数理解析研究所講究録
第 277 巻 1976 年 58-66

On the Higman-Sims simple group of order $44{,}352{,}000 = 2^9\cdot 3^2\cdot 5^3\cdot 7\cdot 11 = 176\cdot 175\cdot 10\cdot 9\cdot 8\cdot 2$

木村 浩 (北大理)

Let y be a field automorphism of $PGL(2,q^2)$ of order 2, where q is a power of an odd prime number.

<u>Theorem</u>. Let G be a 2-transitive group on $\Omega = \{1,2,\cdots,n\}$, n is even. If $G_{1,2}$ is $PGL(2,q^2)\langle y\rangle$, then either

(1) G has a RNS, or

(2) $q = 3$, $n = 176$ and G is the Higman-Sims simple group.

I gave an outline of a proof of this theorem

Notation: Let X be a subset of a permutation group Y. Let F(X) denote the set of all fixed points of X and $\alpha(X)$ be the number of points in F(X). $N_Y(X)$ acts on F(X). Let $\chi_1(X)$ and $\chi(X)$ be the kernel of this representation and its image, respectively.

1. Properties of $PGL(2,q^2)\langle y\rangle$.

Let t' be an element of $PGL(2,q^2)$ of order q^2-1 and x be an involution of $PSL(2,q^2)$ which normalizes $\langle t'\rangle$. Set $\langle s\rangle = O_2(\langle t'\rangle)$ and $\langle t\rangle = O(\langle t'\rangle)$. We may assume $\langle t'\rangle^y = \langle t'\rangle$ and $[x,y] = 1$. Let τ be a unique involution of $\langle s\rangle$.

(1.1) $\langle y,s\rangle$ is quasi-dihedral if $4\nmid q-1$ and
$\langle yx,s\rangle$ is quasi-dihedral if $4\mid q-1$

(1.2) $PGL(2,q^2)\langle y\rangle$ has 3 classes of involutions.

τ, y and xs are representatives of these classes.

2. Let I be an involution of G with the cyle structure $(1,2)\cdots$. Then I normalizes $G_{1,2}$ and we may assume $[I,G_{1,2}] = 1$. By (1,2) every involution of G is conjugate to I, $I\tau$, Ixs or Iy.

3. Conjugation of involutions.

Lemma 3.1. $\tau \not\sim y,\ xs$.

Lemma 3.2. $y \not\sim xs$

By Lemma 3.1 and a theorem of Witt $\chi(\tau)$ is 2-transitive on $F(\tau)$.

4. Structure of $\chi(\tau)$.

Let $\bar{g}$ denote the image in $\chi(\tau)$ of an element g of $C_G(\tau)$.

Lemma 4.1. $\chi(\bar{x})$ is 2-transitive on $F(\bar{x})$.

Let T be a Sylow 2-subgroup of $\chi_1(\tau)$ contained in $S = \langle x,s,y\rangle$.

By the structure of $\chi(\tau)_{1,2}$ we have the following cases.

(I) $s^2 \notin T \not\subset \langle s\rangle$

(II) $s^2 \in T \not\subset \langle s\rangle$

(III) $T \subset \langle s\rangle$.

Lemma 4.5. $\chi(\tau) \supset RNS \Rightarrow I \not\sim \tau$.

Lemma 4.6. $\chi(\tau) \supset RNS \Rightarrow q = 3$

$Iy \sim \tau$

Lemma 4.7. $\alpha(\tau)$ is a power of $2 \Rightarrow IXs \not\sim \tau$.

Lemma 4.12. $q = 3$ or $\bar{t} \neq 1$.

Lemma 4.4. In the case (I) $T = \langle xys^j\rangle$ or $\langle ys^j\rangle$

$\langle xys^j\rangle \Downarrow [s^j,xy]=1$ $\qquad$ $\langle ys^j\rangle \Downarrow [y,s^j]=1$

where $|s^j| = 4$, and $\chi(\tau) \supset$ RNS.

5. The case (I)

Lemma 5.1. $q = 3 \Rightarrow G$ is H-S

Lemma 5.2. $q \neq 3 \Rightarrow G \supset$ RNS.

