TRANSITIVE EXTENSIONS OF A CLASS OF DOUBLY TRANSITIVE GROUPS

MICHIO SUZUKI*

To the memory of Professor TADASI NAKAYAMA

1. When a permutation group G on a set Ω is given, a transitive extension G_1 of G is defined to be a transitive permutation group on the set Γ which is a union of Ω and a new point ∞ such that the stabilizer of ∞ in G_1 is isomorphic to G as a permutation group on Ω. The purpose of this paper is to prove that many known simple groups which can be represented as doubly transitive groups admit no transitive extension. Precise statement is found in Theorem 2. For example, the simple groups discovered by Ree [5] do not admit transitive extensions. Theorem 2 includes also a recent result of D. R. Hughes [3] which states that the unitary group $U_3(q)$ $q > 2$ does not admit a transitive extension. As an application we prove a recent theorem of H. Nagao [4], which generalizes a theorem of Wielandt on the non-existence of 8-transitive permutation groups not containing the alternating groups under Schreier's conjecture.

2. We will introduce notation which will be used throughout this paper.

Let G be a doubly transitive group on Ω and let H be the stabilizer of a point a of Ω. Suppose that a conjugate class C of G consisting of elements of order 2 is given. Then there is an element s of C such that we have a decomposition of G into a union of two double cosets:

$$G = H \cup HsH \text{ where } s \in C.$$

We define

$$D = H \cap H^s,$$

and remark that s normalizes D.

For a transitive extension, a theorem of E. Witt is fundamental (Witt [10]), which will be stated here as Lemma 1.

LEMMA 1. *Suppose that G admits a transitive extension. Then the extended group G_1 is generated by G and an element t satisfying the following properties:*

$$G_1 = \langle G, t \rangle, \qquad H^t = H, \qquad D^t = D,$$

$(st)^3 \in D$ *and t is conjugate to s in G_1.*

Proof. Since G_1 is triply transitive, G_1 contains an element t such that t exchanges ∞ and a, and leaves $s(a)$ invariant. Then t satisfies all the requirements except possibly the last. The group $N = \langle D, s, t \rangle$ normalizes D and N/D is the non-abelian group of order 6. Hence two groups $\langle D, s \rangle$ and $\langle D, t \rangle$ are conjugate. So there is an element t_1 in $\langle D, t \rangle - D$ which is conjugate to s. The element t_1 meets all the requirements.

We need two lemmas from group theory.

LEMMA 2. *If a finite group G admits an involutive automorphism t which satisfies the property*:

$$x^t = x \ \ implies \ \ x = 1,$$

then G is abelian and $x^t = x^{-1}$ for all x in G.

LEMMA 3. *Suppose that a 2-group G contains an element u of order 2 such that $|G_0(u)| = 4$. Then G contains a cyclic subgroup of index 2, and is generated by two elements u and v satisfying the following relations:*

$$v^{2n} = u^2 = 1, \qquad u^{-1}vu = v^k$$

where $|G| = 4n$ and $k = -1$ or $k = -1 + n$.

The first is a lemma of Burnside [1], while the second is in [6]. The two possible groups in Lemma 3 are dihedral if $k = -1$ and semi-dihedral otherwise.

3. The following theorem is a partial statement of a more complete result, but is sufficient in many applications.

THEOREM 1. *Let G be a transitive permutation group on Ω and H the stabilizer of a point a of Ω. Suppose that H contains a normal subgroup Q satisfying the following conditions:*

(1) *Q is regular on $\Omega - \{a\}$;*

(2) *Q is a characteristic subgroup of H;*

(3) *the order $|Q|$ of Q is a power of a prime number p.*

If G admits a transitive extension, then we have one of the following two cases:

(a) *$p = 2$ and Q contains a cyclic normal subgroup of index 2,*

(b) *$p > 2$ and Q is abelian.*

Proof. Suppose that G has a transitive extension G_1. Let C be a conjugate class of G containing an element of order 2. We shall choose C in various ways. Let s be an element of C not contained in H.

