mathscr{K}}$ of the residue class fields. If $\mathscr{K}$ lies over a prime divisor $\mathscr{Y}$ of K, $\sigma\mathscr{K}$ also lies over $\mathscr{Y}$ and $\bar{\sigma}$ fixes every element of $K_{\mathscr{Y}}$.

From these facts, it follows that

$$e_{L^1/K}(\sigma\mathscr{K}) = e_{L/_K}(\mathscr{K})$$

and if $[L : K] < \infty$

$$d_{L^1/_K}(\sigma\mathscr{K}) = d_{L/_K}(\mathscr{K}).$$

We have the following theorem for finite normal extensions.

Theorem. *Let L_l be a finite normal extension of K/k, and $\mathscr{K}$ a prime divisor of L lying over a prime divisor $\mathscr{Y}$ of K. Then every prime divisor of L lying over $\mathscr{Y}$ is of the form $\sigma\mathscr{K}$, where σ is an element of $G(L/K)$*

Proof. We have already seen that $\sigma\mathscr{K}$ lies over $\mathscr{Y}$ for every $\sigma \in G(L/K)$. To prove the converse statement, let $\mathscr{K} = \mathscr{K}_1, \ldots, \mathscr{K}_h$ be all the prime divisors of L lying over $\mathscr{Y}$. Find $aY \in L$ such that

$$\begin{aligned} &v_{\mathscr{K}}(Y) > 0\\ &v_{\mathscr{K}_j}(Y) = 0 \text{ for } j = 2, \ldots h. \end{aligned}$$

□

Then ,

$$v_{\mathscr{K}}(N_{L/_K}Y) = [L:K]_i \sum_{\sigma \in G(L/K)} v_K(\sigma Y) = [L:K]_i \sum_{\sigma \in G(L/K)} v_{\sigma^{-1}\mathscr{K}}(Y) > 0,$$

since each $\sigma^{-1}\mathscr{K}$ for $\sigma \in G(L/K)$ is a certain $\mathscr{K}_i$. Because $\mathscr{K}$ lies over $\mathscr{Y}$, we deduce that 112

$$v_{\mathscr{Y}}(N_{L/_K}Y) > 0,$$

and consequently for $j = 2, \ldots, h$, we have

$$v_{\mathscr{K}_j}(N_{L/_K}Y) = [L:K]_i \sum_{\sigma \in G(L/K)} v_{\sigma^{-1}\mathscr{K}_j}(Y) > 0.$$

Since at least one term of the sum on the right must be positive, and since the only prime divisor lying over $\mathscr{Y}$ whose valuation on Y is positive is $\mathscr{K}$, there exists an automorphism σ_j such that $\mathscr{K} = \sigma_j^{-1}\mathscr{K}_j$, $\mathscr{K}_j = \sigma_j\mathscr{K}$ for every j. Our theorem is proved.

For the rest of the lecture, we shall assume that L/l is a finite normal extension of K/k and $G(L/K)$ the Galois group.

If $\mathscr{K}$ is a prime divisor of L, we define the *decomposition group* (Zerlegungs gruppe) $Z(\mathscr{K})$ of $\mathscr{K}$ to be the subgroup of $G(L/K)$ of all elements $\sigma \in G(L/K)$ such that $\sigma\mathscr{K} = \mathscr{K}$. It follows that if $\sigma, \sigma^1 \in G(L/K)$, $\sigma\mathscr{K} = \sigma^1\mathscr{K}$ if and only if σ and σ^1 belong to the same left coset of $G(L/K)$ modulo $Z(\mathscr{K})$. Because of the above theorem, we are able to deduce that the number of prime divisors of L lying over a fixed prime divisor of K is equal to the index in $G(L/K)$ of the decomposition group of any one of them.

It is also easy to obtain the relation between the decomposition groups of two prime divisors $\mathscr{K}$ and $\sigma\mathscr{K}$ lying over the same prime divisor of K. In fact, we have

$$\tau \in Z(\sigma\mathscr{K}) \Leftrightarrow \tau\sigma\mathscr{K} = \sigma\mathscr{K} \Leftrightarrow \sigma^{\gamma}\tau\sigma\mathscr{K} = \mathscr{K} \Leftrightarrow \sigma^{-1}\tau\sigma \in Z(\mathscr{K})$$

113 and therefore $Z(\sigma\mathscr{K}) = \sigma Z(\mathscr{K})\sigma^{-1}$

Theorem. *Let $\mathscr{K}$ be a prime divisor of L lying over the prime divisor $\mathscr{Y}$ of K. Then $L_{\mathscr{K}}/K_{\mathscr{Y}}$ is a normal extension. Every element σ of $Z(\mathscr{K})$ induces an automorphism $\bar{\sigma}$ of $L_{\mathscr{K}}$ over $K_{\mathscr{Y}}$, and every automorphism of $L_{\mathscr{K}}$ over $K_{\mathscr{Y}}$ is got in this way.*

Proof. Let $\mathscr{K} = \mathscr{K}_1, \mathscr{K}_2, \ldots, \mathscr{K}_h$ be all the prime divisors of L lying over $\mathscr{Y}$. If $\bar{y} \in L_{\mathscr{K}}$, we can find a representative of $\bar{y}$ in the valuation ring $\mathscr{O}_{\mathscr{K}}$ of $\mathscr{K}$ such that

$$v_{\mathscr{K}_j}(y) > 0 \text{ for } j = 2, \ldots, h.$$

□

In fact, if y^1 is any representative of $\bar{y}$, choose a $y \in L$ such that

$$v_{\mathscr{K}}(y - y^1) > 0$$
$$v_{\mathscr{K}\,j}(y) > 0 \text{ for } j = 2, \ldots, h.$$

y satisfies the required condition.

The field polynomial of y over K is given by

$$f(X) = \left\{\prod_{\sigma\in G}(X - \sigma y)\right\}^{[L:K]_i}$$

Now, if $\sigma \notin Z(\mathscr{K}), \sigma^{-1}\mathscr{K} \neq \mathscr{K}$ and therefore $v_{\mathscr{K}}(\sigma y) = v_{\sigma^{-1}\mathscr{K}}$ $(y) > 0$. Passing to the quotient modulo $\mathscr{K}$ in the above equation, we get

$$\overline{f(X)} = \left\{\prod_{\sigma\in Z(\mathscr{K})}(X - \overline{\sigma y})\right\}^{[L:K]_i} X^M,$$

114 where M is a non-negative integer. But this is a polynomial over $K_{\mathscr{Y}}$ which is satisfied by $\bar{y}$, and which has all its roots lying in $L_{\mathscr{K}}$. $L_{\mathscr{K}}$ is thus a normal extension of $K_{\mathscr{Y}}$.

Now if $\sigma \in Z(\mathscr{K}), \sigma\mathscr{K} = \mathscr{K}$ and by what we have already seen, σ induces a $K_{\mathscr{Y}}$ isomorphism $\bar{\sigma}$ of $L_{\mathscr{K}}$ onto $L_{\mathscr{K}}$, i.e. an automorphism of $L_{\mathscr{K}}$. To prove the final part of the theorem, notice that $L_{\mathscr{K}}$ is a separable extension of the fixed field $(K_{\mathscr{Y}})$ of the Galois group $G(L_{\mathscr{K}}/K_{\mathscr{Y}})$, and is therefore simple. Hence any automorphism of $L_{\mathscr{K}}/K_{\mathscr{Y}}$ is uniquely determined by its effect on a single element $\bar{y}$. But the working above proves that every conjugate of $\bar{y}$ io of the form $\overline{\sigma y} = \bar{\sigma}(\bar{y})$ for some $\sigma \in G(L/K)$. Hence every automorphism of $L_{\mathscr{K}}$ over $K_{\mathscr{Y}}$ is of the form $\bar{\sigma}$ with $\sigma \in G(L/K)$. Our theorem is proved.

We define the *inertia group* $T(\mathscr{K})$ of a prime divisor $\mathscr{K}$ of L to be the subgroup of all elements σ of $Z(\mathscr{K})$ for which $\bar{\sigma}$ is the identity automorphism of $L_{\mathscr{K}}$. It is clearly a normal subgroup of $Z(\mathscr{K})$. The theorem proved above then establishes an isomorphism $G(L_{\mathscr{K}}/K_{\mathscr{Y}}) \simeq \dfrac{Z(\mathscr{K})}{T(\mathscr{K})}$.

We now given some consequences of the theorems of this lecture.

1. $[G : (e)] = [L : K]_s = h[Z(\mathscr{K}) : (e)]$.

2. $[Z(\mathscr{K}) : T(\mathscr{K})] = [L_{\mathscr{K}} : K_{\mathscr{Y}}]_s = d_{L/K}(\mathscr{K})_s$

3. $[L; K] = \sum\limits_{\nu=1}^{h} e_{L/_K}(\mathscr{K}_\nu) d_{L/_K}(\mathscr{K}_\nu) = he_{L/_K}(\mathscr{K}) d_{L/_K}(\mathscr{K})$

$$\begin{aligned} \therefore\ e_{L/_K}(\mathscr{K}) d_{L/K}(\mathscr{K}) &= \frac{[L : K]}{[L : K]_s}[Z(\mathscr{K}) : (e)] \\ &= [L : K]_i [Z(\mathscr{K}) : (e)] \end{aligned}$$

Hence, 115

4. $[Z(\mathscr{K}) : (e)] = \dfrac{e_{L/K}(\mathscr{K}) d_{L/K}(\mathscr{K})}{[L : K]_i}$

5. $[T(\mathscr{K}) : (e)] = \dfrac{e_{L/K}(\mathscr{K}) d_{L/K}(\mathscr{K})}{[L : K]_i d_{L/K}(\mathscr{K})_s} = e_{L/K}(\mathscr{K}) \frac{d_{L/K}(\mathscr{K})_i}{[L:K]_i}$

It follows from (5) that if L is separable over K, $T(\mathscr{K}) \neq 1$ if and only if at least one of $e_{L/K}(\mathscr{K})$ or $d_{L/K}(\mathscr{K})_i$ is greater than one.

Lecture 20

34 Divisors in an Extension

Let L/l be an arbitrary extension of K/k. We wish to imbed the group of divisors of K in the group of divisors of L in such a way that the principal divisor $(X)_K$ in K of an element X of K goes into the principal divisor of the element X in L. This condition may also be rewritten in the form 116

$$\prod_{i=1}^{m} \mathscr{Y}_i^{v_{\mathscr{Y}_i}(X)} \longrightarrow \prod_{i=1}^{m} \prod_{j=1}^{h_i} \mathscr{K}_{ij}^{e_{L/K}(\mathscr{K}_{ij}) v_{\mathscr{Y}_i}(X)}$$

where $\mathscr{Y}_i (i = 1, \ldots, m)$ are the prime divisors of K occurring in X and $\mathscr{K}_{ij} (j = 1, \ldots, h_i)$ are all the prime divisors of L lying over $\mathscr{Y}_i$. This motivates the following

Definition. *If $\mathscr{U} = \prod\limits_{i=1}^{m} \mathscr{Y}_i^{v_{\mathscr{Y}_i}(\mathscr{U})}$ is any divisor of K, we shall identity it with the divisor $\prod\limits_{i=1}^{m} \prod\limits_{j=1}^{h_i} \mathscr{K}_{ij}^{e_{L/K}(\mathscr{K}_{ij}) v_{\mathscr{Y}\,i}(\mathscr{U})}$ in L.*

It is easy to see that this accomplishes an isomorphic imbedding of the group v_K of divisors of K in the group v_L of divisors of L which takes the principal divisor $(X)_K$ to the principal divisor $(X)_L$. Hence we also get a homomorphism of the class group $\mathscr{K}_K$ of K the class group $\mathscr{K}_L$ of L. From now on, we shall use the same for a divisor or class of K or its image as a divisor or class of L.

