A REMARK ON HURWITZ GROUPS

A REMARK ON HURWITZ GROUPS

Takanori MATSUNO*

ABSTRACT

By a theorem of Hurwitz, a compact Riemann surface of genus $g \geqq 2$ cannot have more than $84(g-1)$ automorphisms [H]. It is known that the bound is attained for infinitely many values of g [Mac1]. In this short note, we show that the bound is often not sharp.

Key Words : Hurwitz group, Riemann surface, automorphism, branched covering

1. Introduction

Let X be a compact Riemann surface of genus $g \geqq 2$. We denote by $\mathrm{Aut}(X)$ the full automorphism group of X. By a theorem of Hurwitz, the order $|\mathrm{Aut}(X)|$ is finite and the following inequality holds [H]:

$$|\mathrm{Aut}(X)| \leqq 84(g-1).$$

We call $\mathrm{Aut}(X)$ as Hurwitz group if the bound is attained. It is known that the bound is attained for infinitely many values of g [Mac1]. The purpose of this short note is to show that the bound is often not sharp. We give our main theorem in the final section. Throughout this note, we often use the theory of branched coverings of complex manifolds [N].

2. Examples of Hurwitz groups

In this section, we give a few examples of Hurwitz groups using the method of the theory of branched coverigns of complex manifolds [N][M1][M2]. Let

$$\pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, q_0) = \langle \gamma_0, \gamma_1, \gamma_\infty \mid \gamma_\infty \gamma_1 \gamma_0 = 1 \rangle$$

be the fundamental group of $\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ with some reference point $q_0 \in \mathbf{P}^1(\mathbb{C})$. Here γ_0,γ_1 and γ_∞ are loops once rounding counterclockwise direction around 0, 1 and ∞, respectively.

Example 1. Consider the permutations:

$$\begin{aligned} A_1 &= (1\,5)(2\,3) \\ B_1 &= (1\,6\,7)(2\,4\,5) \\ A_1 B_1 &= (1\,2\,3\,4\,5\,6\,7). \end{aligned}$$

They generate the simple group, say G_1, of order 168 and $G_1 \cong \mathrm{PSL}(2,7)$. (For the computation, we use the "GAP".)

(Received August 23, 2016)

* Dept. of Industrial Systems Engineering : Natural Science

Let $\Phi_1 : \pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, x_0) \to G_1$ be a surjective group homomorphism defined by:

$$\Phi_1(\gamma_0) = A_1^{-1}, \Phi_1(\gamma_1) = B_1^{-1}, \Phi_1(\gamma_\infty) = A_1 B_1.$$

Then there exists an unbranched Galois covering

$$f_1^0 : X_1^0 \to \mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$$

corresponding to $\mathrm{Ker}\Phi_1$. This f_1^0 extends to a Galois branched covering $f_1 : X_1 \to \mathbf{P}^1(\mathbb{C})$ of type $(2, 3, 7)$. From the Riemann-Hurwitz formula, the genus of X_1 is 3 and the Hurwitz bound is attained. X_1 is known as the Klein's quartic curve [K].

Example 2. Consider the permutations:

$$\begin{aligned} A_2 &= (1\,8)(2\,7)(4\,6)(5\,9) \\ B_2 &= (1\,8\,2)(3\,4\,7)(5\,9\,6) \\ A_2 B_2 &= (1\,2\,3\,4\,5\,6\,7). \end{aligned}$$

They generate the simple group, say G_2, of order 504 and $G_2 \cong \mathrm{PSL}(2,8)$. (For the computation, we use again the "GAP".) Let $\Phi_2 : \pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, x_0) \to G_2$ be a surjective group homomorphism defined by:

$$\Phi_2(\gamma_0) = A_2^{-1}, \Phi_2(\gamma_1) = B_2^{-1}, \Phi_2(\gamma_\infty) = A_2 B_2.$$

Then there exists an unbranched Galois covering

$$f_2^0 : X_2^0 \to \mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$$

corresponding to $\mathrm{Ker}\Phi_2$. This f_2^0 extends to a Galois branched covering $f_2 : X_2 \to \mathbf{P}^1(\mathbb{C})$ of type $(2, 3, 7)$. From the Riemann-Hurwitz formula, the genus of X_2 is 7 and the Hurwitz bound is attained. X_2 is known as the Macbeath's curve [Mac2].