By assumption (1), G is doubly transitive. Hence

$$G = H \cup HsQ.$$

By Lemma 1, there is an element t of G_1 such that

$$G_1 = \langle G, t \rangle, \ H^t = H, \ (st)^3 \in D = H \cap H^s$$

and t is conjugate to s in G_1. Then we have

$$G_1 = G \cup Gt \cup GtsQ$$

and $Gtsu = Gtsv$ for $u, v \in Q$ implies $u = v$. Since Q is a characteristic subgroup of H, t normalizes Q. Hence

$$Gtsut = Gtstu^t = Gstsu^t = Gtsu^t.$$

For any element x of G_1 let $i(x)$ denote the number of points of $\varOmega \cup \{\infty\}$ left invariant by x. Then the above formula yields that

$$i(t) = |C_Q(t)|.$$

We distinguish two cases according as $p = 2$ or $p > 2$. Suppose first $p = 2$. Then Q contains an element j of order 2. In this case we take C to be the class containing j. Since j leaves exactly one point on $\varOmega$, we have $i(j) = 2$. Since j and t are conjugate,

$$2 = i(j) = i(t) = |C_Q(t)|.$$

The group $Q_1 = \langle Q, t \rangle$ is a 2-group. Hence by Lemma 3, Q_1, and hence Q, contains a cyclic subgroup of index 2. Thus we have proved (a).

Suppose that $p > 2$. If the group H is of odd order, then any element of order 2 in G, in particular, s has no fixed point on $\varOmega$. Hence we have

$$1 = i(s) = i(t) = |C_Q(t)|.$$

Therefore by Lemma 2, Q is abelian. If on the other hand H is of even order, the subgroup $D = H \cap H^s$ contains an element k of order 2. Since k normalizes Q and ts normalizes D, we have

$$Gtsuk = Gtsu^k.$$

Hence $i(k) = 2 + |C_Q(k)|$. This yields that, taking for C the class of k,

$$|C_Q(t)| = 2 + |C_Q(k)|.$$

Since Q is a p-group, both $|C_Q(t)|$ and $|C_Q(k)|$ are powers of the odd prime p. The above equality yields that

$$|C_Q(k)| = 1.$$

Again by Lemma 2, Q is abelian.

4. Application. Let S be one of the following groups: the two-dimensional linear fractional groups $L_2(q)$, the three-dimensional unitary groups $U_3(q)$, the groups $S_z(q)$ defined in [7] or the Ree groups $R(q)$ defined in [5] as a subgroup of the group of type G_2. Here the number q is a power of a prime number p. In the first two cases p may be arbitrary but $p = 2$ for $S_z(q)$ and $p = 3$ for $R(q)$. Except $L_2(2)$, $L_2(3)$, $U_3(2)$, $S_z(2)$ and $R(3)$, these groups are simple. In any case the center of S is trivial. S acts naturally on the set of all the Sylow p-groups by conjugation and this representation of S is faithful. The stabilizer of a Sylow p-group Q is the normalizer of Q. The groups in the particular class considered above have the property that Q is regular on the set of Sylow p-groups $\neq Q$. This is equivalent to the properties that

$$Q \cap Q^x = \{1\} \text{ if } Q^x \neq Q,$$

and the number of Sylow p-groups is exactly $1 + |Q|$.

Let $\text{Aut } S$ be the totality of automorphisms of S. We consider S as a subgroup of $\text{Aut } S$ by identifying S and the totality of inner automorphisms. Consider any group G such that

$$\text{Aut } S \supseteq G \supseteq S,$$

and regard G as a permutation group acting on the set of all the Sylow p-groups of S. This representation of G is faithful because the centralizer of S in $\text{Aut } S$ is trivial. We prove the following lemma.