We have the following theorem comparing the degree in K of a divisor of K and its degree in L 117

Theorem. *There exists a positive rational number $\lambda_{L/K}$ depending only on L and K such that for any divisor $\mathscr{U}$ of K,*

$$d_L(\mathscr{U}) = d_K(\mathscr{U})/\lambda_{L/K}.$$

Proof. Obviously it suffices to prove that for any two prime divisors $\mathscr{Y}$ and $\mathscr{U}$ of K, we have

$$\frac{d_L(\mathscr{Y})}{d_K(\mathscr{Y})} = \frac{d_L(\mathscr{U}}{d_K(\mathscr{U})}$$

□

Assume on the contrary that we have

$$\frac{d_L(\mathscr{Y})}{d_K(\mathscr{Y})} < \frac{d_L(\mathscr{U}}{d_K(\mathscr{U})}$$

i.e.,

$$\frac{d_L(\mathscr{Y})}{d_L(\mathscr{U})} < \frac{d_K(\mathscr{Y})}{d_K(\mathscr{U})}$$

Then there is a positive rational m/n such that

$$\frac{d_L(\mathscr{Y})}{d_L(\mathscr{U})} < \frac{m}{n} < \frac{d_K(\mathscr{Y})}{d_K(\mathscr{U})}$$

It follows that for sufficiently large integral t, we have

$$d_K(\mathscr{Y}^{nt}\mathscr{U}^{-mt}) = t(nd_k(\mathscr{Y}) - md_K(\mathscr{U})) > 2g_K - 1$$

and

$$d_L(\mathscr{Y}^{nt}\mathscr{U}^{-mt}) = t(nd_L(\mathscr{Y}) - md_L(\mathscr{U})) < 0$$

118 It follows from the first inequality and the Riemann-Roch theorem that there exists an element $X \neq 0$ in K divisible by the divisor $\mathscr{U}^{mt}\mathscr{Y}^{-nt}$. Hence,

$$(X)_K = \mathscr{U}\mathscr{U}^{mt}\mathscr{Y}^{-nt}, \mathscr{U} \text{ integral}$$

and

$$d_L((X)) = d_L(\mathscr{U}) - t(nd_L(\mathscr{Y}) - md_L(\mathscr{U})) > 0$$

by the second inequality. But this is impossible and our theorem is proved.

If $[L : K] < \infty$, the value of $\lambda_{L/K}$ is $\dfrac{[l : k]}{L : K}$. For, if $\mathscr{Y}$ be any prime divisor of K and $\mathscr{K}_i(i = 1, \ldots, h)$ be the prime divisors of L lying over $\mathscr{Y}$, we have

$$d_L(\mathscr{Y}) = \sum_{i=1}^{h} d_L(\mathscr{K}_i) e_{L/K}(\mathscr{K}_i)$$

$$= \frac{1}{[l : k]} \sum_{i=1}^{h} d_{L/K}(\mathscr{K}_i) d_K(\mathscr{Y}) e_{L/K}(\mathscr{K}_i) = \frac{[L : K]}{[l : k]} d_L(\mathscr{Y}).$$

Now let L/l be an extension of K/k of finite degree and L_1 the smallest normal extension of K containing L. Let l_1 be the algebraic closure of l in L_1. Clearly L_1/l_1 is an algebraic function field with constant field l_1. Let $G = G(L_1/K)$ be the Galois group of L_1 over K and H be the 119 subgroup of all automorphisms of L_1 fixing every element of L. Let G/H be the set of left cosets of G modulo H. If Y is an element of L, it is well-known that the norm of Y over K is given by

$$N_{L/_K}(Y) = \left[\prod_{\bar{\sigma} \in G/H} \sigma Y \right]^{[L:K]_i},$$

the product being over any set of representatives of the cosets in G/H. This suggests the following definition for the norm of a divisor of L. (As already explained, we shall use the same symbol for a divisor of L and its canonical image as a divisor of L_1). If $\mathscr{U}$ is a divisor of L, we put

$$\text{Norm}_{L/_K} \mathscr{U} = Nm_{L/_K} \mathscr{U} = \left\{ \prod_{\sigma \in \bar{G}/H} \sigma \mathscr{U} \right\}^{[L:K]_i}$$

The definition is independent of the choice of the representative σ of $\bar{\sigma}$, since $\sigma\mathscr{U} = \mathscr{U}$ if $\sigma \in H$. (More generally, if L_{1/l_1} and $L_2/_{l_2}$ are two extension of an algebraic function field and σ an isomorphism of L_1 onto L_2 mapping l_1 onto l_2 and fixing every element of K, σ maps every divisor $\mathscr{U}$ of K considered as a divisor of L_1 onto $\mathscr{U}$ considered as a divisor of L_2).

We list below the essential properties of the norm

1. The norm of a divisor of L is a divisor of K. Hence the norm mapping is a homomorphism of ϑ_L into ϑ_K

2. If $\mathscr{K}$ is a prime divisor of L lying over the prime divisor $\mathscr{Y}$ of K, we have
$$Nm_{L/K}\mathscr{K} = \mathscr{Y}^{d_{L/K}(\mathscr{K})}$$

120

3. If $y \in L$,
$$Nm_{L/K}(y)_L = (Nm_{L/K}y)_K$$

4. If $\mathscr{U} \in \vartheta_K$,
$$Nm_{L/K}\mathscr{U} = \mathscr{U}^{[L:K]}$$

5. If $L_1 \supset L \supset K$ is a tower of extensions of algebraic function fields, and $\mathscr{U} \in v_{L_1}$,
$$Nm_{L_1/K}\mathscr{U} = Nm_{L/K}(Nm_{L_1/L}\mathscr{U})$$

Proof. (3) and (4) are immediate consequences of the definition of the norm. It is also clear that the norm defines a homomorphism of ϑ_L into itself. We have only to prove that the image is contained in ϑ_K to complete the demonstration of (1). But this will follow if we can prove (2). □

Again, it is enough to prove (5) for prime divisors $\mathscr{K}_1$ of L_1 because of (1). But using (2), (5) reduces to the already proved equality
$$d_{L_1/K}(\mathscr{K}_1) = d_{L_1/L}(\mathscr{K}_1)d_{L/K}(\mathscr{K})$$
for a prime divisor $\mathscr{K}_1$ of L_1 which lies over $\mathscr{K}$ of L.

It only remains to prove (2). Let again G be the Galois group of the smallest normal extension L_1 of K containing L.

121 Then L_1 is also normal over L and its Galois group over L is the subgroup H of G of all automorphisms which fix every element of L. Let $\mathscr{K}_1$ be any prime divisor of L_1 lying over the prime divisor $\mathscr{K}$ of L.

We shall denote by Z_K and Z_L the decomposition group of $\mathscr{K}_1$ over K and L respectively. The, since L_1 is normal over L, we have

$$\mathscr{K} = \left\{\prod_{\bar{\sigma}\in H/Z_L} \sigma\mathscr{K}_1\right\}^{e_{L_1/L}(\mathscr{K}_1)},$$

and therefore

$$\begin{aligned}
(N_{L/K}\mathscr{K})^{[Z_L:(e)]} &= \left[\prod_{\bar{\tau}\in G/H} \tau\left\{\prod_{\bar{\sigma}\in H/Z_L} \sigma\mathscr{K}_1\right\}^{[Z_L:(e)]}\right]^{e_{L_1/L}(\mathscr{K})[L:K]_i}\\
&= \left[\prod_{\tau\in G/H} \tau\left\{\prod_{\sigma\in H} \sigma\mathscr{K}_1\right\}\right]^{e_{L_1/L}(\mathscr{K}_1)[L:K]_i} = \left[\prod_{\tau\in G} \tau\mathscr{K}_1\right]^{e_{L_1/L}(\mathscr{K}_1)[L:K]_i}\\
&= \left\{\prod_{\bar{\tau}\in G/Z_K} \tau\mathscr{K}_1\right\}^{e_{L_1/L}(\mathscr{K}_1)[L:K]_i[Z_K:(e)]}\\
&= \mathscr{Y}^{\frac{e_{L_1/L}(\mathscr{K}_1)[L:K]_i[Z_K:(e)]}{e_{L_1/K}(\mathscr{K}_1)}} = \mathscr{Y}^{[Z_L:(e)]d_{L/K}(\mathscr{K})},
\end{aligned}$$

since

$$\begin{aligned}
\frac{e_{L_1/L}(\mathscr{K}_1)[L:K]_i[Z_K:(e)]}{e_{L_1/K}(\mathscr{K}_1)} &= \frac{e_{L/L}(\mathscr{K}_1)}{[L_1,:L]_i}.\frac{[L_1:K]_i[Z_K:(e)]}{e_{L_1/K}(\mathscr{K}_1)}\\
&= \frac{[Z_L:(e)]}{d_{L_1/L(\mathscr{K}_1)}}.d_{L_1/K}(\mathscr{K}_1) = [Z_L:(e)]d_{L/K}(\mathscr{K})
\end{aligned}$$

122 Since the group of divisors is free, it is also torsion free and our formula follows.

Finally, for any divisor $\mathscr{U}$ of L, we have

$$d_K(N_{L/_K}\mathscr{U}) = [l:k]d_L(\mathscr{U}).$$

It is enough to prove this for a prime divisor $\mathscr{K}$. But by the above result, we have

$$d_K(N_{L/_K}\mathscr{K}) = d_K(\mathscr{Y}^{d_{L/K}(\mathscr{K})}) = d_{L/K}(\mathscr{K})d_K(\mathscr{Y}) = d_L(\mathscr{K})[l:k]$$

which is the result we want.

35 Ramification

We wish to prove two theorems on ramification. The first one is easy.

Theorem. *If L/l is an algebraic extension of K/k such that L is purely inseparable over K, there is exactly one prime divisor $\mathscr{K}$ of L lying over a given prime divisor $\mathscr{Y}$ of K and $\mathscr{Y} = \mathscr{Y}^{pt}$ where p is the characteristic of K and t a non-negative integer.*

123 *Proof.* Let Y be any element of L. Since L is purely inseparable over K, there exists an integer n such that $Y_0 = Y^{p^n} \in K$. Then, if $\mathscr{K}$ be any prime divisor lying over $\mathscr{Y}$, we have

$$p^n v_{\mathscr{K}}(Y) = v_{\mathscr{K}}(Y_o) = e_{L/K}(\mathscr{K}) v_{\mathscr{Y}}(Y_o)$$

and therefore the value of $v_{\mathscr{K}}(Y)$ is uniquely determined by $v_{\mathscr{Y}}(Y_0)$. Hence $\mathscr{K}$ is unique. □

If we choose Y such that $v_{\mathscr{K}}(Y) = 1$, we deduce that $e_{L/K}(\mathscr{K})$ divides p^n, and our theorem is proved.

We say that a prime divisor $\mathscr{K}$ of an extension L of an algebraic function field K is *ramified* if $e_{L/K}(\mathscr{K}) > 1$. We have the following

Theorem. *If L is separably algebraic over K, there are at most a finite number of prime divisors of L which are either ramified or inseparable over K.*

Proof. We give the proof in three steps. We first prove the theorem for finite normal extension, then for finite separable extension, and finally in the general case. □

First assume that L is finite and normal over K. A prime divisor $\mathscr{K}$ of L is either ramified or inseparable only if $[T(\mathscr{K}) : (e)] = e_{L/K}(\mathscr{K}) d_{L/K}(\mathscr{K})_i > 1$.

This implies that there is an automorphism σ of L in the group $T(\mathscr{K})$ which is not the identity automorphism. Since L is finite and separable over K it is a simple extension $K(Z)$ of K. Hence $\sigma Z \neq Z$.

124 Al least one of the elements $Z, \dfrac{1}{Z}$ lies in $\mathscr{O}_{\mathscr{K}}$, and since $\sigma \in T(\mathscr{K})$

we deduce that one of the two inequalities

$$v_{\mathscr{K}}(Z - \sigma Z) > 0 \text{ or } v_{\mathscr{K}}\left(\frac{1}{Z} - \frac{1}{\sigma Z}\right) > 0$$

should hold. Since there are only finitely many automorphisms σ of L over K and only finitely many prime divisors $\mathscr{K}$ for which one of the two inequalities above can be valid, the theorem is proved in this case.

If L/K were finite and separable but not normal, let L_1 be the smallest normal extension of K containing L. If a prime divisor $\mathscr{K}$ of L is ramified or inseparable over K, the same property should also hold for any prime divisor of L_1 lying over $\mathscr{K}$. Hence the theorem in this case follows from the first part.

Finally, suppose L/K is any separably algebraic extension It l is the constant field of L, L is evidently a finite separable extension of the composite extension Kl. Also, a prime divisor of L in ramified (inseparable) over K if and only if it is either ramified (inseparable) over Kl or the prime divisor of Kl over which it lies is ramified (inseparable) over K. Our theorem follows from what we have proved above and the following lemma.

