Journal of the Mathematical Society of Japan Vol. 3, No. 1, May. 1951.

On the Group of Automorphisms of a Function Field

Kenkichi IWASAWA and Tsuneo TAMAGAWA

§ 1. Let K be an algebraic function field over an algebraically closed constant field k. It is well-known that the group of automorphisms of K over k is a finite group, when the genus of K is greater than 1. In the classical case, where k is the field of complex numbers, this theorem was proved by Klein and Poincaré[1] by making use of the analytic theory of Riemann surfaces. On the other hand, Weierstrass and Hurwitz gave more algebraical proofs in the same case[2], which essentially depend upon the existence of so-called Weierstrass points of K. Because of its algebraic nature, the latter method is immediately applicable to the case of an arbitrary constant field of characteristic zero. In the case of characteristic $p \neq 0$, H. L. Schmid proved the theorem along similar lines[3]; the proof being based upon F. K. Schmidt's generalization of the classical theory of Weierstrass points in such a case[4].

Now it has been remarked, since Hurwitz, that the representation of the group G of automorphisms of K by the linear transformations, induced by G in the set of all differentials of the first kind of K, is very important for the study of the structure of G. The purpose of the present paper is to show that we can indeed prove the finiteness of G by the help of such a representation instead of the theorem on Weierstrass points. In the next paragraph we analyze the structure of the subgroup $G(p)$ of G, consisting of those automorphisms of K, which leave a given prime divisor P of K fixed, where K may be any function field of genus greater than zero. The finiteness of $G(p)$ is also proved by H. L. Schmid; but his proof depends essentially upon formal calculations of polynomials, whereas our method is more group-theoretical. In the last paragraph we then prove our theorem by considering the above mentioned representation of G and by using a theorem of Burnside on irreducible groups of linear transformations.

---

1) Cf. Poincaré [3]
2) Cf. Weierstrass [6] and Hurwitz [2]
3) Cf. H. L. Schmid [4]
4) Cf. F. K. Schmidt [5]

§ 2. Let K be an algebraic function field over an algebraically closed constant field K, whose characteristic p may be either zero or a prime number. In this paragraph we always assume that the genus g of K is different from zero.

Lemma 1. *Let σ be an automorphism of K*[5]*, which maps a rational subfield $K'=k(x)$ onto itself. If the degree $n=[K:K']$ is prime to p*[6]*, then σ has a finite order, which does not exceed $n(2n+2g-2)(2n+2g-3)(2n+2g-4)$.*

Proof. Let $P^{(1)}, \ldots\ldots, P^{(s)}$ be all the prime divisors of K, which divide the different of K/K', and let $Q^{(i)} (i=1, \ldots\ldots, s)$ be the projection of $P^{(i)}$ in K'. Choose any $Q=Q^{(i)}$, and consider the decomposition

$$Q=P_1^{e_1}\cdots\cdots\cdots P_t^{e_t}$$

of Q in K. As n is prime to p, the contribution of each P_i to the different of K/K' is given by

$$P_1^{e_1-1}\cdots\cdots\cdots P_t^{e_t-1}$$

whose degree is equal to

$$\sum_{i=1}^{t}(e_i-1)=\sum_{i=1}^{t}e_i-t=n-t\leqq n-1$$

On the other hand, the degree d of the different of K/K' is given by

$$d=2n+2(g-1), \tag{1}$$

which is greater than $2(n-1)$, since we have assumed $g>0$. Therefore there exist at least three, but at most d different prime divisors among $Q^{(i)}$.

Now σ obviously leaves the different of K/K' fixed, and it permutes $P^{(i)}$ and $Q^{(i)}$ among themselves. Therefore some of σ, say σ^l, where

$$l\leqq d(d-1)(d-2), \tag{2}$$

leaves three different $Q^{(i)}$'s invariant. However, an automorphism of a rational function field $K'=K(x)$, which leaves three different prime divisors

5) In the following we always consider only those automorphisms of K, which leave every element in k fixed.

6) If p is zero, n may be an arbitrary integer.

fixed, is the identity. Consequently σ^l leaves all elements of K' fixed. As there exist at most n relative automorphisms of K with respect to K', some power of σ^l, say σ^{lm} is the identity automorphism of K, where m is not greater than n. From (1), (2) we have

$$lm \leqq n(2n+2g-2)(2n+2g-3)(2n+2g-4),$$

which proves our lemma.