LEMMA 4. *Let $H = N_G(Q)$. Then Q is a characteristic subgroup of H.*

Proof. Since Aut S is known for each S we are considering, this lemma can be checked. We can also show the validity as follows. If Q is not the maximal normal p-group of H, then the group $D = H \cap H^s$ contains a normal p-subgroup $P \neq \{1\}$. Put $H_1 = H \cap S$ and $D_1 = D \cap S$. Since D_1 is a p'-group, we have $[P, D_1] = 1$. We may take the element s in $N_S(D_1)$, so that $N_S(D_1) = \langle D_1, s \rangle$. P normalizes $N_S(D_1)$. Since there are as many elements in $N_S(D_1) - D_1$ as in D_1, P must centralize $N_S(D_1)$, in particular $s \in C_S(P)$. It is easy to see that

$$|C_S(P)| = r(r+1) \cdot |D_1| \text{ with } r = |C_Q(P)|.$$

Since $[D_1, P] = 1$, D_1 normalizes $C_Q(P)$. Since P is a p-group, $C_Q(P) \neq \{1\}$. This yields that $C_Q(P) = Q$ for $S = L_2(q)$, because Q is the only non-trivial D_1-subgroup of Q.

If $S = U_3(q)$, the center $Z(Q)$ is the only proper D_1-subgroup. P centralizes $Q/Z(Q)$ and $Z(Q)$. If x is a fixed element of P, then for any element u of Q we have $u^x = uv$ with $v \in Z(Q)$. The mapping $u \to v$ is a homomorphism of Q into $Z(Q)$. Hence $C_Q(x)$ has index less than $|Z(Q)|$, which is q. Since $|Q| = q^3$, and since $C_Q(x)$ is a D_1-subgroup, we have $C_Q(x) = Q$ and so $C_Q(P) = Q$.

If $S = S_z(q)$, $Z(Q)$ is the only proper D_1-subgroup. Hence $r \geqq q$. Then $r + 1$ must divide $|S|/|D_1| = q^2(q^2 + 1)$. This yields that $r = q^2$ and $C_Q(P) = Q$.

If $S = R(q)$, $|Q| = q^3$ and there is a characteristic subgroup Q_1 of order q^2 which is a direct product of $Z(Q)$ and a D_1-subgroup Q_2. In $R(q)$, D_1 is a group of order $q - 1$ and contains a unique element j of order 2. The subgroup Q_2 is in fact $C_Q(j)$. Hence Q_2 is P-invariant. Since $Z(Q)$ and Q_2 are minimal D_1-subgroup, both are centralized by P. Hence we have $r \geqq q^2$. Again $r + 1$ must divide $q^3 + 1$ since $|S| = q^3(q^3 + 1)(q - 1)$. This yields that $r = q^3$.

In all cases P centralizes Q. Since $S = \{Q, s\}$, P centralizes S. This is a contradiction because the centralizer of S in Aut S is trivial.

The main theorem of this paper is the following.

THEOREM 2. *Let G be a permutation group defined above, so that Aut $S \supseteq G \supseteq S$ where S is $U_3(q)$, $S_z(q)$ or $R(q)$. Then G does not admit a transitive extension except when $S = U_3(2)$ and $S_z(2)$.*

Proof. By definition and by Lemma 4 G satisfies all the conditions of Theorem 1. Hence we have either (a) or (b). But Q is non-abelian except the group $S_z(2)$. Therefore we must have (a). If q is a power of 2, the 2-group Q is of exponent 4. Hence we must have $|Q| \leqq 8$ and $q = 2$. In both exceptional cases transitive extensions are easy to determine.

Remarks. (1) A similar theorem is true for $S = L_2(q)$ as is well-known. Not all statements of Theorem 2 are new. Hughes has shown that $U_3(q)$ and $S_z(q)$ with $q > 2$ does not admit an extension. He has published the result for $S_z(q)$ in [2] and the result for $U_3(q)$ is to appear [3]. The author is grateful to Professor Hughes for communicating his result before publication.

(2) Among the simple groups known so far the alternating groups, the Mathieu groups, the linear fractional groups $L_n(q)$ and the groups discussed in Theorem 2 have doubly transitive representations. For other simple groups it is not known whether they have doubly transitive presentations, and it has been believed they do not.

5. The method used in the section 3 can be refined to give a more complete result. It has been conjectured that the class of doubly transitive groups which satisfy the assumptions of Theorem 1 coincides with the class of groups G satisfying Aut $S \supseteq G \supseteq S$ for simple groups discussed in the preceeding section. However, since the conjecture has been verified so far only in the case when Q contains a Sylow 2-group of G [8], we will give a refinement here. Throughout this section we use the notation and results obtained in the section 3.