Lemma. *If L/l is an algebraic function field which is separably algebraic over K/k and the that $L = Kl$, there are no prime divisors of L ramified or separable over K.*

Proof. If $\mathscr{K}$ is a prime divisor of L which is ramified (inseparable) over K, find an element $Y \in Kl$ such that $V_{\mathscr{K}}(Y) = 1(\bar{Y} \in L_{\mathscr{K}}$ is inseparable **125**
over $K_{\mathscr{Y}}$). Since Y is a rational combination of a finite number of elements of K and l, Y lies in a finite extension $K(\alpha_1, \ldots \alpha_n)$ of K, where α_i are elements of l. We may also assume that $L_1 = K(\alpha_1, \ldots \alpha_n)$ is a normal separable extension of K; for it is already separable, and we have only to adjoin to it the conjugates of the α_i (which are finite in number) to make it normal. Also by our choice of Y, we see that the prime divisor $\mathscr{K}_1$ of L_1 over which $\mathscr{K}$ lies is ramified (inseparable) over K. □

Let $T(\mathscr{K}_1)$ be the inertia group of $\mathscr{K}_1$ in L_1 over K. Then, we should have

$$[T(\mathscr{K}_1) : (e)] = e_{L_1/K}(\mathscr{K}_1) d_{L_1/K}(\mathscr{K}_1)_i > 1,$$

and there exists an element $\sigma \in T(\mathscr{K}_1)$ which is not the identity. But since $\sigma \in T(\mathscr{K}_1)$,

$$v_{\mathscr{K}_1}(\alpha_\nu - \sigma\alpha_\nu) > 0 \quad (\nu = 1, 2, \ldots n)$$

and the α_ν being constants, we should have

$$\alpha_\nu = \sigma\alpha_\nu$$

Hence σ is the identity automorphism when restricted to K and fixes each one of elements $\alpha_1, \ldots, \alpha_n$. Hence σ should be the identity automorphism of $L_1 = K(\alpha_1, \ldots \alpha_n)$. This is a contradiction and our theorem is proved.

Lecture 21

36 Constant Field Extensions

126 An extension L/l of an algebraic function field K/k is said to be a *constant field extension* If L is the composite extension Kl of K and l.

The following question arises. Given an algebraic function field K/k and an extension l of k, is it possible to find a constant field extension L'/l' of K/k such that l is k-isomorphic to l' ? This is not possible in general, since the constant field of $L' = Kl'$ will in general be larger than the isomorphic image l' of $l\cdot$. More precisely, we have the following

Theorem. *Let K/k be an algebraic function field and l'_0 an extension of k. Then there exists an algebraic function field L/l which is an extension of K/k with the following properties:*

(1) *there exists a subfield l_0 of l containing k and a k-isomorphism $\lambda : l_0 \to l'_0$*

(2) $L = Kl_0$.

If L^*/l^* is another extension of K/k with a subfield l^*_0 of l^* and a k-isomorphism $\lambda^* : l^*_0 \to l'_0$ having the properties (1) and (2), there exists a K-isomorphism $\rho : L^* \to L$ such that the restriction of ρ to l^*_0 coincides with the map $\lambda_0^{-1}\lambda^*$ of l^*_0 onto l_0.

l is a purely inseparable finite extension of l_0. 127

Proof. Construction of a composite field $L = Kl_0$. □

Let $\{u'_i\}$ be a transcendence basis of l'_0 over k. Take a $\{u_i\}$ of independent transcendental elements u_i over K in one-one correspondence $u_i \leftrightarrow u'_i$ with the set $\{u'_i\}$ and let Ω be the algebraic closure of $K(\{u_i\})$. Then we have an isomorphism λ of $k(u'_i)$ onto $k(u_i)$ trivial on k, defined by $\lambda u'_i = u_i.\lambda$ can be extended to an isomorphism λ of l'_0 onto subfield l'_0 of Ω, and Ω contains the composite field $Kl_0 = L$. Let l be the algebraic closure of l_0 in L.

If X is a transcendental element of K over k, X is also transcendental over l_0. For if it were not, there exists a finite subset $(u_1, \ldots u_n)$ of the u_i such that X is algebraic over $k(u_1, \ldots u_n)$. Hence there exists a relation of the form

$$f_o(u_1, \ldots u_n)X^r + \cdots\cdots + f_r(u_1, \ldots u_n) = 0,\ f_i \in k[u_1, \ldots u_n],$$

with at least one non-constant polynomial f_i. But this would imply that the set $(u_1, \ldots u_n)$ is algebraically related over K, a contradiction.

Also, since $L = Kl_0$, and $l_0 \supset k$,

$$[L : l_0(X)] \leq [K : k(X)] < \infty,$$

and therefore L/l is an algebraic function field with constant field $l \supset l_0$. 128 The conditions (1) and (2) are evidently fulfilled. Moreover, since, X is transcendental over l, we have

$$[l : l_0] = [l(X) : l_0(X)] \leq [L : l_0(X)] < \infty$$

Only the second part of the theorem asserting uniqueness upto isomorphism and the last part asserting that l is purely in-separable over l_0 remain to be proved.

Suppose L^*/l^* is another extension of K/k satisfying the conditions of the theorem. We have to set up an isomorphism $\rho : L^* \to L$ such that ρ fixes the elements of K and ρ restricted to l^*_0 is the isomorphism $\lambda_1 = \lambda_0^{-1}\lambda^*$ of l^*_0 onto l_0. Since any element of $L^* = Kl^*_0$ can be written in the form

$$\frac{\sum k_i l^*_i}{\sum k'_j l'^*_j} k_i, k'_j \in K, l^*_i, l'^*_j \in l^*_0,$$

we should necessarily have

$$\rho\left(\frac{\sum k_i l_i^*}{\sum k'_j l'^*_j}\right) = \frac{\sum k_i \lambda_1(l_i^*)}{\sum k'_j \lambda_1(l'^*_j)}$$

We make this the definition of ρ. In order to prove that it is well defined, we have to verify that if 0 has the representation $\sum k_i l_i^*$, then $\sum k_i \lambda_1(l_i^*) = 0$. To prove that the map is an isomorphism (and also to prove that the denominator of the right side does not vanish when $\sum k'_j l'^*_j \neq 0$) we have to prove that $\sum k_i \lambda(l_i^*) = 0 \Rightarrow \sum k_i l_i^* = 0$.

Thus, we have set up the required isomorphism provided we can **129**
prove that

$$\sum k_i l_i^* = 0 \Leftrightarrow \sum k_i \lambda_1(l_i^*) = 0.$$

But since these expressions involve only a finite number of elements of l_0 and l_0^*, we may assume that l_0 (and consequently l_0^*) is finitely generated over k.

A simple argument shows that to prove the pure inseparability of l over l_0 we may also assume that l_0 is finitely generated over k.

First assume that l_0 is a purely transcendental extension $k(u_1, \ldots u_n)$ of k. Then $l_0^* = k(u_1^*, \ldots u_n^*)$, where $u_i^* = \lambda_1^{-1}(u_i)$. Then $u_1, \ldots u_n$ are algebraically independent over K, and so are $u_1^*, \ldots, u_n^*$. Hence there exists an isomorphism $\rho : L^* = K(u_1^*, \ldots, u_n^*) \to K(u_1, \ldots u_n) = L$. In this case, the constant field l coincides with $l_0 = k(u_1, \ldots, u_n)$. This follows from the following more general

Lemma . *If A is a field which is algebraically closed in another field B, and if $X_1, \ldots, X_n$ is a set of algebraically independent elements over $B, A(X_1, \ldots X_n)$ is algebraically closed in $B(X_1, \ldots, X_n)$.*

Proof. We may clearly assume that $n = 1, X_1 = X$. □

Let $\alpha = \alpha_0 \dfrac{f(X)}{g(X)}$ be any element of $B(X)$, where $\alpha_0 \neq 0$ is an element of B and $f(X)$ and $g(X)$ are coprime polynomials over B with leading **130**
coefficients 1. If α is algebraic over $A(X)$, we have

$$\varphi_r(X)\alpha^r + \cdots\cdots\cdots + \varphi_o(X) = 0, \varphi_i(X) \in A[X],$$

$$\varphi_o, \ldots, \varphi_r \quad \text{coprime}$$

i.e., $$\varphi_r(X)\alpha_o^r f^r(X) + \cdots\cdots + \varphi_o(X)g^r(X) = 0.$$

Let ξ be any root of $f(X)$. Substituting $X = \xi$ in the above equation (which we may do since X is transcendental over B) we obtain

$$\varphi_o(\xi)g^r(\xi) = 0$$

and since $g(\xi) \neq 0$, f and g being coprime,

$$\varphi_0(\xi) = 0$$

and so ξ is algebraic over A. Since every root of f is algebraic over A and $f(X)$ has leading coefficient 1, the coefficients of f are algebraic over A and hence lie in A. Similarly, g is also a polynomial over A. Substituting for X a root δ of $f(X) - g(X)$, we get, since $f(\delta) = g(\delta) \neq 0, \varphi_r(\delta)\alpha_0^r + \cdots + \varphi_0(\delta) = 0$, hence α_0 is algebraic over A and therefore in A, since not all $\varphi_i(\delta) = 0(\varphi_0, \ldots \varphi_r$ being coprime). Our lemma is proved.

We are therefore left with the case when l_0 is a finite algebraic extension of k. 131 Then we have $l_0 = k(\alpha_1, \ldots, \alpha_m)$. We use induction on m. The result is trivial when $m = 0$.

Suppose the result holds for $m - 1$ in the place of m. Put $k_1 = k(\alpha_1, \ldots, \alpha_{m-1})$ and $K_1 = Kk_1 = K(\alpha_1, \ldots, \alpha_{m-1})$. Let $\alpha_i^* = \lambda_1^{-1}(\alpha_i)$, $k_1^* = k^*(\alpha_1^* \cdots \alpha_{m-1}^*)$ and $K_1^* = Kk_1^* = K(\alpha_1^*, \ldots \alpha_{m-1}^*)$. Let l_1 and l_1^* be the algebraic closures of k_1 and k_1^* in K_1 and K_1^* respectively. By our induction hypothesis, we have

(1) an isomorphism $\rho_1 : K_1^* \to K_1$ such that ρ_1 when restricted to k_1^* coincides with the restriction of λ_1 to k_1^*, and

(2) l_1 and l_1^* are purely inseparable extensions of k_1 and k_1^* respectively.

Put $\alpha_m = \alpha$ and $\alpha_m^* = \lambda_1^{-1}(\alpha_m) = \alpha^*$. Then, $L = K_1(\alpha)$ and $L^* = K_1^*(\alpha^*)$. We would be through if we can extend the isomorphism ρ_1 to an isomorphism $\rho : L^* \to L$ such that $\rho(\alpha^*) = \lambda_1(\alpha^*)$ and if we prove that the constant field l of L is purely inseparable over l_0.

To prove that we can extend the isomorphism ρ_1 to ρ, it is necessary and sufficient to show that if $F^*(X)$ is the irreducible polynomial of α^* over $K_1^*, \rho_1 F^*(X)$ is the irreducible polynomial of α over K_1.

Assume that $F^*(X)$ has leading coefficient 1. Since one of its roots is algebraic over k_1^*, all its roots are algebraic over k_1^* and $F^*(X)$ is therefore a polynomial with coefficients in the algebraic closure, l_1^* of k_1^* in K_1^*. Also, since l_1^* is purely inseparable over k_1^*, the irreducible polynomial of 132 α^* over k_1^* is a certain power of $F^*(X)$ of the form $(F^*(X))^{p^t}$, $t \geq 0$. Since λ_1 is an isomorphism of $l_o^* = k_1^*(\alpha^*)$ onto $l_o = k_1(\alpha)$ with $\lambda_1(\alpha^*) = \alpha$, we deduce that $\lambda_1(F^*(X))^{p^t} = \rho_1(F^*(X))^{p^t}$ is the irreducible polynomial of α over k_1.

Again, since ρ_1 maps k_1^* onto k_1, it maps the algebraic closure l_1^* of k_1^* in K_1^* onto the algebraic closure l_1 of k_1 in K_1. This proves that the irreducible equation of α over K_1 (or what is the same, l_1) with leading coefficient 1 is equal to $\rho_1 F^*(X)$ since $\rho_1 F^*(X)$ is obviously the only irreducible factor of $\rho_1(F^*(X))^{p^t}$ over l_1.

Hence ρ_1 can be extended to an isomorphism ρ having the requisite properties.

To prove that l is purely inseparable over l_0, notice that since l_1 is purely inseparable over $k_1, l_1(\alpha)$ is purely in-separable over $k_1(\alpha) = l_0$. It is therefore sufficient to prove that l is purely inseparable over $l_1(\alpha)$.