Now we study the structure of the group $G(P)$, consisting of all automorphisms of K, which leave a prime divisor P of K fixed. For that purpose, let us consider the set $L(P^n)$ of all elements in K whose denominators divide P^n. $L(P^n)$ is a finite dimensional linear space over k, and we denote its dimension by $l(P^n)$. We have then, obviously,

$$k=L(P^0) \subseteqq L(P^1) \subseteqq L(P^2) \subseteqq \cdots\cdots,$$

$$1=l(P^0) \leqq l(P^1) \leqq l(P^2) \leqq \cdots\cdots$$

However the Riemann-Roch theorem tells us that either $l(P^{n+1})=l(P^n)$ or $l(P^{n+1})=l(P^n)+1$ and that the latter case surely occurs if $n>2g-2$. It follows that we can choose a basis

$$x_1, x_2, \cdots\cdots, x_r \qquad (r=l(P^{2g+1}))$$

of $L(P^{2g+1})$ in such a way, that $x_i, x_{i+1}, \cdots\cdots, x_r$ form a basis of some $L(P^{n_i})$ $(n_i \leqq 2g+1)$ for every $i \leqq r$. The denominators of x_1 and x_2 are then just P^{2g+1} and P^{2g} respectively.

Now any automorphism σ of $G(P)$ obviously induces a linear transformation in every $L(P^n)$. In particular we have, for $L(P^{2g+1})$,

$$\sigma(x_j)=\textstyle\sum_{i=1}^r a_{ij}x_i, \qquad a_{ij}\in k, \qquad j=1, \cdots\cdots, r,$$

or simply in a matrix equation

$$(\sigma(x_1), \cdots\cdots, \sigma(x_r))=(x_1, \cdots\cdots, x)A_\sigma, \quad A_\sigma=(a_{ij}).$$

As a result of the particular choice of our basis, A_σ has the following triangular form

$$A_\sigma=\begin{pmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ * & & & a_r \end{pmatrix} \qquad (a_i=a_{ij})$$

and $\sigma \rightarrow A_\sigma$ gives a representation of $G(P)$. Moreover this representation is an isomorphic one. In fact, if A_σ is the unit matrix, σ leaves x_1 and x_2 and, consequently, every element in $k(x_1, x_2)$ fixed. But this field $k(x_1, x_2)$ coincides with K, as one readily sees from the fact that the degree $[K: k(x_1, x_2)]$ divides both degrees $[K: k(x_1)]=2g+1$ and $[K: k(x_2)]=2g$. It follows that such σ is the identity automorphism of K.

By the help of this isomorphic representation we can prove the following

Lemma 2. *The order of any element σ in $G(P)$ is finite and has a bound which depends only upon g and p.*

Proof. Consider the eigen values $u_1, u_2, \ldots\ldots, u_r$ of A_σ and suppose first that all u_i are different from each other. By changing the basis suitably, we may then assume that A_σ is a diagonal matrix, or, in other words,

$$\sigma(x_i)=u_i x_i, \qquad i=1, 2, \ldots\ldots, r.$$

The subfields $k(x_1)$, $k(x_2)$ are, consequently, mapped onto itself by σ. As one of the degrees $[K: k(x_1)]=2g+1$ and $[K: k(x_2)]=2g$ is prime to p, it follows, from Lemma 1, that σ has a finite order, which is bounded by a number depending only upon g and $n=2g+1$ or $2g$.

Now assumme that some u_i and u_j coincide $(i \neq j)$. We can then find linearly independent elements x and y in $L(P^{2g+1})$, such that

$$\sigma(x)=u_i x, \qquad \sigma(y)=u_i(x+y)$$

For $z=\dfrac{y}{x}$ we have then

$$\sigma(z)=z+1,$$

and the field $k(z)$ is mapped onto itself by σ. Moreover, the degree $n=[K: k(z)]$ is not greater than $2(2g+1)$, for the degrees of the denominators of x and y are most $2g+1$ and that of z is, consequently, at most $2(2g+1)$. Therefore, if the characteristic p of k is zero, it follows again from Lemma 1 that the order of σ is finite and has a bound depending only upen g. On the other hand, if p is not zero, we have $\sigma^p(z)=z$, and σ^p is a relative automorphism of K with respect to $k(z)$. It follows that the order of σ^p dose not exceed n and that the order of σ is at most

$2p(2g+1)$.