6. The case (II)

There is no group statisfying the conditions in Theorem.

7. The case (III).

Lemma 7.10. $T = \langle\tau\rangle$.

Lemma 7.11. $\chi(\tau) \supset$ RNS $\Rightarrow q \neq 3$.

Lemma 7.12. $\chi(\bar{x}) \supset$ RNS.

From these lemmas we have that G has a RNS.

8. By the proof of Theorem we have the following.

Corollary. Let G be as in Theorem. If G has a RNS, the following conditions are satisfied.

(1) $n = \alpha(\tau)^2 = \alpha(y)^2$.

(2) $\bar{t} \neq 1$, and

(3) $\chi_1(\tau) = \langle xys'\rangle$ if $\langle y,s\rangle$ is quasi-dihedral,

$\chi_1(\tau) = \langle ys'\rangle$ if $\langle xy,s\rangle$ is quasi-dihedral

or

$\chi_1(\tau) = \langle\tau\rangle$, where s' is an element of $\langle s\rangle$ of order 4.

Important theorems for the proof of Theorem are the following:

1. Theorems of Aschbacher.

(i) Doubly transitive groups in which the stabilizer of two points is abelian, J. Alg. 18 (1971).

(ii) 2-transitive groups whose 2-point stabilizer has 2-rank 1, J. Alg. 36 (1975).

2. A theorem of Baer.

Engelsche Elemente noethersche Gruppen, Math. Ann. 133 (1957).

3. A Theorem of Bender.

Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine Fixpukte haben, Math. Z. 104 (1968).

4. A theorem of Huppert.

Zweifach transitive, auflösbare Permutationsgruppen, Math. Z. 68 (1957).

5. Degree formula (Ito-Nagao-Kimura).

Let G be a 2-transitive group on $\Omega = \{1,\cdots,n\}$. Let ζ be an involution of $G_{1,2}$. Let $\beta(\zeta)$ be the number of involutions of G with cycle structures $(1,2)\cdots$ which are conjugate to ζ and $\gamma(\zeta)$ be the number of involutions of $G_{1,2}$ which are conjugate to ζ. Then

$$n = \frac{\beta(\zeta)}{\gamma(\zeta)}\alpha(\zeta)(\alpha(\zeta)-1) + \alpha(\zeta), \text{ and}$$

$$|C_G(\zeta)| = \alpha(\zeta)(\alpha(\zeta)-1)\frac{|G_{1,2}|}{\gamma(\zeta)} .$$

Degree formula is useful in a proof of Theorem.

As an example we shall prove Lemma 3.1. and the case (I).

Proof of Lemma 3.1.

	τ	y	xs
$\lvert G_{1,2} : C_{G_{1,2}}(\ )\rvert$	$\frac{q^2(q^2+1)}{2}$	$q(q^2+1)$	$\frac{q^2(q^2-1)}{2}$
(q = 3	45	30	36)

(1) Assume $\tau \sim y \nsim xs$. Since $\gamma(\tau) = |G_{1,2}|(1/4(q^2 - 1) + 1/2q(q^2 - 1)) = |G_{1,2}|(q + 2)/4q(q^2 - 1)$,
$|C_G(\tau)| = 4i(i - 1)\, q(q^2 - 1)/(q + 2)$ by the degree formula. We next prove $\chi(\tau)$ is a rank 3 permutation group on $F(\tau)$ with subdegrees 1, $q(i - 1)/q + 2$ and $2(i - 1)/q + 2$. Consider the length of the $C_{G_1}(\tau)$-orbit containing the point 2.

$$|2^{C_{G_1}(\tau)}| = |C_{G_1}(\tau) : C_{G_{1,2}}(\tau)|\,.$$

$$= |C_G(\tau) : C_{G_{1,2}}(\tau)|/|C_G(\tau) : C_{G_1}(\tau)|$$

$= i(i - 1)q/i'(q + 2)$, where $i' = |C_G(\tau) : C_{G_1}(\tau)|$. Similarly

$|2^{C_{G_1}(y)}| = 2i(i - 1)/i''(q + 2)$, where $i'' = |C_G(y) : C_{G_1}(y)|$.