Now since l_1 is algebraically closed in K_1, the irreducible polynomial of α over K_1 with leading coefficient l coincides with its irreducible polynomial over l_1. Therefore we have

$$[K_1(\alpha) : K_1] = [l_1(\alpha) : l_1]$$

and similarly $$[l_1(\alpha, X) : l_1(X)] = [l_1(\alpha) : l_1].$$

From these two equalities and the following one 133

$$\begin{aligned}[K_1(\alpha) : l_1(X)] &= [K_1(\alpha) : K_1][K_1 : l_1(X)] \\ &= [K_1(\alpha) : l_1(\alpha, X)][l_1(\alpha, X) : l_1(X)].\end{aligned}$$

we deduce that

$$[K_1 : l_1(X)] = [K_1(\alpha) : l_1(\alpha, X)].$$

Now, let β be a constant of $K_1(\alpha)$. Then there exists an integer $t \geq 1$ such that β^{p^t} is separably algebraic over $l_1(\alpha)$. By a well-known theorem, the extension $l_1(\alpha, \beta^{p^t})$ is a simple extension $l_1(\gamma)$ of l_1. We have

$$[K_1(\alpha) : l_1(\alpha, \beta^{p^t}, X)] = [K_1(\gamma) : l_1(\gamma, X)] = [K_1 : l_1(X)]$$

by an argument which is familiar to us, and using our previous equality, we get

$$[K_1(\alpha) : l_1(\alpha, \beta^{p^t}, X)] = [K_1(\alpha) : l_1(\alpha, X)]$$

and hence $l_1(\alpha, \beta^{p^t}, X) = l_1(\alpha, X)$ and $\beta^{p^t} \in l_1(\alpha, X)$. Since β^{p^t} is algebraic over $l_1(\alpha)$ which is algebraically closed in $l_1(\alpha, X), \beta^{p^t} \in l_1(\alpha)$ and β is purely inseparable over $l_1(\alpha)$.

Our theorem is completely proved. We shall give an example where $l \neq l_0$. Let k_0 be a field of characteristic $p > 0$ and u and v two algebraically independent elements over k_0. Let $k = k_0(u, v)$ and X a variable 134 over k. Put $K = k(X, Y)$ where Y satisfies the equation $Y^p = uX^p + v$. We shall show that the constant field is k. If it were not, let k^1 be the constant field. Since $K = k(X, Y)$ is of degree l or p over $k(X)$ and since $[k^1(X) : k(X)] = [k^1 : k] > 1$, we deduce that $K = k^1(X)$. Hence $Y = u^{1/p}X + v^{1/p} \in k^1(X)$. But since X is transcendental over k, (and hence also over $k(u^{1/p}, v^{1/p})$, we deduce that $u^{1/p}$ and $v^{1/p}$ are both in k^1. Hence

$$[k^1 : k] \geq [k(u^{1/p}, v^{1/p}) : k] = [k(u^{1/p}, v^{1/p}) : k(u^{1/p})][k(u^{1/p}) : k] = p^2,$$

while on the other hand

$$[k^1 : k] = [k^1(X) : k(X)] \leq [K : k(X)] \leq$$

which is a contradiction.

Now, take $l_0 = k(v^{1/p})$. Then Kl_0 clearly contains the element $\dfrac{Y - v^{1/p}}{X} = u^{1/p}$ and hence $l = k(u^{1/p}, v^{1/p}), l \neq l_o$ and $[l : l_o] = p$.

Lecture 22

37 Constant Field Extensions

We require some preliminary lemmas. 135

Lemma 1. *Let A, B and C be subfields of a given field, $B \supset A$ and C algebraic of finite degree n over A. Then the composite extension BC is algebraic over B of degree at most n. Moreover if $y_1, \ldots y_n$ is a basis of C over A, BC is spanned by the same set of elements $y_1, \ldots y_n$ over B. The degree of BC over B is equal to n if and only if B and C are linearly disjoint over A.*

Proof. Since $y_1, \ldots y_n$ span C over A, we have in particular $C = A(y_1, \ldots, y_n)$ and since $B \supset A$, $BC = B(y_1, \ldots y_n)$. Hence any element of BC can be written as a polynomial in $y_1, \ldots y_n$ with coefficients in B (since $y_1, \ldots y_n$ are algebraic over A), and since any monomial in $y_1, \ldots, y_n$ can be written as a linear combination of $y_1, \ldots, y_n$ with coefficients in A, we deduce that BC is the vector space spanned by $y_1, \ldots ..y_n$ over B. Hence $[BC : B] \leq n$. □

If $[BC : B] = n, y_1, \ldots y_n$ should also be linearly independent over B, and since $(y_1, \ldots y_n)$ is an arbitrary set of n elements of C linearly independent over A, B and C are linearly disjoint over A. The converse is also evident.

Lemma 2. *(a) Let B be any purely transcendental extension of A and C any field containing A and algebraically disjoint with B over A. Then C and B are linearly disjoint over A.* 136

(b) *Let A be algebraically closed in B and $C = A(\alpha)$ a simple algebraic extension of A. Then B and C are linearly disjoint over A.*

Proof. (a) Let $B = A(u_\lambda)_{\lambda \in A}$ where u_λ is a set of algebraically independent elements over A. If B and C are not linearly disjoint, there is a set of elements $c_1, \ldots c_n \in C$ which are linearly independent over A and polynomials $f_i(u_1, \ldots u_m), u_i, \in \{u_i\}_{\lambda \in A}$ not all of which vanish identically such that

$$c_1 f_1(u_1, \cdots u_m) + \cdots + c_n f_n(u_1, \ldots u_m) = 0, \; f_i \in A[u_1, \ldots, u_m]$$

Since $u_1, \ldots u_m$ are algebraically independent over A, they are algebraically independent over C also. We may therefore equate to zero separately the coefficients of each of the monomial expressions in $u_1, \ldots u_m$ occurring in the left hand side of the above equation. At least one of these provides a non-trivial linear combination of the c_i with coefficients in A which vanishes. This is a contradiction.

(b) Since A is algebraically closed in B, the irreducible monic polynomial of α over B is actually a polynomial over A, as we have proved earlier. Hence $[B(\alpha) : B] = [A(\alpha) : A]$, and our result follows from Lemma 1.

□

Lemma 3. *Let A, B, C, D be subfields of a given field such that $B \supset$ 137 $A, D \supset C \supset A$. Then B and D are linearly disjoint over A if and only if $(i)B$ and C are linearly disjoint and (ii) D and the composite extension BC are linearly disjoint over C.*

Proof. Suppose first that B and D are linearly disjoint. Then (i) is evidently fulfilled. To prove (ii), suppose $d_i(i = 1, \ldots n)$ is a set of elements of D linearly independent over C. If they are linearly dependent over BC, there exists a relation of the form

$$\sum_i d_i \sum_j c_{ij} b_j = 0 \, , c_{ij} \in C, b_j \in B,$$

with b_j linearly independent over C and not all c_{ij} being zero. On interchanging the orders of summation, we get

$$\sum_j b_j \sum_j d_i c_{ij} = 0,$$

and we deduce from our hypothesis that

$$\sum_i c_{ij} d_i = 0 \quad \text{for all} \quad j.$$

□

But since d_i are linearly independent over C, we have $c_{ij} = 0$ for all i and j. This is a contradiction.

Suppose conversely that (i) and (ii) are fulfilled. Then any set of elements of B linearly independent over A are, by (i), linearly independent over C, and (since they are also elements of BC) by (ii), linearly independent over D. Our lemma is proved.

We can now prove the following

Theorem. *Let $L = Kl_0$ be a constant field extension of K with the field of constants $l \supset l_0$. Then the following conditions are equivalent* 138

(A) K and l are linearly disjoint over k.

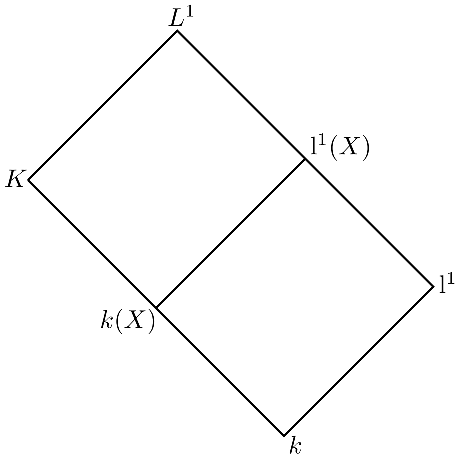
(B) For every finitely generated subfield l'_0 of l_0 over k, and $L^1 = Kl^1_0$, the constant field of L^1 coincides with 1^1_0.

If these are fulfilled, (B) holds for any (not necessarily finitely generated) subfield l^1_0 of l_0, in particular for l_0 itself, i,e., $l = l_0$.

Proof. We shall first show that (A) implies (B) for any subfield l^1_0 of l_0. Let l^1 be the constant field of $L^1 = Kl^1_0$. It follows from (A) that l^1 and K are linearly disjoint over k.

Let X be any transcendental element of K over k. Then by Lemma 3, K and 1^1 are linearly disjoint over k if and only if (i) $k(X)$ and l^1 are linearly disjoint over k and (ii) K and $l^1 k(X) = l^1(X)$ are linearly disjoint over $k(X)$.

By lemma 2, since $k(X)$ are 1^1 are algebraically disjoint (i) is always satisfied. By lemma 1, since $1_0^1(X) \subset 1^1(X)$ and $L^1 = K1_0^1(X)$, we have the inequalities



$$[L^1 : l^1(X)] \leq [L^1 : l_o^1(X)] \leq [K : k(X)].$$

□

Again by lemma 1, since $L^1 = Kl^1(X)$, the equality

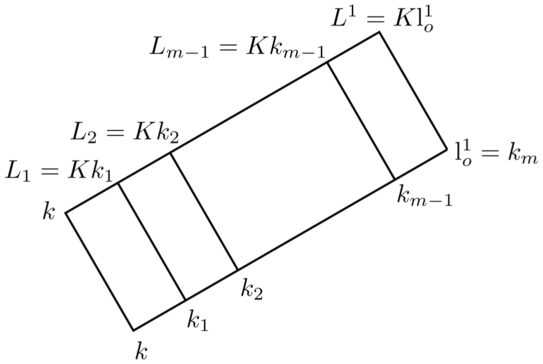
$$[L^1 : l^1(X)] = [K : k(X)]$$

follows from the linear disjointness of K and $l^1(X)$ over $k(X)$.

139 From these we deduce that if (A) holds, $l^1(X) = l_0^1(X)$, and since X is transcendental over $l^1, l^1 = l_0^1$.

Conversely suppose (B) holds for every finitely generated subfield l_0^1 of l_0. To prove that 1 and K are linearly disjoint, it is enough to prove that any finitely generated subfield of 1 over k is linearly disjoint with K over k. But clearly a finitely generated subfield of l is contained in the constant field $l^1 = l_0^1$ of $L^1 = Kl_0^1$, where l_0^1 is a suitable finitely generated extension of k. It is therefore enough to prove that any finitely generated subfield l_0^1 of l_0 over k is linearly disjoint with K over k.

Let $l_0^1 = k(\alpha_1, \ldots \alpha_m)$. Put $k_i = k(\alpha_1, \ldots \alpha_i)$, and $l_i = Kk_i$. To show that l_0^1 and K are linearly disjoint over k, it is enough to show that k_1 and K are linearly disjoint over k, k_2 and $L_1 = KK_1$ are linearly disjoint over k_1, etc., and finally $l_0^1 = k_m$ and $L_{m-1} = KKk_{m-1}$ are linearly disjoint over k_{m-1} (Lemma 3). But by (B) each k_i is algebraically closed in L_i and since k_{i+1} is a simple extension of k_i, our result follows from Lemma 2.



Corollary. *If either K or l_0 is separably generated over k, then $l = l_0$.*

Proof. By the above theorem, we may assume that l_0 is finitely generated over k. Morover, since we have already seen that $l = l_0$ for a purely transcendental extension l_0 of k (see Lecture 21), we may assume that l_0 is finitely algebraic over k. □ 140

Suppose now that l_0 is separably algebraic over k. Then $L = Kl_0$ is separably algebraic over K. But if $\alpha \in l$, the irreducible monic polynomial of α over K lies in k and is therefore separable over k. Hence l is separable over l_0, and is also purely inseparable $l = l_0$.