Now take a prime element u for P, i. e. such an element u in K, which is divisible by P, but not by P^2. For any σ in $G(P)$, $\sigma(u)$ is again a prime element for P, and we have

$$\sigma(u) \equiv \gamma u \mod \mathfrak{P}^2 \tag{3}$$

where γ is a suitable constant and $\mathfrak{P}$ is the prime ideal in the valuation ring of P. As γ is uniquely determined by the above congruence, we may denote it by γ_σ. $\sigma \rightarrow \gamma_\sigma$ is then a representation of $G(P)$ in k, and, if we denote by N the kernel of this representation, $G(P)/N$ is isomorphic to the multiplicative group Γ of γ_σ. However, we know by Lemma 2 that the orders of elements in $G(P)$ are bounded. Therefore, the orders of elements in $G(P)/N$ or in Γ are also bounded. It follows that Γ is the group of all m-th roots of unity in k, where m is a suitable integer prime to p. Therefore $G(P)/N$ is also a cyclic group of order m and $G(P)$ contains an element of order m. As m is prime to p, we can then prove, by a standard argument[7], that

$$m \leqq 6(2g-1). \tag{4}$$

We consider, now, the structure of the normal subgroup N. From (3) it follows immediately that the eigen values α_i of A_σ are powers of γ, and, in particular,

$$\alpha_1 = \gamma^{-(2g+1)}, \qquad \alpha_2 = \gamma^{-2g}$$

This shows that N consists of all those σ in $G(P)$, for which the matrix A_σ has the form

$$\begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ & * & & 1 \end{pmatrix} \tag{5}$$

However, if the characteristic of k is zero, such a matrix can not have a finite order unless it is the unit matrix. Therefore, we see, by Lemma 2,

7) Cf. H. L. Schmid [4]. Note that P ramifies completely in the extension of degree m and that the degree of the different of that extension is at least $m-1$. Cf. the proof of Lemma 4 below.

that N is the unit group if $p=0$. On the other hand, if p is not zero, the group N, which is isomorphic to a group of matrices of the form (5), is a nilpotent group and the order of any element in N is a power of p. In order to show that N is actually a finite p-group in such a case, we first prove some lemmas.

Lemma 3. *Let H be a group of automorphisms of a function field K of genus $g>0$, such that*

1) *H is abelian and the order of any element in H is a power of p,*
2) *every element in H leaves a prime divisor P fixed,*
3) *the fixed field*[8] *of any non-trivial finite subgroup of H is a rational function field.*

Then H is a cyclic group of order either 1, p or p^2.

Proof. Suppose that H is not the unit group, and take a subgroup $U=\{\sigma\}$ of order p. By assumption, the fixed field of U is a rational function field $k(x)$. We can take x in such a way that the denominator of x is P^p. As H is abelian, any τ in H then maps $k(x)$ onto itself, and as the denominator of x is invariant under τ and since the order of τ is a power of p, we have

$$(6) \qquad \tau(x)=x+a \qquad a\in k.$$

It follows that $\tau^p(x)=x$, $\tau^p\in U$, $\tau^{p^2}=e$, so that the order of any τ in H is at most p^2.

To prove the lemma, it is therefore sufficient to show that H contains no subgroup of order p other than U. Suppose, for a moment, that there exists such a subgroup $V=\{\tau\}$ of order p. We shall deduce a contradiction from this assumption. As τ is not in U, a is not zero in (6). Therefore, replacing x by $\frac{x}{a}$, we may assume

$$(7) \qquad \tau(x)=x+1, \qquad \sigma(x)=x$$

In a similar way, we can find an element y such that the denominator of y is p^{p^2} and

---

8) The fixed field K' of a finite group G of automorphisms of K is the set of all elements of G. K/K' is then a Galois extension with the Galoisgroup G. In particular we have $[K:K']=[G:e]$

(8) $$\sigma(y)=y+1, \qquad \tau(y)=y.$$

As y is not contained in $k(x)$, we have $K=k(x, y)$. On the other hand x^p-x and y^p-y are both contained in the fixed field K' of the subgroup $UV=\{\sigma, \tau\}$ of order p^2. However, as these elements have the same denominators P^{p^2} and K' is a rational function field with $[K:K']=p^2$, we must have

$$y^p-y=\beta(x^p-x)+\gamma \qquad \beta, \gamma\in k.$$

If we then put

(9) $$z=y-\beta^{\frac{1}{p}}x,$$

we have

(10) $$z^p-z-\gamma=(\beta^{\frac{1}{p}}-\beta)x.$$

Therefore, if $\beta^{\frac{1}{p}}-\beta=0$, z is constant in k, and (9) gives us $k(x)=k(y)$, which is obviously a contradiction. On the other hand, if $\beta^{\frac{1}{p}}-\beta\neq 0$ (9) and (10) show that x and y are both contained in $k(z)$. We have then $K=k(x, y)=k(z)$, which also contradicts the assumption that the genus of K is not zero. The lemma is thus proved[9].