Set $y^g = \tau$ with g in G. If $1^{C_G(\tau)}$ and $(1^{C_G(y)})^g$ are different $C_G(\tau)$-orbits, then $i - 1 \leq i(i - 1)q/i'(q + 2) + 2i(i - 1)/i''(q + 2) \leq i - 2$, a contradiction. Thus $1^{C_G(\tau)} = (1^{C_G(y)})^g (= 1^{gC_G(\tau)})$ and $i' = i''$. Since $|2^{C_{G_1}(\tau)}|$

$\neq |2^{C_{G_1}(y)g}|$, $C_{G_1}(\tau)$ has at least three orbits of length 1,

$|2^{C_{G_1}(\tau)}|$ and $|2^{C_{G_1}(y)}|$. Thus $i - 1 \leq i(i - 1)q/i'(q + 2) + 2i(i - 1)/i'(q + 2) \leq i - 1$. Hence $i = i'$ and $\chi(\tau)$ is of rank 3. $C_{G_{1,2}}(y)$ is conjugate to a subgroup of $C_{G_1}(\tau)$. Since

$\langle s, x, y\rangle$ is a Sylow 2-subgroup of $C_{G_1}(\tau)$ and $u^2 = \tau$ for every element u in $\langle s, x, y\rangle$ of order 4, a square of every element in $C_{G_{1,2}}(y)$ of order 4 is y. On the other hand $C_{G_{1,2}}(y)$ is isomorphic to $PGL(2, q) \times \langle y\rangle$, a contradiction.

(2). Assume $\tau \sim xs \not\sim y$. As in the case (1), $\chi(\tau)$ is also of rank 3. Thus $C_{G_{1,2}}(xs)$ is conjugate to a subgroup of $C_{G_1}(\tau)$. A Sylow 2-subgroup of $C_{G_{1,2}}(xs)$ is $\langle xs\rangle \times Z_4$, which is a contradiction.

(3). Assume $\tau \sim y \sim xs$. As in the case (1), $\chi(\tau)$ is of rank 4 and we have also a contradiction. This proves the lemma.

The case I

Lemma 5.1. In the case I G is the Higman-Sims simple group if $\bar{t} = 1$.

Proof. By Lemma 4.12 $q = 3$. By Lemma 4.4 T is $\langle xys^2 \rangle$, $\langle \bar{x}, \bar{s} \rangle$ is dihedral of order 8 and $\chi(\tau)$ has a RNS. Since $\chi(\tau)_{1,2}$ is non-abelian, $\chi(\tau)$ is not solvable by [7]. By Lemma 4.1 $\chi(\tau)_1$ has two classes of involutions. By [5. Theorem 7.7.3] $\chi(\tau)_1$ has a subgroup $\bar{X}$ of index 2 and $\bar{X}_{1,2}$ is a four-group. By [1] $\chi(\tau)$ is a semi-direct product of V by PSL(2, 4), where V is a 2-dimensional vector space over the field GF(4) of 4 elements, and $i = 16$. By Lemma 4.5 and Lemma 4.7 τ is not conjugate to I or Ixs.

By Lemma 3.3 $\chi(y)$ is a rank 3 group on F(y) with subdegrees 1, $5(\alpha(y) - 1)/11$ and $6(\alpha(y) - 1)/11$. Set $\alpha(y) = 11m + 1$. If $\tau \sim I\tau \not\sim Iy$, $\gamma(\tau) = \beta(\tau)$ and $n = 16^2$. Since $\gamma(y) = 66$, by the degree formula $11m(11m + 1)\beta(y)/66 + 11m + 1 = 16^2$, where $\beta(y)$ is a sum of elements in a subset of $\{1, 30, 36\}$. A calculation yields that there exists no integer m satisfying the above condition. Similarly we have a contradiction in the case $\tau \sim I\tau \sim Iy$. Thus $\tau \sim Iy \not\sim I\tau$, $y \sim I \sim I\tau \sim Ixs$, $\chi(y) = 12$ and $n = 30 \cdot 16 \cdot 15/45 + 16 = 176$.