Suppose next that K is separably generated over k. Let $X \in K$ be transcendental over k and such that $K/k(X)$ is separable. Then $L = Kl_0(X)$ is separable over $l_0(X)$. Hence any element of l is separably algebraic over $l_0(X)$, and since l_0 is algebraically closed in $l_0(X), l$ is separable over l_0. The result follows as before.

Our next theorem runs as follows.

Theorem. *Let $L = l_0K$ be a constant field extension and $\lambda_{L/K}$ the rational number satisfying*

$$\lambda_{L/K} d_L(\mathscr{U}) = d_K(\mathscr{U})$$

for any divisor $\mathscr{U}$ of K. Then $\lambda_{L/K}$ is a power of the characteristic with non-negative exponent ($\lambda_{L/K} = 1$ if the characteristic is zero). It is equal to one if and only if K and l are linearly disjoint over k.

Proof. Let X be a transcendental element of K. Choose $\mathscr{U}$ to be the numerator of (X). Then, we see that

$$d_K(\mathscr{U}) = [K : k(X)] \text{ and } d_L(\mathscr{U}) = [L : l(X)]$$

141 Hence,

$$\lambda_{L/K} = 1 \Leftrightarrow d_L(\mathscr{U}) = d_K(\mathscr{U}) \Leftrightarrow [L : l(X)] = [K : k(X)].$$

But as we have already seen (see proof of the first theorem of this lecture) $[L : l(X)] = [K : k(X)]$ if and only if K and l are linearly disjoint over k. □

In particular, if the characteristic is zero, K is separably generated over k, and by the corollary of the first theorem, the condition (B) of our first theorem is satisfied. Hence (A) holds, i.e., K and l are linearly disjoint over k. Hence $\lambda_{L/K} = 1$.

If the characteristic $p > 0$, let K_0 be the largest separable extension of $k(X)$ contained in K, and $L_0 = K_0 l_0$. Then as above, K_0 and l_0 are linearly disjoint over k. Hence we obtain

$$[K_0 : k(X)] = [L_0 : l_0(X)]$$

Also, K/K_0 is a purely inseparable extension of degree p^s, $s \geq 0$ and therefore so is $L = Kl_0$ inseparable of degree p^s, where $s_0 \leq s$ (lemma 1). Therefore we have

$$\lambda_{L/K} = \frac{[K : k(X)]}{[L : l(X)]} = \frac{[K : k(X)][l(X) : l_0(X)]}{[L : l_0(X)]}$$

$$= \frac{[K : K_0][K_0 : k(X)]}{[L : L_0][L_0 : l_0(X)]}[l : l_0] = p^{s-s_0}[l : l_o]$$

142 Thus, we see that $\lambda_{L/K}$ is a power of p divisible by $[l : l_0]$. Our theorem is proved.

In particular, we see that if K or l_0 is separably generated over k, K and l are linearly disjoint over k and therefore $\lambda_{L/K} = 1$.

The last theorem of this section relates to the residue class field of a prime divisor in a constant filed extension.

Theorem. *Let $L = Kl$, where I is separably generated over k. If $\mathscr{K}$ is a prime divisor of L lying over the prime divisor $\mathscr{Y}$ of K, $L_{\mathscr{R}}$ is the composite of the two subfields $K_{\mathscr{Y}}$ and l.*

Proof. It is clearly sufficient to prove the theorem when (1) l is purely transcendental over k and (2) when l is separably algebraic over k. □

Case 1. *Since $K_{\mathscr{Y}}$ is algebraic over K, l and $K_{\mathscr{Y}}$ are linearly disjoint over k. Let us agree to denote the image in $L_{\mathscr{K}}$ of any element Y in the valuation ring $\mathscr{O}_{\mathscr{K}}$ by $\bar{Y}$. Any $Y \in \mathscr{O}_{\mathscr{K}}$ can be written in the form*

$$\frac{\sum\limits_{i=1}^{n} k_i l_i}{\sum\limits_{j=1}^{m} k_j^1 l_j^1}, \quad k_i, k_j^1 \in K, l_i, l_j^1 \in 1,$$

and the two sets of elements (l_i) and (l_j^1) being linearly independent over k. Find elements a, b of K such that $v_{\mathscr{Y}}(a) = \min\limits_{i=1}^{n} v_{\mathscr{Y}}(k_i)$ and $v_{\mathscr{Y}}(b) = -\min\limits_{j=1}^{m} v_{\mathscr{Y}}(k_j^1)$. Then clearly for at least one $j\, v_{\mathscr{Y}}(k_j^1 b) = 0, k_j^1 \neq 0$. The image $L_{\mathfrak{R}}$ of the element $\dfrac{aY}{b}$ is then **143**

$$\frac{\sum \overline{(k_i a)} l_i}{\sum \overline{(k_j^1 b)} l_j^1}$$

Since the l_i are linearly independent over k, they are also linearly independent $K_{\mathscr{Y}}$ and therefore the numerator does not vanish. Similarly the *denominator does not vanish, and therefore the image of* $\frac{aY}{b}$ *in* $L_{\mathscr{X}}$ *is a non-zero element of* $K_{\mathscr{Y}}l$*. Since* $Y \in \mathscr{O}_{\mathscr{X}}$*, it follows that* $\frac{b}{a} \in \mathscr{O}_{\mathscr{Y}}$ *and hence* $\overline{Y} = \left(\frac{\overline{b}}{\overline{a}}\right)\left(\frac{\overline{aY}}{\overline{b}}\right) \in K_{\mathscr{Y}}l$*.*

Since $K_{\mathscr{Y}}$ and l are linearly disjoint, the structure of $L_{\mathscr{X}}$ is uniquely determined; in fact $L_{\mathscr{X}}$ is purely transcendental over K, and a transcendence basis of l over k is also a transcendence basis of $L_{\mathscr{X}}$ over $K_{\mathscr{Y}}$. Since the map $Y \to \overline{Y}$ is also uniquely fixed, we see that there is exactly one prime divisor $\mathscr{X}$ of L lying over the prime divisor $\mathscr{Y}$ of K.

Case 2. *In this case we may not only assume that l is separably algebraic over k, but also that it is finite. In fact, any element* α *of* $L_{\mathscr{X}}$ *is clearly the image by the place of* $\mathscr{X}$ *of an element of* Kl^1*, where* l^1 *is a finite extension of k. If we have proved the theorem for finite separable extensions, it would follow that* $\alpha \in l^1K_{\mathscr{Y}} \subset lK_{\mathscr{Y}}$ *and we would be through.*

Suppose l is separably algebraic and of finite degree over k. Then it is simple and we have $l = k(\alpha)$, where α is separably algebraic over k of degree n, say. Let $\mathscr{X} = \mathscr{X}_1, \mathscr{X}_2, \ldots, \mathscr{X}_n$ be all the prime divisors of L lying over $\mathscr{Y}$. Let L^1 be the smallest normal extension of K containing L, and $\mathscr{X}^1$ a prime divisor of L^1 lying over $\mathscr{X}$. Let $\sigma_i (i = 1, \ldots, m)$ be all the automorphisms of L^1 over K. Then since $\sigma_i\mathscr{X}^1$ again lies over the prime divisor of K, its restriction to L is one of the $\mathscr{X}_j$. 144

Let $\overline{Z} \in L_{\mathscr{X}}$. Find an element $C \in L$ such that

$$v_{\mathscr{X}}(C - Z) > 0,$$

and
$$v_{\mathscr{X}\,j}(C) \geq 0, (j = 2, \ldots h)$$

By the first condition , $\overline{C} = \overline{Z} \in L_{\mathscr{X}}$.

Since $C \in K(\alpha)$, it can be written uniquely in the form

$$C = a_o + a_1\alpha + \cdots\cdots + a_{n-1}\alpha^{n-1}, a_i \in K$$

(the degree of α over K being the same as over k, according to a previous statement).

Taking conjugates in the above equation over K, we obtain a set of n equations

$$C^{(i)} = a_0 + a_1\alpha^{(i)} + \cdots\cdots + a_{n-1}\alpha^{(i)^{n-1}}$$

Since α is separable of degree n over K, the determinant $|\alpha^{(i)j}|(i = 1, \ldots, n; j = o, \ldots, n-1)$ has a non-zero value, and we may solve the above equations for a_k to obtain

$$a_k = \frac{\begin{vmatrix} 1\alpha^{(1)} & \cdots & \alpha^{(1)^{k-2}}C_1 & \cdots & \alpha^{(1)^{n-1}} \\ 1\alpha^{(n)} & \cdots & \alpha^{(n)^{k-2}}C^n & \cdots & \alpha^{(n)^{n-1}} \end{vmatrix}}{\begin{vmatrix} 1\alpha^{(1)} & \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \alpha^{(1)^{n-1}} \\ 1\alpha^{(n)} & \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \alpha^{(n)^{n-1}} \end{vmatrix}}$$

145

The denominator is a constant of the filed L^1. The numerator is a linear combination of the $C^{(i)}$ with constant coefficients. But we have

$$v_{\mathscr{K}^1}(C^{(i)}) = v_{\sigma_\nu^{-1}\mathscr{K}'}(C) = e_{L^1/L}(\sigma_\nu^{-1}\mathscr{K}^1)v_{\mathscr{K}j}(C) \geq 0$$

where σ_ν is an automorphism of L^1/K taking C to $C^{(i)}$ and $\mathscr{K}_j$ is the prime divisor of L lying below $\sigma_n u^{-1}\mathscr{K}^1$.

We may therefore conclude that

$$v_{\mathscr{K}^1}(a_k) \geq 0, v_{\mathscr{K}}(a_k) \geq 0$$

This means that the a_k are in $\mathscr{O}_{\mathscr{K}}$ and therefore

$$\bar{Z} = \bar{C} = \bar{a_o} + \bar{a_1}\alpha + \cdots\cdots + \overline{a_{n-1}}\alpha^{n-1} \in lK_{\mathscr{Y}}.$$

Our theorem is proved.

From the proof of the theorem when l_0 is purely transcendental, the following fact emerges. If $\mathscr{K}$ is a prime divisor of $L = Kl_0, l_0$ being purely transcendental, and $\mathscr{K}$ lies over a prime divisor $\mathscr{Y}$ of K, we have

$$v_{\mathscr{K}}\left(\sum_1^n l_i a_i\right) = \min_{i=1}^{n}(v_{\mathscr{Y}}(a_i))$$

if $l_i \in l_0$ and $a_i \in K$. This follows in fact from the equation 146

$$\overline{\sum_{i=1}^n l_i a_i} = \sum_{i=1}^n l_i \bar{a}_i, \text{ if } a_i \in \mathscr{O}_{\mathscr{Y}}.$$

Lecture 23

38 Genus of a Constant Field Extension

The notations will be the same as in the previous lecture; in addition, 147 we shall denote by g_R the genus of a function field R and by $F_R(\mathscr{U})$ the vector space over the constant field of R of elements divisible by the divisor $\mathscr{U}$. The dimension of $F_R(\mathscr{U})$ will be denoted by $N_R(\mathscr{U}).\Lambda_R(\mathscr{U})$ shall denote the vector space of repartitions of R divisible by the divisor $\mathscr{U}$.