Lemma 4. *Let K be a function field of genus $g>0$ and H group of automorphisms of K, which satisfies the conditions* 1), 2) *of the previous Lemma. H is then a finite group, and its order does not exceed $p^2(2g-1)$.*

Proof. Let U be an arbitrary finite subgroup of order n in H and K' its fixed field. The genus g' of K' is given by the following formula:

(11) $$2(g-1)=d+2n(g'-1),$$

where d is the degree of the different of K/K'. However, in the present case, d is always at least $n-1$, for the prime divisor P ramifies completely in the extension K/K'. Therefore if $2(g-1)<n-1$, namely if $2g\leqq n$, g' must be zero. It follows that there exists a maximal subgroup V of order less than $2g$, such that its fixed field K'' has a genus different from zero.

9) A slightly finer consideration shows us that the condition 2) is not necessary in the present lemma.

The factor group H/V, considered as a group of automorphisms of K'', obviously satisfies all conditions of the previous lemma. The order of H/V is, consequently, at most p^2, and the order of H itself does not exceed $p^2(2g-1)$.

Finally we prove a purely group-theoretical lemma.

Lemma 5. *Let G be a finite or infinite group of order $\geqq n$, containing a central subgroup Z of order p, such that the factor group G/Z is an elementary abelian p-group*[10]. *Then G contains an abelian subgroup of order at least $\sqrt{pn}$.*

Proof. We may assume that G is a finite group, for otherwise, we may replace G by a suitable finite subgroup of order $\geqq n$. Let U be a maximal abelian normal subgroup of G. Z is then contained in U, and U/Z is an elementary abelian p-group. We select $\sigma_1, \ldots\ldots, \sigma_s$ in U, such that the cosets of σ_i modulo Z form a basis of U/Z. For an arbitrary σ in G, we then put

$$\sigma\sigma_i\sigma^{-1}\sigma_i^{-1}=\zeta_i \qquad i=1, \ldots\ldots, s.$$

As G/Z is abelian, $\zeta_i=\zeta_i(\sigma)$ is contained in Z, and we see easily that the mapping

$$\sigma\rightarrow(\zeta_1(\sigma), \ldots\ldots, \zeta_s(\sigma))$$

is a homomorphism from G into the direct product of s copies of Z. Moreover the kernel of this homomorphism coincides with U, for U is a maximal abelian normal subgroup of G. It follows that the order of G/U is at most p^s. On the other hand, the order of U is equal to p^{s+1}. We have, consequently,

$$n\leqq[G:e]=[G:U][U:e]\leqq p^s.\ p^{s+1},$$

$$\sqrt{pn}\leqq p^{s+1}=[U:e],$$

which proves our lemma.

We now return to the group $G(P)$ and show that the nilpotent normal subgroup N of $G(p)$ is a finite group. Let $x=x_{r-1}$ be the next to last element in the above chosen basis $x_1, \ldots\ldots, x_r$ or $L(P^{2g+1})$. Because of

---

10) A group is called an elementary abelian p-group, when it is abelian and the p-th power of any element of the group is the unit element.

the choice of our basis, x is an element in K, such that it has a denominator of the least possible positive power of P, say P^n, among all elements in K. From (5) we have

$$\sigma(x)=x+a_\sigma, \qquad a_\sigma\in k,$$

for any σ in N, and $\sigma\rightarrow a_\sigma$ gives a homomorphism from N into the additive group of k. Therefore, if we denote the kernel of this homomorphism by N_1, N/N_1 is an elementary abelian p-group. Moreover, as any σ in N_1 is a relative automophism of $K/k(x)$, the order of N_1 is at most $m=[K:k(x)]$. As N is nilpotent, we can find a subgroup N_2 of index p in N_1, such that it is normal in N and N_1/N_2 is contained in the center of N/N_2. Let K' be the fixed field of N_2. From the relation

$$p[K:K']=[N_1:N_2][N_2:e]=[N_1:e]\leqq[K:k(x)],$$

we see that the genus g' of K' is not zero, for othewise, K would contain a non-constant element whose denominator is a proper divisor of P^m. Since N/N_2 can be considered as a group of automorphisms of K', we see, from Lemma 4, that the order of any abelian subgroup of N/N_2 is at most $p^2(2g'-1)$. On the other hand, if we put $Z=N_1/N_2$, the group N/N_2 has the structure mentioned in Lemma 5. Therefore, if the order of N/N_2 is not less than n', it contains an abelian subgroup of order $\geqq\sqrt{pn'}$. It then follows that

