ON CHEVALLEY'S PROOF OF LUROTH'S THEOREM

SERGE LANG AND JOHN TATE

Let k be a function field in one variable over a constant field k_0, and let g be its genus. By a subfield of k we shall always mean a subfield k' properly containing k_0 so that k' is likewise a function field with k_0 as constants. We let g' be the genus of k'.

If k/k' is separable, then the classical formula

$$2g - 2 = n(2g' - 2) + \mu$$

where μ is a non-negative integer and $n = (k:k')$ shows that $g' \leqq g$. If k/k' is inseparable, then g' may be greater than g. Nevertheless, we have:

THEOREM 1. *If k is separably generated over k_0 then $g' \leqq g$.*

PROOF. In view of the above remarks we may assume k/k' is purely inseparable. Let p be the characteristic. Then k/k' is a p-tower in which each step is of degree p and is inseparable. We may further assume that $(k:k') = p$ because a subfield of a separably generated field is also separably generated. (This is an immediate consequence of MacLane's criterion that k is separably generated over k_0 if and only if k is linearly disjoint from $k_0^{1/p}$ over k_0.)

Let x be a separating variable for k over k_0 so that we may write $k = k_0(x, y)$ where y is separable over $k_0(x)$. Then we also have $k = k_0(x, y^p)$. We see that $k_0(x^p, y^p) \subset k'$ and in fact we must have $k' = k_0(x^p, y^p)$ because

$$(k: k_0(x^p, y^p)) = (k_0(x, y^p): k_0(x^p, y^p)) \leqq p = (k: k').$$

Thus $k' = k_0 k^p$. But k^p/k_0^p is an isomorphic image of k/k_0, and therefore the genus of k^p (considered as function field over the constant field k_0^p) is g. Since k' may be regarded as a constant field extension of k^p its genus g' is at most g, as was to be shown.

That the genus cannot increase in a constant field extension is proved in [1] and [2].

Our theorem generalizes the argument used by Chevalley [2, p. 106] to prove Luroth's theorem. Namely, a rational field R is a separably generated field of genus zero. By Theorem 1 any subfield R' is of genus zero. A prime of degree 1 in R induces a prime of degree 1 in R' and hence, by a well known criterion, R' is a rational field.

If the field k is not separably generated, however, the behavior of

Received by the editors December 3, 1951.

its subfields may be much more pathological and for fields of genus zero we can prove the converse of Theorem 1. In fact we prove more:

THEOREM 2. *A field of genus zero which is not separably generated over its constant field contains subfields of arbitrarily high genus.*

PROOF. Let k be a field of genus zero. It is well known and easy to show [1, chap. XVI, 4] that k is either a rational field, or $k=k_0(x, y)$ where x, y satisfy a quadratic equation

$$F(x, y) = ay^2 + (bx + c)y + dx^2 + ex + f = 0.$$

If k is not separably generated, then the characteristic of the field must be 2 and the partial derivatives $\partial F/\partial x$ and $\partial F/\partial y$ must both vanish. Consequently $k=k_0(x, y)$ where x, y satisfy an equation of the type

$$y^2 = ax^2 + b, \qquad a, b \in k_0. \tag{1}$$

Furthermore, $k_0(a^{1/2}, b^{1/2})$ has degree 4 over k_0. Suppose otherwise, that is, $(k_0(a^{1/2}, b^{1/2}):k_0) \leqq 2$, and say $a^{1/2}$ is a generator of $k_0(a^{1/2}, b^{1/2})$. Then we can write $b^{1/2}=c+da^{1/2}$ with c, d in k_0. In a suitable extension we have $y=a^{1/2}x+b^{1/2}$, and hence $y=a^{1/2}(x+d)+c$. This shows that y and $a^{1/2}$ generate the same field over $k_0(x)$, and that k is rational, contrary to assumption.

We shall now construct hyperelliptic subfields k' of k of arbitrarily high genus.

Let $k'=k_0(z, w)$ where $z=x^2$ and $w=x^{2n+1}+y$, $n\geqq 1$. Then $w^2 =z^{2n+1}+az+b$. We shall prove that k' has genus n by developing the theory of inseparable quadratic extensions of a rational field in analogy with the classical separable theory. We need a lemma.

LEMMA. *Let k_0 be any field of characteristic 2. Let $k_0(x)$ be the rational field in the variable x, and let $k/k_0(x)$ be an inseparable extension of degree 2. Let $f(x)$ be a polynomial in $k_0[x]$ of least degree such that $k=k_0(x, y)$ where $y^2=f(x)$. (Such a polynomial will be called minimal.) Then $\{1, y\}$ is a minimal basis for the integers of k over $k_0[x]$.*

PROOF. Suppose $(r(x)+s(x)y)/t(x)$ is integral over $k_0[x]$ with $r(x)$, $s(x)$, $t(x)$ in $k_0[x]$. We may assume deg r and deg $s<$deg t. We must then show that $r=s=0$. For some polynomial g we have

$$r^2 + s^2f = t^2g.$$

If $s\neq 0$, then g competes with f as a field generator, so deg $g\geqq$deg f. This yields deg $r^2=$deg t^2g, which is impossible. Hence $s=0$ and therefore $r=0$ also, by comparing degrees again. This proves that $\{1, y\}$ is a minimal basis.