Theorem 1. *If $\lambda_{L/K} = 1$, i.e., if K and l are linearly disjoint over $k, g_L \leq g_K$. For any divisor $\mathscr{U}$ of K, a base of $F_K(\mathscr{U})$ is a part of a base of $F_L(\mathscr{U})$, and hence $N_K(\mathscr{U}) \leq N_L(\mathscr{U})$.*

Proof. The last part immediately follows from the fact that $F_K(\mathscr{U}) \subset F_L(\mathscr{U})$, if we observe that K and l are linearly disjoint over k and that $l = l_0$. Taking a divisor $\mathscr{U}$ of K such that

$$-d_K(\mathscr{U}) > 2g_K - 2, -d_L(\mathscr{U}) > 2g_L - 2, \qquad \text{we have}$$
$$N_K(\mathscr{U}) = d_K(\mathscr{U}) - g_K + 1,$$
$$N_L(\mathscr{U}) = d_L(\mathscr{U}) - g_L + 1,$$

and it follows from the previous inequality that $g_L \leq g_K$. □

Theorem 2. *If l_0 is separably generated over $k, g_K = g_L$ and a basis of $F_K(\mathscr{U})$ is also a base of $F_L(\mathscr{U})$ for any divisor $\mathscr{U}$ of K; hence $N_L(\mathscr{U}) = N_K(\mathscr{U})$.*

Proof. We first consider the case $l_0 = k(u), u$ transcendental over k. Let 148
$Z \in F_L(\mathscr{U})$. Then Z can be written uniquely in the from

$$Z = \frac{F(u)}{G(u)} = \frac{\sum\limits_{\nu=o}^{n} a_\nu u^\nu}{u^m + \sum\limits_{\mu=o}^{m-1} b_\mu u^\mu}, a_\nu, b_\mu \in K$$

with F and G coprime. We shall show that $b_\mu \in K$. □

Let $\mathscr{K}$ be a prime divisor of L lying over a prime divisor $\mathscr{Y}$ of K. Then by the remark at the end of the previous lecture,

$$v_{\mathscr{K}}(G(u)) = v_{\mathscr{K}}(u^m + b_{m-1}u^{m-1} + \cdots + b_m) = \min(0, v_{\mathscr{Y}}(b_1), \ldots, v_{\mathscr{Y}}(b_m)) \leq 0$$

Hence the only possible prime divisors which occur in the numerator $\mathfrak{z}_{G(U)}$ of $G(u)$ are those which over K. But now, since $Z \in F_L(\mathscr{U})$, the divisor

$$(Z)\mathscr{U}^{-1} = \frac{\mathfrak{z}_F \mathscr{N}_G}{\mathscr{N}_F \mathfrak{z}_G \mathscr{U}}$$

is integral, and since $\mathfrak{z}_G$ and $\mathscr{N}_G$ are coprime, any prime divisor occurring in $\mathfrak{z}_G$ must divide $\mathfrak{z}_F$. But since F and G are coprime, there exist polynomials $F_1(u)$ and $G_1(u)$ with

$$F(u)F_1(u) + G(u)G_1(u) = 1.$$

If $F_1(u) = c_o + c_1 u + \cdots + c_t u^t$ and $\mathscr{U}$ a prime divisor of L variable over K, we would have

$$v_{\mathscr{U}}(F_1(u)) \geq \min_\nu (v_{\mathscr{U}}(c_\nu) + \gamma v_{\mathscr{U}}(u)) = 0$$

149 since $v_{\mathscr{U}}(u) = v_{\mathscr{U}}(V_{\mathscr{U}}(c_\nu)) = 0$. Similarly $v_{\mathscr{U}}(G_1(u)) \geq 0$. Hence we have

$$\begin{aligned} 0 = v(1) &\geq \min(v_{\mathscr{U}}(F(u)) + v_{\mathscr{U}}(F_1(u)), v_{\mathscr{U}}(G(u)) + v_{\mathscr{U}}(G(u)) \\ &\geq \min(v_{\mathscr{U}}((F(u))), v_{\mathscr{U}}(g(u))), \end{aligned}$$

and therefore $\mathfrak{z}_{G(u)}$ and $\mathfrak{z}_{F(u)}$ can not have a common prime divisor. Therefore $\mathfrak{z}_{G(u)} = \mathscr{N}$ and $G(u)$ is constant.

It follows that for any prime prime divisor $\mathscr{Y}$ of K,

$$v_{\mathscr{Y}}(Z) = v_{\mathscr{Y}}(F(u)) = \min_{\nu} v_{\mathscr{Y}}(a_\nu) \geq v_{\mathscr{Y}}(\mathscr{U})$$

and therefore $a_\nu \in F_K(\mathscr{U})$.

Thus, we see that $F_L(\mathscr{U})$ is the vector space generated over $l = l_0$ by $F_K(\mathscr{U})$. from the liner disjointness of K and l, we deduce that $N_K(\mathscr{U}) = N_L(\mathscr{U})$.

Next suppose $l = l_0 = k(\alpha)$ is finite separable (and therefore simple) over k. Any element $Z \in F_L(\mathscr{U})$ can be written uniquely in the form

$$Z = c_0 + c_1\alpha + \alpha + c_{n-1}\alpha^{n-1}, c_i \in K$$

where n is the degree of α over k or K.

Let L_1 be the smallest normal extension of L over K. Taking conjugates in the above equation over K, we obtain

$$Z^{(i)} = c_0 + c_1\alpha^{(i)} + \cdots + c_{n-1}\alpha^{(i)^{n-1}}(i = 1, \ldots n)$$

We may solve for c_k of obtain 150

$$a_k = \frac{\begin{vmatrix} 1\alpha^{(1)} & \cdots & \alpha^{(1)^{k-2}}Z^{(1)} & \cdots & \alpha^{(1)^k} & \cdots & \alpha^{(1)^{n-1}} \\ 1\alpha^{(n)} & \cdots & \alpha^{(n)^{k-2}}Z^{n} & \cdots & \alpha^{(n)^k} & \cdots & \alpha^{(n)^{n-1}} \end{vmatrix}}{\begin{vmatrix} 1\alpha^{(1)} & \cdots\cdots\cdots\cdots\cdots\cdots & \alpha^{(1)^{n-1}} \\ 1\alpha^{(n)} & \cdots\cdots\cdots\cdots\cdots\cdots & \alpha^{(n)^{n-1}} \end{vmatrix}}$$

The denominator is a constant $\neq 0$ and the numerator is a linear combination of $Z^{(i)}$ with constant coefficients. Since $\mathscr{U}$ is a divisor of K, it may be easily verified that every conjugate $Z^{(i)}$ of Z is divisible by $\mathscr{U}$ in L_1. Hence the c_k are divisible by $\mathscr{U}$ in L_1 and hence in K. We have proved in this case also that $F_L(\mathscr{U})$ is generated by $F_K(\mathscr{U})$ over i. The equality $N_L(\mathscr{U}) = N_K(\mathscr{U})$ again follows from the liner disjointness of K and $l = l_o$ over k.

The case of any separably generated extension l_0 now follows along familiar lines. Any $Z \in F_L(\mathscr{U})$ is contained in a field $L^1 = Kl^1$, where l^1 is a finitely separably generated extension of k; hence it is an element of $F_{L^1}(\mathscr{U})$. But in the case of a finitely separably generated extension, the theorem follows by induction if we use the first two cases. Hence we again obtain the fact that $F_L(\mathscr{U})$ is generated by $F_K(\mathscr{U})$ over l, and the equality $N_L(\mathscr{U}) = N_K(\mathscr{U})$.

Choosing a divisor $\mathscr{U}$ with $-d_k(\mathscr{U}) > 2g_K - 2, -d_L(\mathscr{U}) > 2g_L - 2$

151 we have $\quad - d_K(\mathscr{U}) = N_K(\mathscr{U}) - g_K + 1,$

and $\quad - d_L(\mathscr{U}) = N_L(\mathscr{U}) - g_L + 1.$

But since $\lambda_{L/K} = 1$, it follows that $d_K(\mathscr{U}) = d_L(\mathscr{U})$ and therefore $g_L = g_K$. The theorem is completely proved.

Theorem 3. *For any constant field extension L of K, we have $g_L\lambda_{L/K} \leq g_K$. (In particular $g_L \leq g_K$).*

Proof. Since the genus is preserved for for a purely transcendental extension of the constant field, and since $\lambda_{L/K} = 1$for such an extension, it follows from the obvious formula $\lambda_{L/L^1}\lambda_{L^1/K} = \lambda_{L/K}L \supset L^1 \supset K$ that it is enough to prove the theorem for algebraic extension l_0 of k. □

First assume that l_0 is a finite extension of k with a basis $\alpha_1, \ldots, \alpha_n$ over k. By lemma 1 of the previous lecture, L/K is a finite extension of degree $n_o \leq n$, and we may assume that $\alpha_1, \ldots, \alpha_{n_0}$ form a basis of L over K.

Let us denote by $\mathscr{X}_K$ and $\mathscr{X}_L$ the vector spaces of repartitions of K and L over k and l respectively. We define a map σ of the direct product $\prod\limits_{\nu=1}^{n_o} \mathscr{X}_K$ of $\mathscr{X}_K$ by itself n_o times into the space $\mathscr{X}_L$ by defining the image of $(\mathscr{C}_1, \ldots, \mathscr{C}_{n_0}) \in \prod\limits_{\nu=1}^{n_0} \mathscr{X}_K$ in $\mathscr{X}_L$ to be the repartition $\mathscr{C}$ of L defined by

$$\mathscr{C}(\mathscr{K}) = \sum_{\nu=1}^{n_o} \alpha_\nu \mathscr{C}_\nu(\mathscr{Y})$$

152 for any prime divisor $\mathscr{K}$ of L, where $\mathscr{Y}$ is the prime divisor of K lying below $\mathscr{K}$. It is easy to verify that $\mathscr{C}$ so defined is a repartition, and that σ is a k-isomorphism of $\prod\limits_{\nu=1}^{n_0} \mathscr{X}_K$ into $\mathscr{X}_L$. Let the image under σ be the subspace $\mathscr{X}_L^o$ of $\mathscr{X}_L \mathscr{X}_L^o$ is a vector subspace of $\mathscr{X}_L$, if the latter is considered as a vector space over k.

If $y = \sum\limits_{1}^{n_0} \alpha_\nu x_\nu,\ x_\nu \in K$, is any element of L, the element $(x_1, \ldots, x_{n_0})$ of $\prod\limits_{\nu=1}^{n_0} \mathscr{X}_K$ (keeping in mind that we have identified $K(L)$ with a subspace of $\mathscr{X}_K(\mathscr{X}_L)$ and we may use the same symbol for an element of $K(L)$ and the corresponding repartition in $\mathscr{X}_K(\mathscr{X}_L)$) clearly goes to the repartition y of $\mathscr{X}_L$. Hence, $\mathscr{X}_L^0 \supset L$. We assert that for any divisor $\mathscr{U}$ of K, we have

$$\mathscr{X}_L = \mathscr{X}_L^0 + \Lambda_L(\mathscr{U})$$

To prove this, consider a repartition $\mathscr{C}$ of L. Let $\mathscr{K}_1, \ldots, \mathscr{K}_r$ be the prime divisors of L lying over a prime divisor $\mathscr{Y}$ of K. We can find an element $y(\mathscr{Y})$ of L satisfying

$$v_{\mathscr{K}_\nu}(y(\mathscr{Y}) - \mathscr{C}(\mathscr{K}_\nu)) \geq v_{\mathscr{K}_\nu}(\mathscr{U}),\ (\nu = 1, \ldots r)$$

Define a repartition $\mathscr{Y}$ of L by

$\mathscr{Y}(\mathscr{K}) = y(\mathscr{Y})$ if $\mathscr{K}$ lies over $\mathscr{Y}$ and $v_{\mathscr{K}^1}(\mathscr{U}) < 0$ or if $\mathscr{K}$ lies over $\mathscr{Y}$ and $v_{\mathscr{K}}(\mathscr{C}) \neq 0$ for some prime divisor $\mathscr{K}^1$ lying over $\mathscr{Y}$, $\mathscr{Y}(\mathscr{K}) = 0$ otherwise.

Clearly, $\mathscr{C} - \mathscr{Y} \Lambda_L(\mathscr{U})$. We shall show that $\mathscr{Y} \varepsilon \mathscr{X}_L^0$. Let $y(\mathscr{Y}) = \sum\limits_{\nu=1}^{n_o} \alpha_\nu y_\nu^1(\mathscr{Y}), y_\nu^1(\mathscr{Y}) \in K$. Define repartitions $\mathscr{Y}_\nu^1$ of $K (\nu = 1, \ldots n_0)$ by putting 153

$\mathscr{Y}_\nu^1(\mathscr{Y}) = y^1(\mathscr{Y})$ if $v_{\mathscr{Y}}(\mathscr{U}) \neq 0$ or $v_{\mathscr{K}}(\mathscr{C}) < 0$ for some $\mathscr{K}$ lying over $\mathscr{Y}$, $\mathscr{Y}_\nu^1(\mathscr{Y}) = 0$ otherwise.

We then have $\sigma((\mathscr{Y}_1^1, \ldots, \mathscr{Y}_{n_o}^1)) = \mathscr{Y} \in \mathscr{X}_L^0$. Our assertion in proved.

Now, if $\mathscr{N}$ denotes the unit divisor, we have

$$\dim_k \frac{\mathscr{X}_k}{\Lambda_K(\mathscr{N}) + K} = g_K$$

and
$$\dim_l \frac{\mathscr{X}_L}{\Lambda_L(\mathscr{N}) + L} = g_L$$

From the first equation,

$$n_0 g_K = \dim_k \frac{\prod\limits_{\nu=1}^{n_0} \mathscr{X}_K}{\prod\limits_{\nu=1}^{n_0} \Lambda_K(\mathscr{N}) + \prod\limits_{\nu=1}^{n_0} K}$$

and applying σ

$$n_0 g_K = \dim_K \frac{\mathscr{X}_L^0}{\Lambda_L^0(\mathscr{N}) + L},$$

154 where $\Lambda_L^0(\mathscr{U})$ is the k-subspace $\sigma(\prod\limits_{\nu=1}^{n_0} \Lambda_K(\mathscr{U}))$ of $\mathscr{X}_L$ for any divisor $\mathscr{U}$ of K.