If G contains a regular normal subgroup R, then the group $N = RQ$ is a normal subgroup of G which is a doubly transitive Frobenius group. Therefore G is a group of semi-linear transformations $y = ax^\sigma + b$ over a near field F. We remark that the condition (3) limits the structure of F to the following possibilities: $F = GF(2^n)$, $2^n - 1 =$ a Mersenne prime; $F = GF(p)$ for a Fermat prime p or F is a near field of 9 elements.

THEOREM 3. *Let G be a transitive permutation group satisfying the conditions of Theorem 1. Suppose that G does not contain any regular normal subgroup. Then G admits no transitive extension except possibly $|Q| = 3, 4, 8$ and 9.*

Proof. Suppose that G has a transitive extension G_1. We distinguish two cases according as $p = 2$ or $p > 2$, and consider first the case $p = 2$.

As shown in the section 3, the group $Q_1 = \langle Q, t \rangle$ is either dihedral or semi-dihedral. Hence Q contains a characteristic subgroups of all possible order if $|Q| > 8$. Hence if $|Q| > 8$, Aut Q is a 2-group. Assume that this is the case. Since $C_G(Q) \subseteq Q$ by the condition (1), D is a 2-group as $D \subseteq$ Aut Q. By assumption $D \neq \{1\}$.

Let k be an element of order 2 in D. Then by Lemma 1, there is an element t_1 in the extended group G_1 such that t_1 satisfies the properties in Lemma 1 and is conjugate to k. Then

$$|C_Q(t_1)| = 2 + |C_Q(k)|,$$

which yields that $|C_Q(k)| = 2$. Q contains a characteristic cyclic group of order 4. The element k inverts a generator of this subgroup of order 4. Since k is arbitrary, we conclude that k is the unique element of order 2 in D. Hence in particular k commutes with s.

It follows that

$$C_G(k) = C_H(k) \cup C_H(k)sC_Q(k) \text{ and } C_H(k) = C_Q(k)D.$$

Since $|C_Q(k)| = 2$, we have $|C_G(k)/D| = 6$. We count the number of elements of order 2 in $C_G(k)$ and find that there are exactly 7 elements of order 2 in $C_G(k)$.

The element k leaves exactly 4 points. Hence k has exactly $(|Q| - 2)/2$ transpositions. If b is a point such that $c = k(b) \neq b$, there is a unique element u of order 2 which leaves ∞, b and c invariant. Since $k^{-1}uk$ fixes ∞, b and c, we obtain $k^{-1}uk = u$. Hence $u \in C_G(k)$ and $C_G(k)$ contains at least $|Q|/2 - 1$ elements of order 2 besides k. Hence

$$|Q|/2 \leqq 7 \text{ or } |Q| \leqq 8$$

since $|Q|$ is a power of 2.

Assume next $p > 2$ and assume that the group H is of odd order. Then t inverts every element of Q. If $x \in D$, then the commutator $[t, x]$ is an element of D by Lemma 1 and $[t, x] \in C_D(Q)$. Hence we obtain $[t, x] = 1$. The element st acts on D in the same way as s. The element $d = (st)^3$ belongs to D and is inverted by s. Hence we have $d = d^{-1}$. Since D is of odd order, $d = 1$ or $(st)^3 = 1$. Since d and s induces the same automorphism in D, s commutes with every element of D.

Let u be an element $\neq 1$ of Q. Then

$$sus = vhsw \text{ where } v, w \in Q \text{ and } h \in D.$$

The elements v, w and h are determined uniquely by u. We claim $h = 1$ for all $u \neq 1$ of Q. Transform the above equality by t and use $(ts)^3 = 1$. Then

$$
\begin{aligned}
v^{-1}hstsw^{-1} &= stsu^{-1}sts \\
&= st(w^{-1}sh^{-1}v^{-1})ts \\
&= swstsh^{-1}vs \\
&= h^{-1}v^{-1}suh^{-1}tusw^{-1}h^{-1} \\
&= h^{-1}v^{-1}suh^{-1}u^{-1}h^{-1}tshw^{-1}h^{-1}.
\end{aligned}
$$

Since $H = G \cap G^t$, we have

$$sw^{-1}hwh^{-1}s \in H \text{ or } w^{-1}hwh^{-1} \in H \cap H^s = D.$$

But $w^{-1}hwh^{-1} \in Q$ so that w commutes with h. We obtain therefore

$$svhv^{-1}hs = uh^{-1}u^{-1}h^{-1} \in H \cap H^s = D.$$

Hence both u and v commute with h and $h^4 = 1$. Since D is of odd order, we obtain $h = 1$ as claimed.