Example 3. Consider the permutations:

$$\begin{aligned} A_3 &= (1\,15)(2\,7)(3\,8)(4\,13)(5\,11)(6\,9) \\ B_3 &= (1\,15\,2)(3\,9\,7)(4\,14\,8)(5\,12\,13)(6\,10\,11) \\ A_3B_3 &= (1\,2\,3\,4\,5\,6\,7)(8\,9\,10\,11\,12\,13\,14). \end{aligned}$$

They generate the simple group, say G_3, of order 653837184000 and $G_3 \cong \mathrm{A}_{15}$. (For the computation, we use again the "GAP".) Let $\Phi_3 : \pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, x_0) \to G_3$ be a surjective group homomorphism defined by:

$$\Phi_3(\gamma_0) = A_3^{-1}, \Phi_3(\gamma_1) = B_3^{-1}, \Phi_3(\gamma_\infty) = A_3B_3.$$

Then there exists an unbranched Galois covering

$$f_3^0 : X_3^0 \to \mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$$

corresponding to $\mathrm{Ker}\Phi_3$. This f_3^0 extends to a Galois branched covering $f_3 : X_3 \to \mathbf{P}^1(\mathbb{C})$ of type $(2, 3, 7)$. From the Riemann-Hurwitz formula, the genus of X_3 is 7783776001 and the Hurwitz bound is attained.

3. Macbeath's theorem

In this section, we discuss Macbeath's theorem from a theoretic ponit of view of branched coverings of complex manifolds. Let X be a compact Riemann surface of genus $g_1 \geqq 2$ and let $\pi : X \to \mathbf{P}^1(\mathbb{C})$ be a Galois branched covering of type $(2, 3, 7)$. Then the degree of π is $84(g_1 - 1)$ and the following equality holds:

$$|\mathrm{Aut}(X)| = 84(g_1 - 1).$$

We may assume the number of branching poits of π over 0,1 and ∞ are $42(g_1 - 1)$, $28(g_1 - 1)$ and $12(g_1 - 1)$, respectively. Let $t = 82(g_1 - 1)$ be the total number of such branching points in X. Let $P_j \in X$ $(j = 1, \cdots, t)$ be the branching points in X. Let $\Pi_1^0 = \pi_1(X \setminus \{P_1, \cdots, P_t\}, x_0)$ be the fundamental group of $X \setminus \{P_1, \cdots, P_t\}$. Let δ_j be the loop in X once rounding counterclockwise direction around P_j $(j = 1, \cdots, t)$. Let J be the smallest normal sbugroup in Π_1^0 which contains $\{\delta_1, \cdots, \delta_t\}$. Let $\Pi_1 = \pi_1(X, x_0)$ be the fundamental group of X. There exists a natural injection $\iota : X \setminus \{P_1, \cdots, P_t\} \to X$ and ι induces the group homomorphism $\iota_* : \Pi_1^0 \to \Pi_1$. From van Kampen theorem, we have a following exact sequence:

$$1 \to J \to \Pi_1^0 \xrightarrow{\iota_*} \Pi_1 \to 1.$$

Let m be a positive integer and let $\left(\Pi_1^0\right)^m$ (resp. $(\Pi_1)^m$) be the Burnside m-kernel generated by mth power of all elements of Π_1^0 (resp. of Π_1). Let $\left[\Pi_1^0, \Pi_1^0\right]$ (resp. $[\Pi_1, \Pi_1]$) be the commutator subgroup of Π_1^0 (resp. of Π_1). Furthermore we take the products

$$N^0 = \left(\Pi_1^0\right)^m \left[\Pi_1^0, \Pi_1^0\right] \subset \Pi_1^0$$

and

$$N = (\Pi_1)^m [\Pi_1, \Pi_1] \subset \Pi_1.$$

Obviously N^0 and N are characteristic subgroups of Π_1^0 and of Π_1, respectively. There is a exact sequence:

$$1 \to N \to \Pi_1 \xrightarrow{\tau} \Pi_1/N \to 1,$$

where τ is a quotient mapping . It is known that Π_1/N is isomorphic to the direct sum of $2g_1$ copies of the cyclic group $\mathbb{Z}/m\mathbb{Z}$ of order m:

$$\Pi_1/N \cong \mathbb{Z}/m\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m\mathbb{Z}.$$