On the other hand,

$$\begin{aligned} ng_L &= n \dim_l \frac{\mathscr{X}_L}{\Lambda_L(\mathscr{N}) + L} = \dim_k \frac{\mathscr{X}_L}{\Lambda_L(\mathscr{N}) + L} \\ &= \dim_k \frac{\mathscr{X}_L^o + \Lambda_L(\mathscr{N}) + L}{\Lambda_L(\mathscr{N}) + L} = \dim_k \frac{\mathscr{X}_L^o}{\mathscr{X}_L^o \cap (\Lambda_L(\mathscr{N}) + L)} \\ &= \dim_k \frac{\mathscr{X}_L^0}{\Lambda_L^o(\mathscr{N}) + L} - \dim_k \frac{\mathscr{X}_L^0 \cap (\Lambda_L(\mathscr{N}) + L)}{\Lambda_L^o(\mathscr{N}) + L} \end{aligned}$$

($\Lambda_L^0(\mathscr{N})$ is obviously a subspace of $\mathscr{X}_L^0 \cap (\Lambda_L(\mathscr{N}) + L)$). Hence we deduce that

$$\begin{aligned} ng_L &\leq n_0 g_K \\ g_L &\leq \frac{n_0}{n} g_K \end{aligned}$$

But if X is any element of K transcendental over k, we obtain

$$\begin{aligned} \lambda_{L/K} = \frac{d_K(\mathscr{N}_X)}{d_L(\mathscr{N}_X)} = \frac{[K : k(X)]}{[L : l(X)]} &= \frac{[K : k(X)]}{[L : k(X)]}.[l(X) : k(X)] \\ &= \frac{[l : k]}{[L : k]} = \frac{n}{n_o} \end{aligned}$$

155 and our result is proved in the case of a algebraic extension l_0 of k.

To prove the theorem in the case of an arbitrary algebraic extension, we shall show that there exists a finite extension l^1_0 of k such that for $L^1 = Kl^1_0$, we have $\lambda_{L/L^1} = 1$. It would then follow from theorem 1 that $g_L \leq g_{L^1}$ and our result would follow.

Let $X \in K$ be transcendental over k and $\mathscr{N}_X$ the denominator of X. We have

$$m = d_K(\mathscr{N}_X) = \Big[K : k(X)\Big],$$
$$m_\circ = d_L(\mathscr{N}_X) = \Big[L : l(X)\Big].$$

A base $x_1, \ldots\ldots x_m$ of $K/k(X)$ spans L over $l(X)$, and hence we have $m - m_\circ$ relations

$$\sum_{\nu=1}^{m} x_\nu C_{\nu\mu} = 0, \ \mu = 1, 2, \ldots\ldots, m - m_\circ$$

with coefficients $C_{\nu\mu}$ in $l(X)$ such that the $m - m_\circ$ vectors

$$(C_{1\mu}, \ldots\ldots C_{m\mu}) \ (\mu = 1, \ldots\ldots, m - m_\circ)$$

are linearly independent over $l(X)$. The rational functions $C_{\nu\mu}$ of X over l have coefficients in a finitely generated subfield $l^1_0 \supset k$ of l. Since $L^1 = Kl^1_0$ is spanned by $x_1, \ldots x_m$ over $l^1_0(X)$ and since the $C_{\nu\mu}$ are in $l^1_0(X)$, we deduce that

$$d_{L^1}(\mathscr{N}_X) \leq \Big[L^1 : l^1_X(X)\Big] \leq m_0 = d_L(\mathscr{N}_X),$$

and since we already have $\lambda_{L/L^1} \geq 1$, we deduce that $\lambda_{L/_L 1} = 1$. **156**

Our theorem is completely proved.

Remark. If $\lambda_{L/_K} > 2$, we can actually assert that $\lambda_{L/_K} g_L < g_K$. For suppose $\lambda_{L/_K} g_L = g_K$. Let ω be a non-zero differential of K. Then, we have

$$d_L((\omega)) = \frac{d_K((\omega))}{\lambda_{L/_K}} = \frac{2g_k - 2}{\lambda_{L/_K}},$$

and hence (since $d_L((\omega))$ is an integer) $\lambda_{L/_K}$ divides $2g_K - 2$. But from the equation $\lambda_{L/K} g_L = g_K$, we deduce that $\lambda_{L/K}$ divides g_K and hence $2g_K$.

This implies that $\lambda_{L/K}$ divides $2, \lambda_{L/K} \leq 2$, which is a contradiction. Hence we have the strict inequality.

If however $\lambda_{L/K} = 2$, we may have $2g_L = g_K$ as the following example follows.

Let k be a field of characteristic 2 and $\alpha_\circ, \alpha_1$ two elements of k such that $\left[k\left(\alpha_0^{\frac{1}{2}}, \alpha_1^{\frac{1}{2}}\right) : k\right] = 4$. Then it can be seen easily that if X is a transcendental element over k, the polynomial $Y^2 - (\alpha_1 + \alpha_1 X^2)$ is an irreducible polynomial of Y over $k(X)$. Hence, if Y is a root of the equation $Y^2 = \alpha_0 + \alpha_1 X^2, [k(X, Y) : k(X)] = 2$. Put $K = k(X, Y)$. It can be proved (see the example for $l \neq l_0$ given in Lecture 21) that the constant fields of $k(X, Y)$ is k.

Now, it can be deduced by taking valuations in the equation $Y^2 = \alpha_0 + \alpha_1 X^2$ that $\mathscr{N}_Y = \mathscr{N}_X$. Hence the elements $1, X, X^2, \ldots X^n, Y, YX, \ldots,$
157 YX^{n-1} are all elements of K divisible by $\mathscr{N}_X^{-n}$. Since they are linearly independent, we have $l(\mathscr{N}_X^{-n})] \geq 2n+1$, and the Riemann-Roch theorem gives $g_K = 0$.

Now, let l_0 be any extension of k such that $\left[l_0\left(\alpha_0^{\frac{1}{2}}, \alpha_1^{\frac{1}{2}}\right) : l_0\right] < 4$, and $L = Kl_0$. Since $g_L \lambda_{L/_K} \leq g_K = 0$, we necessarily have $g_L = 0$. We shall show that $\lambda_{L/_K} = 2$. In fact, since $\left[l_0\left(\alpha_0^{\frac{1}{2}}, \alpha_1^{\frac{1}{2}}\right) : l_0\right] \leq 2$, there is a relation of the form

$\beta\alpha_\circ^{\frac{1}{2}} + \gamma\alpha_1^{\frac{1}{2}} = \delta, \beta, \gamma, \delta \in l_0$, not all zero.

We may solve for $\alpha_0^{\frac{1}{2}}$ and $\alpha_1^{\frac{1}{2}}$ from this and the equation

$$\alpha_0^{\frac{1}{2}} + X\alpha_1^{\frac{1}{2}} = Y,$$

since $\beta X - \gamma \neq 0$, thus proving that $\alpha_0^{\frac{1}{2}}, \alpha_1^{\frac{1}{2}} \in l_0(X, Y)$, $l = l_0\left(\alpha_\circ^{\frac{1}{2}}, \alpha_1^{\frac{1}{2}}\right)$. Hence, $L = l(X)$ and $d_L(\mathscr{N}_X) = 1$, Since $d_K(\mathscr{N}_X) = 2, \lambda_{L/K} = 2$.

One can in fact show that the above example covers the general case when $g_L = g_K$ and $\lambda_{L/_K} > 1$.

To prove this, we first observe that we must have $g_L = g_K = 0$, for otherwise, we would obtain

$$g_L < \lambda_{L/K} g_L \leq g_K.$$

If now, W were the canonical class of K, $d(W^{-1}) = 2$ and $N(W^{-1}) = 3$. Hence there exists an integral divisor $\mathscr{U}$ in the class W^{-1} of degree 2, and $N_K(\mathscr{U}^{-1}) = 3$. Let $1, X, Y$ be a basis of $F_K(\mathscr{U}^{-1})$. Then X is not a 158 constant, and since $\mathscr{N}_X$ divides $\mathscr{U}$ and $d(\mathscr{U}) = 2$, we see that $\mathscr{U} = \mathscr{N}_X$. Hence,

$$\left[K : k(X)\right] = d(\mathscr{N}_X) = 2.$$

Now, we assert that $Y \notin k(X)$. For if it were, we can write $Y = \dfrac{f_1(X)}{f_2(X)}$, f_1 and f_2 being coprime polynomials. Then, $(Y) = \dfrac{\mathfrak{z} f_1}{\mathfrak{z} f_2} \mathscr{N}_X^{\deg f_2 - \deg f_1}$, and since $(Y)\mathscr{N}_X$ is integral, we deduce that f_2 is constant and $\deg f_1 = 1$. This contradicts our assumption that $1, X, Y$ are linearly independent. Hence, $k(X, Y) \neq k(X)$, and since $\left[K : k(X)\right] = 2, K = k(X, Y)$. Also, since $\lambda_{L/K} > 1$, Y should be purely inseparable over $k(X)$, and therefore satisfy an equation of the form

$$Y^2 = R(X),$$

$R(X)$ being a rational function of X. Since Y^2 is divisible by $\mathscr{N}_X^{-2}$, we deduce by an argument similar to the one used above that $R(X)$ is a polynomial of degree at most two. Thus,

$$Y^2 = \alpha_\circ + \alpha_1 X + \alpha_2 X^2$$

Since X should also be purely inseparable over $k(Y)$, we deduce that $\alpha_1 = 0$.

Now, if $\left[k\left(\alpha_\circ^{\frac{1}{2}}, \alpha_2^{\frac{1}{2}}\right) : k\right]$ were not equal to 4, it is less than or equal to 2. Hence we have a relation of the form

$$\beta\alpha_\circ^{\frac{1}{2}} + \gamma\alpha_2^{\frac{1}{2}} = \delta, \beta, \gamma, \delta \in k.$$

This together with the relation 159

$$\alpha_\circ^{\frac{1}{2}} + \alpha_2^{\frac{1}{2}} X = Y$$

proves that $\alpha_\circ^{\frac{1}{2}}, \alpha_2^{\frac{1}{2}}$, are both in K and hence in k. This would imply that $Y \in K(X)$, which if false. Hence,

$$\left[k\left(\alpha_\circ^{\frac{1}{2}}, \alpha_2^{\frac{1}{2}}\right) : k\right] = 4.$$

Finally, suppose $\left[l_0\left(\alpha_0^{\frac{1}{2}}, \alpha_2^{\frac{1}{2}}\right) : l_0\right] = 4$. Then for any subfield l_0^1 of l_0 containing k, we have $\left[l_0^1\left(\alpha_0^{\frac{1}{2}}, \alpha_2^{\frac{1}{2}}\right) : l_0^1\right] = 4$. Hence the constant field of Kl_0^1 is l_0^1. This implies that (see Lecture 22) $\lambda_{L/K} = 1, a$ contradiction.

Our assertion is proved.

If $g_L = g_K > 0$, we deduce from the equation

$$g_L = \lambda_{L/K} g_L = g_K$$

that $\lambda_{L/K} = 1$.

