Hokkaido Mathematical Journal Vol. 26 (1997) p. 435–438

Generating alternating groups

Naoki CHIGIRA

(Received March 11, 1996; Revised June 21, 1996)

Abstract. We will give an elementary proof of the following: For any nonidentity element x in the alternating group A_n on n symbols, there exists an element y such that x and y generate A_n.

Key words: the alternating group, block.

Let S_n be the symmetric group on the symbols $\Omega=\{1,2,\ldots,n\}$ and A_n the alternating group on Ω. Isaacs and Zieschang [1] give an elementary proof of the following:

Theorem A *Assume that $n\neq 4$ and let $x\in S_n$ be an arbitrary nonidentity element. Then there exists an element $y\in S_n$ such that $S_n=\langle x, y\rangle$.*

They say "*A result similar to Theorem* A *is known to be valid for the alternating group A_n for all values of n. Although it seems likely that a proof of this result along the lines of our proof of Theorem* A *might exist, there are technical difficulties in some cases, and we have not actually found such a proof.*"

In this note, we will give a proof for A_n along the lines of the proof of Theorem A by Isaacs and Zieschang [1].

Theorem *Let $x\in A_n$ be an arbitrary nonidentity element. Then there exists an element $y\in A_n$ such that $A_n=\langle x, y\rangle$.*

A nonempty subset $\Delta\subseteq\Omega$ is said to be a block for G if Δ^x is either disjoint from or equal to Δ for each element $x\in G$. A group G is said to be primitive if the only blocks for G are the singleton subset or the whole set Ω.

The following theorems and lemma play an important role in our proof.

Theorem (Jordan) *Suppose that G is a primitive subgroup of S_n. If G contains a 3-cycle, then either $G=S_n$ or $G=A_n$.*

1991 Mathematics Subject Classification : 20B15, 20B35.

Proof. See [1, Theorem (Jordan)]. $\square$

Theorem B *Let* $x = (1, 2, 3, \ldots, m)$ *for odd number* m *and* $y = (1, 2, 3, \ldots, n)$ *for odd number* n, *where* $1 < m < n$. *Then* $A_n = \langle x,\, y \rangle$.

Proof. See [1, Theorem B]. $\square$

Lemma 1 *Suppose that* G *is a transitive subgroup of* S_n *on* Ω.

(1) *Let* Δ *be a block for* G. *Then* $|\Delta|$ *divides* n. *Especially, if* $\Delta \neq \Omega$, *then* $|\Delta| \leq n/2$.

(2) *Let* $\alpha \in \Omega$. *Then* G *is primitive on* Ω *if the only blocks containing* α *are* $\{\alpha\}$ *and* Ω.

Proof. See [1, Lemma] and the above paragraph. $\square$

It is easy to prove the following:

Lemma 2 *Suppose that* G *is a transitive subgroup of* S_n *on* Ω.

(1) *If* n *is prime, then* G *is primitive on* Ω.

(2) *If* G *contains a* $(n-1)$*-cycle, then* G *is primitive on* Ω.

Proof. (1) Let $\Delta \subseteq \Omega$ be a block for G containing 1. By Lemma 1 (1), $\Delta = \{1\}$ or Ω. Lemma 1 (2) yields the result.

(2) We may assume that G contains a $(n-1)$-cycle $x = (2, 3, \ldots, n)$. Let $\Delta \subsetneq \Omega$ be a block for G containing 1. Since $\Delta^x \ni 1^x = 1$, we have $\Delta^x = \Delta$. If Δ contains α $(2 \leq \alpha \leq n)$, we have $\Delta = \Omega$ by the action of x. This is a contradiction. This yields that only blocks containing 1 are $\{1\}$ and Ω. By Lemma 1 (2), we have the result. $\square$

Lemma 3 *Let* $y = (2, 3, \ldots, n)$ *for even number* n *and* x *be one of the following elements*:

(1) $x = (1, 2, 3, \ldots, m)$ *if* $n > m > 1$ *and* m *is odd.*

(2) $x = (1, 2)(3, 4)$ *if* $n \geq 4$.