THEOREM 3. *Let $k=k_0(x, (f(x))^{1/2})$ be the field defined in the preceding lemma, with $f(x)$ minimal. Then if $f(x)$ is of degree $n>0$, the genus of k is $-[-n/2]-1$ in exact analogy with the classical case.*

PROOF. We first note that $n>0$ implies that k_0 is the constant field of k. Otherwise $k/k_0(x)$ would be generated by $c^{1/2}$ where c lies in k_0, and this would mean $n=0$.

Let $\mathfrak{a}$ be the divisor of the poles of x in k. Then $\mathfrak{a}$ has degree 2 in k. We now determine the dimension $l(\mathfrak{a}^{-\nu})$ of the vector space of multiples of $\mathfrak{a}^{-\nu}$ in two ways.

First by the Riemann-Roch Theorem we have for large ν

$$l(\mathfrak{a}^{-\nu}) = 2\nu + 1 - g. \tag{2}$$

Secondly, using the fact that $\{1, y\}$ is a minimal basis,

$$\begin{aligned} &\text{an integer } r(x)+s(x)y \text{ is a multiple of } \mathfrak{a}^{-\nu} \\ &\leftrightarrow \mathfrak{a}^{-2\nu} \mid r^2 + s^2 f \\ &\leftrightarrow \deg (r^2 + s^2 f) \leqq 2\nu \\ &\leftrightarrow \deg r \leqq \nu \quad \text{and} \quad \deg s \leqq \nu + [-n/2]. \end{aligned}$$

Each of the preceding equivalences is trivial except possibly the last. But we assumed that $f=a_nx^n+ \cdots +a_0$ is minimal. It follows that a_nx^n is not a square, and therefore

$$\deg (r^2 + s^2 f) = \max (\deg r^2, \deg s^2 f).$$

This immediately implies the last equivalence.

For ν large $(>n/2)$ we obtain

$$l(\mathfrak{a}^{-\nu}) = \nu + 1 + \nu + 1 + [-n/2]. \tag{3}$$

From (2) and (3) we solve for the genus, and get

$$g = - [-n/2] - 1$$

which proves Theorem 3.

In order to complete the proof of Theorem 2 it suffices to show that the polynomial $f(z)=z^{2n+1}+az+b$ is minimal for the extension $k'/k_0(z)$. If this is not the case, let $g(z)$ be minimal. By the lemma we can write

$$(f(z))^{1/2} = r(z) + s(z)(g(z))^{1/2}$$

and squaring we get

$$f(z) = r(z)^2 + s(z)^2 g(z).$$

Differentiating formally with respect to z we get

$$f'(z) = z^{2n} + a = (z^n + a^{1/2})^2 = s(z)^2 g'(z). \tag{4}$$

This shows that in the polynomial domain $k_0(a^{1/2})[z]$, $g'(z)$ is a square: $g'(z) = (l(z) + a^{1/2}m(z))^2$, where the polynomials l and m have coefficients in k_0. Substituting back in (4) we obtain

$$z^n + a^{1/2} = s(z)(l(z) + a^{1/2}m(z)).$$

Comparing coefficients of $a^{1/2}$ we see that $s(z)m(z) = 1$, and that $s(z)$ must be a constant. But in this case deg $g'(z) = 2n$ and therefore deg $g(z) \geqq 2n+1 = \deg f(z)$; $f(z)$ is minimal, and Theorem 2 is proved.

Actually we have not yet shown the existence of inseparably generated fields of genus zero, but this gap is easily filled. Let k_0 be a field of characteristic 2 which contains elements a and b such that $(k_0(a^{1/2}, b^{1/2}):k_0) = 4$. Then the field $k = k_0(x, y)$ defined by equation (1)

$$y^2 = ax^2 + b$$

is of genus zero, is not separably generated, and has k_0 as its field of constants. Indeed, $k/k_0(x)$ is of degree 2. If k_0 were not the constant field, then k would be $k_0(x, c^{1/2})$ where $c \in k_0$, and would therefore be a rational field over $k_0(c^{1/2})$. Then y could be expressed as a rational function in x with coefficients in $k_0(c^{1/2})$; this rational function must in fact be a polynomial because its square is a polynomial. We have $y = a^{1/2}x + b^{1/2}$. This means that $k_0(a^{1/2}, b^{1/2}) \subset k_0(c^{1/2})$ has degree not greater than 2 over k_0, contrary to assumption.

By Theorem 3 we now know that k has genus zero. In the proof of Theorem 2 we have seen that such a field contains hyperelliptic subfields of arbitrarily high genus. By Theorem 1 the field cannot be separably generated, a fact which could of course be established directly.

References

1. E. Artin, *Algebraic numbers and algebraic functions.* I, Notes, New York University, 1950–1951.

2. C. Chevalley, *Introduction to the theory of algebraic functions of one variable,* Mathematical Surveys no. 6, New York, American Mathematical Society, 1951.

3. J. Tate, *Genus change in inseparable extensions of function fields,* Proceedings of the American Mathematical Society vol. 3 (1952) pp. 400–406.

Princeton University