The order $|\mathbb{Z}/m\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m\mathbb{Z}|$ is equal to m^{2g_1}. It is easy to see that $\iota_* : N^0 \to N \to 1$ is exact. Let K^0 be the kernel of the composition $\tau \circ i_* : \Pi_1^0 \to \Pi_1/N$. Obviously, K^0 is a smallest normal subgroup, of Π_1^0, which contains J and N^0. Through the inclusions,

$$K^0 \to \Pi_1^0 \xrightarrow{\pi_*} \pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, q_0),$$

K^0 can be considered as the subgroup of $\pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, q_0)$. It is easy to see that the image of J is the smallest normal subgroup, of $\pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, q_0)$, which contains $\{\gamma_0^2, \gamma_1^3, \gamma_\infty^7\}$. Furthermore, since N^0 is a characteristic subgroup of Π_1^0 and Π_1^0 is a normal subgroup of $\pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, q_0)$, The image of N^0 is also a normal subgroup of $\pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, q_0)$. Thus the image of K^0 is a normal subgroup of $\pi_1(\mathbf{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, q_0)$. Then there exist Galois coverings $\nu^0 : Y^0 \to X \setminus \{P_1, \cdots, P_t\}$ and $\mu^0 : Y^0 \to \mathbf{P}^1(\mathbb{C} \setminus \{0, 1, \infty\}, q_0)$ corespoding to K^0 and we have the following commutative diagram (See Figure 1.):

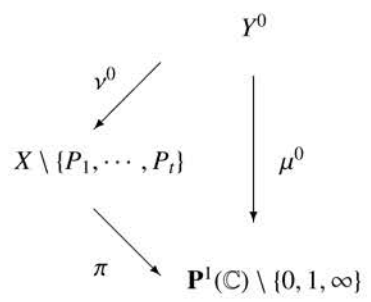

Figure 1.

ν^0 and μ^0 can be extended to Galois branched coverings $\nu : Y \to X$ and $\mu : Y \to \mathbf{P}^1(\mathbb{C})$, respectively. Since $J \subset K^0$, ν is unbranched. So μ is a Galois branched covering of type (2, 3, 7) of $\mathbf{P}^1(\mathbb{C})$. The order of μ is $84(g_1-1)m^{2g_1}$. Let g be the genus of Y. From the Riemann-Hurwitz formula, $g = (g_1-1)m^{2g_1}+1$ and we have $|\mathrm{Aut}(Y)| = 84(g-1)$. Since m is arbitrary positive integer, thus this equality holds for infinitely many values of g [Mac1].

4. Sylow's theorem

Let G be a finite group and p be a prime. Any subgroup whose order is the highest power of p dividing the order $|G|$ is called a p-Sylow subgroup of G. In this section we recall several facts about p-Sylow subgroups, the Sylow theorems, which we will use to prove our main theorem in the next section. These theorems are well-known and the proofs are omitted.

Theorem 1. *Let G be a finite group and p be a prime such that p^k is a divisor of $|G|$. Then, G contains a subgroup of order p^k.*

Theorem 2. *Let G be a finite group and p be a prime such that p is a divisor of $|G|$. Then, all p-Sylow subgroups are conjugate in G.*

Theorem 3. *Let G be a finite group and p be a prime. Let $|G| = p^k m$ with $gcd(m, p) = 1$ and let t be the number of p-Sylow subgroups in G. Then, t is a divisor of $|G|$ and $t \equiv 1 \pmod{p}$.*

5. Main theorem

In this section, we give our main theorem :

Theorem 4. *Let $p_1, \cdots, p_s$ be mutually distinct s prime numbers and let $n_1, \cdots, n_s$ be s positive integers which satisfy the conditions:*

(1) $84 < p_1$,

(2) $84p_1^{n_1}\cdots p_{j-1}^{n_{j-1}} < p_j \quad (j = 2, \cdots, s)$.

Then, if X is a compact Riemann surface of genus $g = p_1^{n_1}\cdots p_s^{n_s} + 1$, the order of $\mathrm{Aut}(X)$ *is strictly less than* $84(g-1)$.