Since $sus = vsw$ with $v, w \in Q$, the set

$$N = Q \cup QsQ$$

is a subgroup of G. Since D normalizes Q and centralizes s, D normalizes N. This implies that N is a normal subgroup of G. Since N is a doubly transitive Frobenius group, G contains a regular normal subgroup. This is not the case.

Assume finally that $p > 2$ and D is of even order. Let k be an element of order 2 in D. Then we have

$$|C_Q(t)| = 3 \text{ and } |C_Q(k)| = 1,$$

where t is conjugate to k. Hence k inverts every element of Q. Since k is an arbitrary element of order 2, we conclude that k is the unique element of order 2 of D. Suppose that $|Q| > 3$. Then $Q = Q_1 \times Q_2$ where $Q_1 = C_Q(t)$ and t inverts every element of Q_2. Clearly kt is an element of order 2 and commutes with every element of Q_2. Since $|Q_2| > 1$, kt is conjugate to k in G_1. Hence we have $|Q_2| = 3$. This proves that $|Q| = 3$ or 9.

6. Exceptional cases and further applications. It is easy to discuss the

exceptional cases in Theorem 3.   We just list the groups which satisfy the conditions of Theorem 1 and admit transitive extensions.   We denote by $\mathfrak{A}_n$ and $\mathfrak{S}_n$ the alternating and symmetric group on n letters respectively.   For a finite near field F_q of q elements, let $L(F_q)$ denote the group of all the linear transformations $y = ax + b$ with a, $b \in F_q$, $L^0(F_q)$ the group of all the semi-linear transformations $y = ax^\sigma + b$, $PGL_2(F_q)$ the group of all linear fractional transformations, and finally $P\Gamma L_2(F_q)$ the group of all semi-linear fractional transformations.

THEOREM 4.   *The groups which satisfy the assumptions of Theorem 1 and admit transitive extensions are* $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$, $\mathfrak{S}_5$, $L(F_p)$ *for Fermat primes* p, $L(F_9)$, $L^0(F_9)$ *for the field* F_9, $L(F_q)$ *and* $L^0(F_q)$ *for* $q = 2^n$ *such that* $2^n - 1 = p$ *are Mersenne primes, and* $PGL_2(F_9)$ *with the non-commutative* F_9.
The extended group is unique in each case and they are

$\mathfrak{A}_5$, $\mathfrak{S}_5$, $\mathfrak{A}_6$, $\mathfrak{S}_6$, $PGL_2(F_p)$, $PGL_2(F_9)$, $P\Gamma P_2(F_9)$, $PGL_2(F_q)$, $P\Gamma L_2(F_q)$ *and the Mathieu group* M_{11}, *respectively.*

We remark that for each value of q considered there is a unique near field F_q, except when $q = 9$.   For $q = 9$, there are two non-isomorphic near fields. If F_9 is the non-commutative near field of 9 elements, then $L(F_q)$ is isomorphic to $U_3(2)$.   In this case the transitive extension is $PGL_2(F_9)$ which Zassenhaus [11] called a Mathieu group M_9.

The following theorem has a few applications.

THEOREM 5.   *Let G be a 4-transitive permutation group such that the stabilizer of two points contains a normal subgroup which is regular on the rest of points.   Then G is one of the following groups:* $\mathfrak{A}_6$, $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{S}_6$, *or* M_{11}.