(3) $x = (1, 2, 3)(4, 5, 6)$ *if* $n \geq 6$.

(4) $x = (1, 2, 3, 4)(5, 6)$ *if* $n \geq 6$.

(5) $x = (1, 2)(3, 4)(5, 6, 7)$ *if* $n \geq 8$.

(6) $x = (1, 2, 3, 4, 5)(6, 7, 8)$ *if* $n \geq 8$.

(7) $x = (1, 2, 3)(4, 5, 6)(7, 8, 9)$ *if* $n \geq 10$.

Then $A_n = \langle x,\, y \rangle$.

Proof. It is easily seen that $\langle x,\, y \rangle$ is a transitive subgroup of A_n on Ω in each case. By Lemma 2 (2) and Jordan's theorem, it suffices to show that $\langle x,\, y\rangle$ contains a 3-cycle.

(1) If $n \neq m+1$, then $((xyx^{-1}y^{-1})(x^{-1}y^{-1}xy))^2 = (1, m+1, n)$. If $n = m+1$, then $xy^{-1} = (1, m+1, m)$.

(2) If $n \geq 8$, then $(x(y^{-3}xy^3))^2 = (1,5,2)$. If $n = 6$, then $(y^{-2}xy^2)((y^{-3}xy^3)^{-1}\, x(y^{-3}xy^3)) = (1,3,4)$. If $n = 4$, then $y = (2,3,4)$.

(3) If $n \geq 8$, then $(x(y^{-1}xy)(y^{-2}xy^2)^{-1})^2 = (4,7,8)$. If $n = 6$, then $x^{-1}y = (1,4,2)$.

(4) If $n \geq 8$, then $(x(y^{-2}xy^2)^{-1})^2 = (1,3,2)$. If $n = 6$, then $x^{-1}y = (1,5,2)$.

(5) We see that $x^2 = (5,7,6)$.

(6) We see that $x^5 = (6,8,7)$.

(7) We see that $(x(y^{-1}xy))^4 = (5,7,9)$. □

Proof of Theorem. We consider first the case where n is odd. It is trivial when $n = 3$. We may assume that $n \geq 5$. If x is a 3-cycle, then we can suppose $x = (1,2,3)$ and we have $\langle x,\, y\rangle = A_n$ for $y = (1,2,3\ldots,n)$ by Theorem B. Therefore we can assume that x moves at least four points.

Suppose that $n \not\equiv 1 \pmod 3$. We can suppose that $1^x = 2$ and $4^x = 5$. We take $y = (2,3,4)(5,6,\ldots,n)$ and let $G = \langle x,\, y\rangle$. Then G is a transitive subgroup of A_n on Ω and G contains a 3-cycle y^{n-4}. It suffices to show that G is primitive. Let $\Delta \subsetneq \Omega$ be a block for G containing 1. If $n = 5$, then G is primitive on Ω by Lemma 2 (1). We may assume that $n \geq 9$. If Δ contains $\alpha \in \{5,6,\ldots,n\}$ then $|\Delta| \geq n-3 > n/2$ because $\Delta^y = \Delta$ and $n \geq 9$. This is a contradiction by Lemma 1 (1). This yields $\Delta \subseteq \{1,2,3,4\}$. Since $|\Delta|$ divides n, $|\Delta|$ is odd. If $|\Delta| = 3$, it is easily seen that $\Delta \neq \Delta^y$. This yields that G is primitive on Ω by Lemma 1 (2). By Jordan's theorem, we have $G = A_n$.