To prove Theorem 4, we need to prepare the following lemma:

Lemma 1. *Let X be a compact Riemann surface of genus $g_X \geqq 2$. Then X does not have any automorphism whose order is a prime number and is greater than $2g_X + 1$.*

Proof of Lemma 1. Suppose that X has an automorphism, say σ whose order is a prime number, say p, with $p > 2g_X + 1$. Then σ generates a cyclic subgroup $H = <\sigma>$ of order p in $\mathrm{Aut}(X)$. We now consider the quotient space $Z = X/H$. The quotient mapping $\gamma : X \to Z = X/H$ is a cyclic branched covering over Z of degree p. γ may branch at several points. Let l be the number of the branching points of γ in X and let g_Z be the genus of Z. From the Riemann-Hurwitz formula, we have

$$2g_X - 2 = p(2g_Z - 2) + l(p-1).$$

If we reduce mod $p-1$, we have

$$2g_X - 2 \equiv 2g_Z - 2 \pmod{p-1}.$$

So as a result, the following congruence equality must hold:

$$2(g_X - g_Z) \equiv 0 \pmod{p-1}.$$

But it is impossible, since

$$0 < 2(g_X - g_Z) \leqq 2g_X < p - 1.$$

Then X cannot have any automorphism whose order is a prime p with $p > 2g_X + 1$.

Proof of Theorem 4. To prove Theorem 4, we use a induction with s. We first prove the case $s = 1$. So now we discuss about the case that p_1 is a prime number with $84 < p_1$ and $g = p_1^{n_1} + 1$. Suppose $|\mathrm{Aut}(X)| = 84(g-1)$, then $|\mathrm{Aut}(X)| = 84p_1^{n_1}$. There exist p_1-Sylow subgroups in $\mathrm{Aut}(X)$ by thorem 1. From Theorem 3, the number of p_1-Sylow subgroups is $kp_1 + 1$ for some non-negative integer k and $kp_1 + 1$ is a divisor of $84p_1^{n_1}$. It is obvious that $kp_1 + 1$ and p_1 canonot have any common divisors except 1. So $kp_1 + 1$ must divide 84. Because of the assumption $84 < p_1$, we have $k = 0$. So $\mathrm{Aut}(X)$ contains the uniqe p_1-Sylow subgroup, say P, of order $p_1^{n_1}$. From Theorem 2, P is a characteristic normal subgroup in $\mathrm{Aut}(X)$. We now consider the quotient space $Y = X/P$ and the commutative diagram (See Figure 2.):

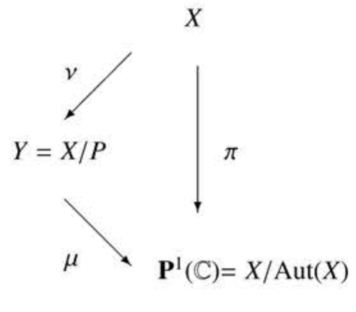

Figure 2.

The quotient mapping $\pi : X \to X/\mathrm{Aut}(X) = \mathbf{P}^1(\mathbb{C})$ is a Galois branched covering of $\mathbf{P}^1(\mathbb{C})$ which branches at three points and is of type $(2, 3, 7)$. The degree of π is

$84p_1^{n_1}$. The quotient mapping $\nu : X \to X/P$ is a Galois branced covering whose degree is $p_1^{n_1}$. Since P is a normal subgroup in Aut(X), $\mu : Y \to \mathbf{P}^1(\mathbb{C})$ is also a Galois branched covering. Since every ramification indices of π, 2,3 and 7, are prime numbers and from the fact that there exists no Galois covering of $\mathbf{P}^1(\mathbb{C})$ which branches at one point nor at two points with different ramification indices, either ν or μ is an unbranched covering. If μ is unbranched, μ is a biholomorphic mapping since $\mathbf{P}^1(\mathbb{C})$ is simply connected. So, ν is unbranched and μ is a Galois branched covering of $\mathbf{P}^1(\mathbb{C})$ which branches at three points and is of type $(2, 3, 7)$ and the order of μ is equal to 84 and the gunus of Y is equal to 2 from the Riemann-Hurwitz formula. Since $|\mathrm{Aut}(Y)| = |\mathrm{Aut}(\mu)| = 84$, Y must have an automorphism of order 7. But, from Lemma 1, Y cannot have an automorphism of order 7. It is a contradiction. So we have proved the case $s = 1$.

Next we assume that Theorem 4 is true for $s - 1$ prime numbers which satisfy the conditions. So if Y is a compact Riemann surface of genus $g_Y = p_1^{n_1} \cdots p_{s-1}^{n_{s-1}} + 1$, then the order of Aut($Y$) is strictly less than $84(g_Y - 1)$.