Proof. Let U be the stabilizer of a point a and let H be the stabilizer of two points a and b.   By assumption H contains a normal subgroup Q which is regular on points different from a nor b.   Since G is 4-transitive, H is doubly transitive.   Hence Q is an elementary abelian p-group ([1], §145).   Thus U satisfies the conditions (1) and (3) of Theorem 1.   The condition (2) was used in the proof only to insure that the element t in the extended group leaves Q invariant.   In G, the group $H_1 = \langle H, t \rangle$ is doubly transitive on the set of points $\neq a, b$.   If this representation of H_1 is not faithful, then G contains a trans-

position and G is a symmetric group. Hence $G = \mathfrak{S}_4$, $\mathfrak{S}_5$ or $\mathfrak{S}_6$. On the other hand if the representation is faithful, then $Q_1 = \langle Q, Q^t \rangle$ is a solvable normal subgroup of the doubly transitive group H_1. Hence a minimal normal subgroup of H_1 contained in Q_1 is regular by a theorem of Burnside ([1], § 154). We may assume that $Q^t = Q$. Thus U must be one of the exceptions described in Theorem 3. Among exceptional groups, only $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{A}_5$, $\mathfrak{S}_5$ and $PGL_2(F_9)$ are triply transitive.

The following are two corollaries.

COROLLARY 1. *Let G be a permutation group on n letters, which does not contain the alternating group $\mathfrak{A}_n$. Assume that G is $(k+2)$-transitive for $k \geqq 2$. If the stabilizer of k distinct letters contain a normal subgroup which is regular on the rest of letters, then $k = 2$ or 3 and G is the Mathieu groups M_{11} or M_{12}.*

Proof. If $k = 2$, this is a restatement of Theorem 4. M_{11} admits a unique transitive extension M_{12} but M_{12} admits no further extension.

COROLLARY 2. *Let G be a permutation group on n letters which does not contain the alternating group $\mathfrak{A}_n$. If G is 7-transitive, then the stabilizer of 5 distinct letters contains a normal subgroup S such that S is non-abelian simple, and $\mathrm{Aut}\, S/S$ involves the symmetric group on 5 letters.*

Proof. Let H be the stabilizer of 5 distinct letters and let L be the stabilizer of the set consisting of these 5 letters. Then H is a normal subgroup of L and $L/H \cong \mathfrak{S}_5$. Wielandt [9] proved that L is faithful on the rest of $n - 5$ letters. A minimal normal subgroup S of L contained in H is not regular by the previous corollary. Hence by a theorem of Burnside [1] S is simple and $C_L(S) = S$. The assertion follows.

Remark. The above corollary is due to H. Nagao [4]. The author is grateful to Professor Nagao for communicating his result before publication. Schreier has conjectured that for any non-abelian simple group S, $\mathrm{Aut}\, S/S$ would be solvable. The author knows no simple group S for which $\mathrm{Aut}\, S/S$ involves $\mathfrak{S}_4$. So either any 6-transitive permutation group on n letters contains the alternating group $\mathfrak{A}_n$ or else the stabilizer of 4 distinct letters involves a very complicated, probably unknown at present, simple group.

References

[1] W. Burnside, Theory of groups, 2nd ed. (1911).

[2] D. R. Hughes, Combinatorial analysis; t-designs and permutation groups, Proc. Sympos. Pure Math., vol. VI (1962), 39-41.

[3] D. R. Hughes, Extensions of designs and groups: The unitary groups, Math. Z. (to appear).

[4] H. Nagao, On multiply transitive permutation groups I, Nagoya J. of Math. **27** (1966), 15-19.

[5] R. Ree, A family of simple groups associated with the simple Lie algebra of type (G_2), Amer. J. Math., **83** (1961), 432-462.

[6] M. Suzuki, A characterization of simple groups $LF(2, p)$, Jour. Fac. Sci. Univ. of Tokyo, I-**6** (1951), 259-293.

[7] M. Suzuki, A new type of simple groups of finite order, Proc. Nat. Acad. Sci. USA, **46** (1960), 868-870.

[8] M. Suzuki, On a class of doubly transitive groups II, Annals of Math. **79** (1964), 514-589.

[9] H. Wielandt, Über den Transitivitätsgrad von Permutationsgruppen, Math. Z. **74** (1960), 297-298.

[10] E. Witt, Die 5-fach transitiven Gruppen von Mathieu, Abh. Math. Sem. Hamburg Univ., **12** (1937), 256-264.

[11] H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, Abh. Math. Sem. Hamburg Univ. **11** (1936), 17-40.

University of Illinois