$$\sqrt{pn'}\leqq p^2(2g'-1).$$

Consequently the order of N/N_2 is at most $p^3(2g'-1)^2$, and the order of N is not greater than $p^3(2g'-1)^2.\ mp^{-1}=p^2m(2g'-1)^2$. However, we know from (11) that

$$2(g-1)\geqq(m-1)+2m(g'-1),$$

or

$$2g-1\geqq m(2g'-1), \quad (2g-1)^2\geqq m(2g'-1)^2.$$

We have thus proved that the order of N is at most $p^2(2g-1)^2$ and obtained the following theorem[11].

11) An example in H. L. Schmid [4] shows that $p^2(2g-1)^2$ seems to be near to the best value of the bounds of the order of such N.

Theorem 1. *Let K be a function field of genus $g>0$ over an algebraically closed constant field k, and let P be an arbitrary prime divisor of K. Then the group $G(P)$ of all automorphisms of K which leave P fixed has the following structure:*

1) *if the characteristic of k is zero, $G(P)$ is a cyclic group of order $\leqq 6(2g-1)$.*

2) *if the characteriatic of k is a prime number p, a p-Sylowgroup N of $G(P)$ is a normal subroup of order $\leqq p^2(2g-1)^2$ and the factor group $G(P)/N$ is a cyclic group of order $\leqq 6(2g-1)$.*

In any case the order of $G(P)$ has a bound depending only upon g and p.

§ 3. Let us now assume that the genus g of K is greater than 1 and denote the set of all differentials of the first kind of K by D. As is well-known D is a g-dimensional linear space over k and any automorphism of K induces a linear transformation in D. Thus the group G of all automorphisms of K can be represented by such linear transformations in D.

Now take an aibitrary automorphism σ in G. We can then find a differential $\omega\neq 0$ in D, such that

$$\sigma(\omega)=a\omega, \qquad a\in k.$$

If follows that σ permutes the $2g-2$ zeros of ω among themselves, and some power of a, say a^l, where

$$l\leqq 2g-2,$$

leaves one of these zeros of ω, say P, fixed. σ^l is therefore contained in $G(P)$ and Theorem 1 then shows us that the order of σ has a bound, depending only upon g and p.

Let M be an irreducible invariant subspace of D with respects to the above representation of G, We denote by G_0 the kernel of the irreducible representation of G in M, so that G/G_0 is isomorphic to the irreducible group of linear transformations. However, we know that the orders of elements in G, a fortiori the orders of elements in G/G_0, are bounded. If follows then from a theorem of Burnside[12] that G/G_0 is a finite group.

Now take a differential $\omega\neq 0$ in M. Since $\sigma(\omega)=\omega$ for any σ in G_0, each such σ permutes the $2g-2$ zeros of ω among themselves. These zeros are not necessarily different from each other, but there exists at

12) Cf. Burnside [1]

least one such zero of ω by the assumption $g>1$. Therefore there exists a subgroup G_1 of G_0, such that the index $[G_0:G_1]$ is at most $(2g-2)$ and such that each σ in G_1 leaves a prime divisor P fixed. G_1 is thus contained in the finite group $G(P)$, and we see, finally, that the group G itself is a finite group.

We have thus proved the following

Theorem 2. *The group G of all automorphisms of a function field of genus $g>1$ over an algebraically closed field k, is always a finite group.*

From the above proof, we can also find a bound for the order of G, which depends only upon g and p, though it is much greater than the best value of such bounds in the case characteristic zero.

Bibliography

(1) Burnside, W. Theory of groups of finite order, 2nd. ed. Note J. p. 491—494.

(2) Hurwitz, A. Analytische Gebilde mit eindeutigen Transformationen in sich, Math. Ann, Bd. 41 (1893), p. 403—422 (Werke Be. I, p. 391—430).

(3) Pòincàrê, H. Sur un théorème de M. Fuchs, Acta Math, Bd. 7 (1885), p. 1—32.

(4) Schmid, H. L. Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik, Crelle's Jour. Bd. 179 (1938),p. 5—15.

(5) Schmidt, F. K. Zur arithmetische Theorie der algebraischen Funktionen. II. Allgemeine der Weierstrasspunkte, Math. Zeitschr., Bd. 45 (1939), p. 73—96.

(6) Weierstrass, K. Aus einem noch nicht veröffentlichten Briefe an Herrn Professor Schwarz, Werke Bd. II, p.235—244.