We now prove the following

Theorem . *If $g_L = g_K$ and $\lambda_{L/K} = 1$, then for any divisor $\mathscr{U}$ of K a basis of $F_K(\mathscr{U})$ over k is also a basis of $F_L(\mathscr{U})$ over l; in particular $N_L(\mathscr{U}) = N_K(\mathscr{U})$.*

Proof. Let us denote by $lF_K(\mathscr{U})$ the vector space generated over l by $F_K(\mathscr{U})$ in L. Clearly we have $lF_K(\mathscr{U}) \subseteq F_L(\mathscr{U})$. Since $\lambda_{L/K} = 1$, l and K are linearly disjoint over k and we obtain

$$N_K(\mathscr{U}) = \dim_l lF_K(\mathscr{U}) \leq \dim_l F_L(\mathscr{U}) = N_L(\mathscr{U})$$

160 Now, let $\mathscr{U}$ be any divisor with $d_K(\mathscr{U}) = d_L(\mathscr{U}) < 2 - 2g_K$. □

Then we have

$$N_K(\mathscr{U}) + d_K(\mathscr{U}) = 1 - g_K,$$
$$N_L(\mathscr{U}) + d_L(\mathscr{U}) = 1 - g_L,$$

and since $d_K(\mathscr{U}) = d_L(\mathscr{U})$ and $g_K = g_L$, we obtain

$$N_K(\mathscr{U}) = N_L(\mathscr{U}),$$

and $$lF_K(\mathscr{U}) = F_L(\mathscr{U}).$$

To draw the same conclusion for an arbitrary divisor $\mathscr{U}$, choose two divisors δ and $\mathcal{L}$ of K such that (i) the least common multiple of δ and $\mathcal{L}$ is $\mathscr{U}$ and (ii)$d(\delta) < 2 - 2g_K, d(\mathcal{L}) < 2 - 2g_L$. This is clearly possible. We then have $F_K(\delta) \cap F_K(\mathcal{L}) = F_K(\mathscr{U}), F_L(\delta) \cap F_L(\mathcal{L}) = F_L(\mathscr{U})$.

Let $\alpha_1, \ldots, \alpha_m$ be a basis of $F_K(\mathscr{U})$. Complete this to a basis $\beta_1, \ldots$, $\beta_1, \alpha_1, \ldots, \alpha_m$ of $F_K(\delta)$ and to a basis $\gamma_1, \ldots$, $\gamma_n, \alpha_1, \ldots, \alpha_m$ of $F_K(\mathcal{L})$. We assert that $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_1, \gamma_1, \ldots, \gamma_n$ are linearly independent elements of K over k. In fact, if we had a linear relation

$$\sum a_i\alpha_i + \sum b_j\beta_j = \sum c_k\gamma_k,\ a_i, b_j, c_k \in k,$$

since the left side is an element of $F_K(\delta)$ and the right side an element of $F_K(\mathcal{L})$, $\sum c_k\gamma_k$ is an element of $F_K(\mathscr{U})$ and therefore $c_k = 0, a_i = 0$ and $b_j = 0$. Hence $\beta_1, \ldots, \beta_l, \alpha_1, \ldots, \alpha_m, \gamma_1, \ldots, \gamma_n$ is also a set of linearly independent elements over l. 161

Now suppose y is an element of $F_L(\mathscr{U}) = F_L(\delta) \cap F_L(\mathcal{L})$. Since $F_L(\delta)$ has for basis $(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots \beta_l)$ over 1 and $y \in F_L(\delta)$, we have

$$y = \sum_i a_i\alpha_i + \sum_j b_j\beta_j,\ a_i, b_j \in l,$$

and similarly, since $y \in F_L(\mathcal{L})$ and $F_L(\mathcal{L})$ has for basis $(\alpha_1, \ldots, \alpha_m, \gamma_1, \ldots, \gamma_n)$, we have

$$y = \sum_j c_j\alpha_j + \sum_K d_k\gamma_k,\ c_j, d_k \in l.$$

Equating the above two expressions for y, we obtain (since $\alpha_1, \ldots$, $\alpha_m, \beta_1, \ldots, \beta_1, \gamma_1, \ldots, \gamma_n$ are linearly independent over l)

$$a_i = c_i\ ,\ b_j = d_k = 0.$$

Thus $y \in lF_K(\mathscr{U})$ and hence we have $F_L(\mathscr{U}) = lF_K(\mathscr{U})$. Again by linear disjointness of l and K over k, we obtain

$$N_K(\mathscr{U}) = N_L(\mathscr{U})$$

Our theorem is proved.

The converse of the above theorem is very easy to prove. If $N_K(\mathscr{U}) = N_L(\mathscr{U})$ for all divisors $\mathscr{U}$, or even only for a sequence of 162 divisors $\mathscr{U}$ with $d_k(\mathscr{U}) \to -\infty$, we have the following equations for $-d_k(\mathscr{U})$ sufficiently large

$$\begin{aligned} N_K(\mathscr{U}) + d_K(\mathscr{U}) &= 1 - g_K, \\ N_L(\mathscr{U}) + d_L(\mathscr{U}) &= 1 - g_L. \end{aligned}$$

Hence we obtain

$$\lambda_{L/K} = \frac{d_K(\mathscr{U})}{d_L(\mathscr{U})} = \frac{-N_K(\mathscr{U}) + 1 - g_K}{-N_L(\mathscr{U}) + 1 - g_L},$$

and letting $d_K(\mathscr{U}) \to -\infty$, and observing that the right hand side has limit 1, we obtain $\lambda_{L/_K} = 1$. Hence $d_K(\mathscr{U}) = d_L(\mathscr{U})$ for any divisor $\mathscr{U}$, and we obtain $g_K = g_L$.

Corollary. *If $g_L = g_K$ and $\lambda_{L/K} = 1$, the natural homomorphism of the class group $\mathscr{K}_K$ of K into the class group $\mathscr{K}_L$ of L is an isomorphism. Under this isomorphism, the canonical class of K goes to the canonical class of L.*

Proof. Let $\mathscr{U}$ be any divisor of K which is a principal divisor in L. Then $d_L(\mathscr{U}) = 0$ and $N_L(\mathscr{U}) = 1$. By the above theorem, $d_K(\mathscr{U}) = 0$ and $N_K(\mathscr{U}) = 1$. This proves that $\mathscr{U}$ is a principal divisor of K, and thus the kernel of the homomorphism of $\mathscr{K}_K$ consists of the unit class alone. Thus, the map is an isomorphism. We shall use the same symbol for a class of K and its image as a class of L. □

163 Also, if W_K is the canonical class of K, $d_L(W_K) = d_K(W_K) = 2g_L - 2$ and $N_L(W_K) = N_K(W_K) = g_L$, which proves that W_K is the canonical class of L.

39 The Zeta Function of an Extension

Let $K/_k$ be an algebraic function field with a finite field of constants k containing q elements. Let k_f be the extension of k of degree f. Since

k is perfect, k_f/k is a separable extension, and hence the constant field of $L_f = Kk_f$ is k_f. Let $\mathscr{Y}$ be a prime divisor of K and $\mathscr{K}_1, \ldots, \mathscr{K}_h$ the prime divisors of L_f lying over $\mathscr{Y}$. Then, since k_f/k is separable, the $\mathscr{K}_i$ are unramified over K, and we have

$$\mathscr{Y} = \mathscr{K}_1 \ldots\ldots \mathscr{K}_h.$$

Now, since k_f/k is separable, we know that $L_{\mathscr{K}_i} = k_{\mathscr{Y}} k_f$, and since the degrees of $K_{\mathscr{Y}}$ and k_f over k are respectively $d_K(\mathscr{Y})$ and f, the degree of $L_{\mathscr{K}_i}$ over k is l.c.m. $[d_K(\mathscr{Y}), f]$. Thus,

$$f d_{L_f}(\mathscr{K}_i) = \frac{f d_K(\mathscr{Y}}{(f, d_K(\mathscr{Y}))}$$

But we know that

$$f = \left[k_f : k\right] = \left[L_f : K\right] = \sum_{i=1}^{h} d_{L_f/K}(\mathscr{K}_i) = h d_{L_f/K}(\mathscr{K}_1),$$

and using the relation

$$d_{L/K}(\mathscr{K}_1) d(\mathscr{Y}) = d_L(\mathscr{K})[l; k],$$

we deduce the formula **164**

$$h = (f, d_K(\mathscr{Y}))$$

An immediate consequence of the above formula is the following

Theorem . *For algebraic function fields with finite constant fields, the least positive value of the degree of its divisors is* 1.

Proof. Let ρ be this least value. Take $f = \rho$ in the above formula. □

We obtain, since ρ divides each $d_K(\mathscr{Y})$,

$$h = \rho$$

and also
$$d_{L_f}(\mathscr{K}_i) = \frac{d_K(\mathscr{Y})}{\rho}.$$

Substituting in the Euler product for $\zeta(s, L_f)$, we obtain

$$\zeta(s, L_f) = \prod_{\mathscr{X}} \left(1 - q^{-sfd_{L_f}(\mathscr{X})}\right)^{-1} = \prod_{\mathscr{Y}} \prod_{i=1}^{h} \left(1 - q^{-sd_K(\mathscr{Y})}\right)^{-1}$$
$$= (\zeta(s, K))^h = (\zeta(s, K))^\rho$$

Since both $\zeta(s, L_f)$ and $\zeta(s, K)$ have a pole of order 1 at $s = 1$, we deduce that $\rho = 1$.

Finally, we prove a theorem expressing the zeta function of a finite constant field extension in term of the L-series of the ground field.

Theorem. *With the same notation as above, we have*

$$\zeta(s, L_f) = \prod_{\nu=1}^{f} L(s, \chi_{f,\nu}, K)$$

165 *where $\chi_{f,\nu}$ is the character on the class group taking the value $e^{\frac{2\pi i\nu}{f}}$ on all classes of degree* 1.

Proof.

$$\zeta(s, L_f) = \prod_{\mathscr{X}} \left(1 - N_{L_f}\mathscr{X}^{-s}\right)^{-1} = \prod_{\mathscr{Y}} \prod_{\mathscr{X}/\mathscr{Y}} \left(1 - q^{-sfd_{L_f}(\mathscr{X})}\right)^{-1}$$
$$= \left\{\prod_{\mathscr{Y}} (1 - N_K\mathscr{Y}^{-s\frac{f}{(f, d_K(\mathscr{Y}))}}\right\}^{-(f, d_K(\mathscr{Y}))}$$
$$= \prod_{\mathscr{Y}} \prod_{\nu=1}^{f} \left(1 - e^{\frac{2\pi i\nu}{f} d_K(\mathscr{Y})} N_K\mathscr{Y}^{-s}\right)^{-1}$$

(the last follows from the easily established formula $\prod\limits_{\nu=1}^{r} \left(1 - e^{\frac{2\pi i\nu}{r}s} z\right) = \left(1 - z^{\frac{r}{(r,s)}}\right)^{(r,s)}$ for positive integral r, s)

$$= \prod_{\nu=1}^{f} \zeta\left(s - \frac{2\pi i\nu}{f \log q}, K\right) = \prod_{\nu=1}^{f} L(s, \chi_{f,\nu}, K)$$

The proof of the theorem is complete. □

Bibliography

[1] Artin, E. - Algebraic numbers and algebraic functions. Princeton 1950-51.

[2] Artin, E. - Quadratische korper im gebiet der hoheren kongruenzen. I and II. Math. Zeit. 19 (1924) p. 153-206, 207-246.

[3] Chevalley, C. - Introduction to the theory of algebraic functions of one variable. Mathematical Surveys. Number VI. Amer. Math. Soc. 1951.

[4] Dedekind, R. & Weber, H. - Theorie der algebraischen funktionen einer veranderlichen J. reine angew. math. 92(1882) p. 181-290.

[5] Hensel, K. & Landsberg, G. - Theorie der algebraischen funktionen einer variablen und ihre anwendung auf algebraische kurven und Abelsche Integrale. Leipzing. 1902.

[6] Kronecker, L. - Grundzuge einer arithmetischen theorie der algebraischen grossen. Werke Band 2.

[7] Riemann, B. - Theorie der Abelschen functionen. J. Reine angew. Math. 54 (1857). Werke Zweite Auflage Erste Abtheilung. VI p. 88-142.

[8] Roch, G. - Über die Anzahl der wilkurlicher Konstanten in algebraischen Funktionen. J. reine angew. Math. 64 (1865) p. 372-376.

[9] Schmid, H. L. & Teichmuller, O. - Ein neuer bewies fur die Funktion algeichung der L-reihen. Abh. Math. sem. Hans. univer. 15 (1943) p. 85-96.

[10] Schmidt, F. K. - Analytische zahlentheorie in korpern der charakteristik p. Math. Zeit. 33 (1931) p. 1-32.

[11] Schidt, F.K. - zur arithmetischen theorie algebrische funktionen I. Math. Zeit. 41 (1936) p. 415-438.

[12] Tate, J. - Genus change in inseparable extensions of function fields. Proc. Amer. Math. Soc. 3 (1952) p. 400-406.

[13] Weil, A. - Zur algebraischen theorie der algebraischen funktionen. J. reine angew. Math. 179 (1938) p. 129-133.

[14] Weissinger, J. - Theorie der divieoren Kongruenzen. Abh. Math. sem. Hans. Univer. 12 (1938) p. 115-126.