Suppose that $n \equiv 1 \pmod 3$. We may assume that $n \geq 7$. We can suppose that $3^x = 4$ and $5^x = 6$. We take $y = (1,2,3)(4,5)(6,7,\ldots,n)$ and let $G = \langle x,\, y\rangle$. Then G is a transitive subgroup of A_n on Ω and G contains a 3-cycle y^{n-5}. Let $\Delta \subsetneq \Omega$ be a block for G containing 1. If $n = 7$, then G is primitive on Ω by Lemma 2 (1). We may assume that $n \geq 13$. If Δ contains a symbol $\alpha \in \{6,7,\ldots,n\}$, then $|\Delta| \geq n-4 > n/2$ since $\Delta^{y^3} = \Delta$ and $n \geq 13$, a contradiction by Lemma 2 (1). We have $\Delta \subseteq \{1,2,3,4,5\}$. Since $|\Delta|$ divides n, $|\Delta|$ is odd and $|\Delta| \neq 3$. If $\Delta = \{1,2,3,4,5\}$, then $\Delta^x = \{1^x, 2^x, 4, 4^x, 6\}$, a contradiction. This yields that G is primitive on

Ω. By Jordan's theorem, we have $G = A_n$.

Now, assume that n is even. Suppose that $n \not\equiv 0 \pmod 3$. It is trivial when $n = 4$. We may assume that $n \geq 8$. We can suppose that $3^x = 4$. We take $y = (1, 2, 3)(4, 5, \ldots, n)$ and let $G = \langle x, y \rangle$. Then G is a transitive subgroup of A_n on Ω and G contains a 3-cycle y^{n-3}. Let $\Delta \subsetneq \Omega$ be a block for G containing 1. If Δ contains a symbol $\alpha \in \{4, 5, \ldots, n\}$, then $|\Delta| \geq n - 2 > n/2$ since $\Delta^{y^3} = \Delta$ and $n \geq 8$. This is a contradiction by Lemma 1 (1). We have $\Delta \subseteq \{1, 2, 3\}$. Since $|\Delta|$ divides n, $\Delta \neq \{1, 2, 3\}$. If $|\Delta| = 2$, it is easily seen that $\Delta \neq \Delta^y$. This yields that G is primitive on Ω by Lemma 1 (2). By Jordan's theorem, we have $G = A_n$.

We may suppose that $n \equiv 0 \pmod 3$. By Lemma 3 (1)–(4), the theorem holds where $n = 6$. We may assume that $n \geq 12$. If x moves at most seven points, then there exists a $(n-1)$-cycle y such that $\langle x, y \rangle = A_n$ by Lemma 3 (1)–(5). Hence we may assume $1^x = 2$, $3^x = 4$, $5^x = 6$ and $7^x = 8$. We take $y = (1, 2, 3)(4, 5)(6, 7)(8, 9, \ldots, n)$ and let $G = \langle x, y \rangle$. Then G is a transitive subgroup of A_n on Ω and G contains a 3-cycle $y^{2(n-7)}$. Let $\Delta \subsetneq \Omega$ be a block for G containing 1. If Δ contains a symbol $\alpha \in \{8, 9, \ldots, n\}$ and if $n > 12$, then $|\Delta| \geq n - 6 > n/2$ since $\Delta^{y^3} = \Delta$. This is a contradiction by Lemma 1 (1). If $n = 12$ and Δ contains a symbol $\alpha \in \{8, 9, 10, 11, 12\}$, then $\Delta \supseteq \{1, 8, 9, 10, 11, 12\}$. In this case we have $\Delta = \Omega$ since $\Delta^y = \Delta$, a contradiction. We have $\Delta \subseteq \{1, 2, 3, 4, 5, 6, 7\}$. If $|\Delta| \geq 2$, we can get a contradiction in any cases by the action of x, y or y^3 on Δ. This yields that G is primitive on Ω by Lemma 1 (2). By Jordan's theorem, we have $G = A_n$. $\square$

References

[1] Isaacs I.M. and Zieschang Thilo, *Generating symmetric groups*. Amer. Math. Monthly **102** (1995), 734–739.

Department of Mathematics
Kumamoto University
Kumamoto 860, Japan
E-mail: chigira@sci.kumamoto-u.ac.jp