Finally we shall prove the simplicity of G. Let N be a minimal normal subgroup. If N is Frobenius group, G has a RNS and n must be a power of 2. Therefore $N_{1,2}$ contains PSL(2, 9). If $N_{1,2}$ = PSL(2, 9), the image in $\chi(\tau)_{1,2}$ of $C_N(\tau)_{1,2}$ is $<\bar{x}, \bar{s}^2>$ since $\chi_1(\tau) = <xys^2>$. We have $\bar{x} \sim \bar{s}^2$ since $\chi(\tau)_1$ = PΓL(2, 4). This contradicts Lemma 4.1. If $N_{1,2}$ = PSL(2, 9)<ys>, the image in $\chi(\tau)_{1,2}$ of $C_N(\tau)_{1,2}$ is isomorphic to $<x, s^2, ys>/<\tau>$, a contradiction. Thus $N_{1,2}$ contains y. Since $y \sim xs$, $N_{1,2} = G_{1,2}$. Since $\chi(\tau)$ is generated by $\bar{x}$ and $\bar{s}^{\chi(\tau)}$, the image in $\chi(\tau)$ of $C_N(\tau)$ is $\chi(\tau)$, that is, $C_N(\tau)$ = $C_G(\tau)$. Since $Z(<x, s, y>) = <\tau>$, $N_{G_1}(<x, s, y>)$ is contained in $C_{G_1}(\tau)$. By the Frattini argument $G_1 = N_1 N_{G_1}(<x, s, y>) = N_1$. Thus G = N. By Parrott-Wong G is the Higman-Sims simple group. This completes a proof of Lemma 5.1.

Lemma 5.2. In the case I G has a RNS if $\bar{t} \neq 1$.

Proof. By Lemma 4.4 $\chi(\tau)$ has a RNS. Therefore by Lemma 4.5-Lemma 4.7 τ is not conjugate to I, Iy or Ixs and $\tau \sim I\tau$. By the degree formula $n = i^2$. By Lemma 3.2 $\gamma(y)$ = even. Since $\alpha(y)$ is even, $\beta(y)$ must be even by the degree formula. Thus $y \nsim I$ and $\alpha(I) = 0$. Assume <y, s> is qusai-dihedral. $\bar{I}$ is contained in a RNS of $\chi(\tau)$. By Lemma 4.1 $\bar{x}$ is not conjugate to $\bar{s}^j$. If $\bar{s}^j \nsim \overline{xs}$, $\chi(\tau)_1$ has three classes of involutions, it is solvable by [5, Theorem 7.7.3] and so is $\chi(\tau)$. This contradicts [8]. Thus $\bar{s}^j \sim \overline{xs}$. Since $[\chi(\tau)_{1,2}:C_{\chi(\tau)_{1,2}}(\bar{u})]$ is even, where $\bar{u}$ is $\bar{x}$ or $\overline{xs}$ and it is 1 for $\bar{u} = \bar{s}^j$, $\gamma(\bar{s}^j)$ is odd and $\gamma(\bar{x})$ is even. By the degree formula $\beta(\bar{s}^j)$ is odd and $\beta(\bar{x})$ is even, that is, $\overline{I}\bar{s}^j \sim \bar{s}^j$. Since $Is^jT = \{Is^j, Is^j\tau, Ixy, Ixy\tau\}$ and $s^jT = \{s^j, s^j\tau, xy, xy\tau\}$, $Ixy \sim xy$ and hence $Iy \sim y$. Since $xT = \{x, x\tau, ys^j, ys^j\tau\}$ and $IxsT = \{Ixs, Ixs\tau, Iys^{1+j}, Iys^{1+j}\tau\}$ $\bar{x} \nsim \overline{I}\overline{xs}$. Therefore $\overline{I}\overline{xs} \sim \overline{I}\bar{s}^j$ since $\alpha(\overline{I}\overline{xs}) > 0$, that is, $Iy \sim Ixs$. This prove that $IG_{1,2}$ contains a unique fixed point free involution I and n is a power of 2. By Lemma 2.2 G has a RNS. This completes a proof of the lemma.