Finally assume the converse of Theorem 4 for s prime numbers, i.e. there exists a compact Riemann surface X of genus $g = p_1^{n_1} \cdots p_{s-1}^{n_{s-1}} p_s^{n_s} + 1$ such that $|\mathrm{Aut}(X)| = 84(g - 1)$ holds. Then the quotient mapping $\pi : X \to X/\mathrm{Aut}(X) = \mathbf{P}^1(\mathbb{C})$ is a Galois branched covering of $\mathbf{P}^1(\mathbb{C})$ which branches at three points and is of type $(2, 3, 7)$. The degree of π is $84p_1^{n_1} \cdots p_s^{n_s}$. By Theorem 3, the number of p_s-Sylow subgroups in Aut(X) is $kp_s + 1$ for some non-negative integer k and $kp_s + 1$ is a divisor of $84p_1^{n_1} \cdots p_{s-1}^{n_{s-1}} p_s^{n_s}$. It is obvious that $kp_s + 1$ and p_s canonot have any common divisors except 1. So $kp_s + 1$ must divide $84p_1^{n_1} \cdots p_{s-1}^{n_{s-1}}$. Because of the assumption $84p_1^{n_1} \cdots p_{s-1}^{n_{s-1}} < p_s$, we have $k = 0$. So Aut(X) contains the uniqe p_s-Sylow subgroup, say Q, of order $p_s^{n_s}$. From Theorem 2, Q is a characteristic normal subgroup in Aut(X). Then we have the following diagram (See Figure 3.):

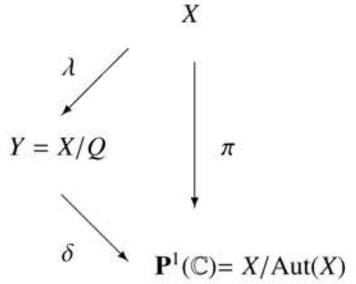

Figure 3.

The quotient mapping $\lambda : X \to X/Q$ is a Galois covering whose degree is $p_s^{n_s}$ and λ is unbranched from the similar argument in the case $s = 1$. So $\delta : Y \to \mathbf{P}^1(\mathbb{C})$ is also a Galois branched covering of $\mathbf{P}^1(\mathbb{C})$ which branches at three points and is of type $(2, 3, 7)$. The degree of δ is equal to $84p_1^{n_1} \cdots p_{s-1}^{n_{s-1}}$. Let g_Y be the genus of Y. Since δ is also of type $(2, 3, 7)$, we have $|\mathrm{Aut}(Y)| = 84(g_Y - 1)$ and $g_Y = p_1^{n_1} \cdots p_{s-1}^{n_{s-1}} + 1$, which contradicts our assumption for $s - 1$ prime numbers. Then the proof is completed.

Remark 1. The case $s = 1$ and $n_1 = 1$ of Theorem 4 is given in [M].

Remark 2. From the similar argument in the proof of Theorem 4, if Aut(X) is a Hurwitz group and is not simple, i.e. Aut(X) has a nontrivial normal subgroup, say N, then the automorphism group of the quotient Aut(X/N) is also a Hurwitz group [M2].

References

[H] A. Hurwitz : *Über algebraishe Gebilde mit eindeutigen Transformationen in sich*, Math. Annalen 41(1893), 403-442.

[K] F. Klein : *Ueber die Transformationen siebenter Ordnung der elliptischen Funktionen*, Math. Annalen 14(1879), 428-471.

[Mac1] A.M. Macbeath : *On a theorem of Hurwitz*, Proc. Glasgow. Math. Assoc. 5 (1961), 90-96.

[Mac2] A.M. Macbeath : *On a curve of genus 7*, Proc. London. Math. Soc.(3)15 (1965), 527-542.

[M] A. Mathew : *Automorphisms of compact Riemann surfaces*, (2011), unpublished paper.

[M1] T. Matsuno : *On a theorem of Zariski-van Kampen type and its applications*, Osaka J. Math. 32 (1995)no.3, 645–658.

[M2] T. Matsuno : *Compact Riemann surfaces with large automorphism groups*, J. Math. Soc. Japan 51 (1999) no.2, 309-329.

[N] M. Namba : *Branched coverings and algebraic functions*, Pitman Research Note in Math. , Ser. 161, Longman Scientific & Technical, 1987.