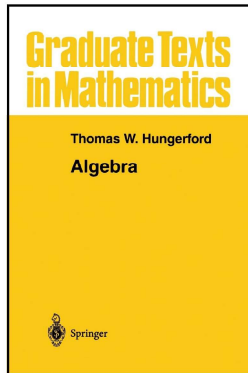


# Modern Algebra

## Chapter I. Groups

### I.6. Symmetric, Alternating, and Dihedral Groups

#### —Proofs of Theorems



## Theorem I.6.3

**Theorem I.6.3.** Every nonidentity permutation in  $S_n$  is uniquely (up to the order of the factors) a product of disjoint cycles, each of which has length at least 2.

**Proof.** Let  $\sigma \in S_n$  be a nonidentity. Define the relation  $\sim$  on  $I_n = \{1, 2, \dots, n\}$  as  $x \sim y$  if and only if  $y = \sigma^m(x)$  for some  $m \in \mathbb{Z}$ . We claim that  $\sim$  is an equivalence relation on  $I_n$ . (1) Reflexive:  $x \sim x$  since  $x = \sigma^0(x)$  for all  $x \in I_n$ ; (2) Symmetric: if  $x \sim y$  then  $y = \sigma^m(x)$  and so  $x = \sigma^{-m}(y)$  and  $y \sim x$ ; (3) Transitive: if  $x \sim y$  and  $y \sim z$  then  $y = \sigma^m(x)$  and  $z = \sigma^n(y)$ , so  $z = \sigma^{n+m}(x)$  and  $x \sim z$ . Denote the equivalence classes of  $\sim$  as  $\{B_i \mid 1 \leq i \leq s\}$ . The equivalence classes are the orbits of  $\sigma$  and partition  $I_n$  by Theorem 0.1.4. Let  $B_1, B_2, \dots, B_r$  ( $1 \leq r \leq s$ ) be those orbits that contain more than one element of  $I_n$  (that is, the orbits of length greater than one).

## Theorem I.6.3 (continued 1)

**Proof (continued).** For each  $i \leq r$ , define  $\sigma_i \in S_n$  by:

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{if } x \in B_i \\ x & \text{if } x \notin B_i \end{cases}$$

(notice that  $\sigma_i$  is well defined since  $x \in B_i$  for only one  $i$ ). Then  $\sigma_i|_{B_i}$  is a bijection from  $B_i$  to  $B_i$ . Since the  $B_i$  are disjoint, then  $\sigma_1, \sigma_2, \dots, \sigma_r$  are disjoint permutations. Next, for  $x \in I_n$  we have  $x \in B_i$  for a unique  $i$  and so  $\sigma(x) = \sigma_i(x) = \sigma_1\sigma_2 \cdots \sigma_r(x)$  since the  $\sigma_k$ 's are disjoint. Therefore,  $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$  on  $I_n$ . Now to show that each  $\sigma_k$  is a cycle.

If  $x \in B_i$  ( $i \leq r$ ) then since  $B_i$  is finite there is a least positive integer  $d$  such that  $\sigma^d(x) = x$  for some  $j$  with  $0 \leq j < d$  (here the nonnegative powers of  $\sigma$  produce images of  $x \in B_i$  and  $d$  is the "first time" that the orbit of  $x$  has wrapped around and intersected itself). Since  $\sigma^{d-j}(x) = x$  and  $0 < d - j \leq d$ , we must have  $j = 0$  and  $\sigma^d(x) = x$  (or else  $d$  is not minimal and could be replaced with  $d - j$  above).

## Theorem I.6.3 (continued 2)

**Proof (continued).** Hence  $(x, \sigma(x), \sigma^2(x), \dots, \sigma^{d-1}(x))$  is a cycle of length at least 2. If  $\sigma^m(x) \in B_i$  then  $m = ad + b$  for some  $a, b \in \mathbb{Z}$  such that  $0 \leq b < d$  (by the Division Algorithm, Theorem 0.6.3).

Hence

$$\sigma^m(x) = \sigma^{ad+b}(x) = \sigma^b \sigma^{ad}(x) = \sigma^b(x)$$

since  $\sigma^d(x) = x$ . So  $\sigma^m(x) = \sigma^b(x)$  where  $0 \leq b < d$  and hence

$$\sigma^m(x) \in \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{d-1}(x)\}.$$

Now for  $x \in B_i$  we have  $B_i = \{\sigma^m(x) \mid m \in \mathbb{Z}\}$  since  $B_i$  is an equivalence class, so we have shown that if  $\sigma^m(x) \in B_i$  then

$$\sigma^m(x) \in \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{d-1}(x)\}, \text{ so that}$$

$$B_i \subseteq \{x, \sigma(x), \dots, \sigma^{d-1}(x)\},$$

and "clearly"

$$\{x, \sigma(x), \sigma^2(x), \dots, \sigma^{d-1}(x)\} \subseteq B_i.$$

## Theorem I.6.3 (continued 3)

**Proof (continued).** Therefore  $B_i = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{d-1}(x)\}$  where  $x$  is some element of  $B_i$ . So  $\sigma_i$  is the cycle  $(x, \sigma(x), \sigma^2(x), \dots, \sigma^{d-1}(x))$ . Suppose  $\tau_1, \tau_2, \dots, \tau_t$  are disjoint nontrivial cycles such that  $\sigma = \tau_1 \tau_2 \cdots \tau_t$  (to show uniqueness). Let  $x \in I_n$  be such that  $\sigma(x) \neq x$ . Since the  $\tau$ 's are disjoint, there exists a unique  $j$  with  $1 \leq j \leq t$  where  $\sigma(x) = \tau_j(x)$ . Now

$$\begin{aligned} \tau_j \sigma &= \tau_j (\tau_1 \tau_2 \cdots \tau_j \cdots \tau_t) \\ &= \tau_1 \tau_j \tau_2 \cdots \tau_j \cdots \tau_t \text{ since the } \tau \text{'s are disjoint} \\ &= \tau_1 \tau_2 \tau_j \cdots \tau_j \cdots \tau_t \\ &= \tau_1 \tau_2 \cdots \tau_j^2 \cdots \tau_t \\ &= \tau_1 \tau_2 \cdots \tau_j \cdots \tau_j \tau_t \\ &= (\tau_1 \tau_2 \cdots \tau_j \cdots \tau_t) \tau_j \\ &= \sigma \tau_j. \end{aligned}$$

## Theorem I.6.3 (continued 4)

**Proof (continued).** So

$$\begin{aligned} \sigma^k(x) &= \sigma^{k-1} \sigma(x) \\ &= \sigma^{k-1} \tau_j(x) \text{ since } \sigma(x) = \tau_j(x) \\ &= \sigma^{k-2} \sigma \tau_j(x) = \sigma^{k-2} \tau_j \sigma(x) \\ &= \sigma^{k-2} \tau_j \tau_j(x) \\ &\vdots \\ &= \tau_j^k(x) \text{ for all } k \in \mathbb{Z}. \end{aligned}$$

So the orbit of  $x$  under  $\tau_j$  is precisely the orbit of  $x$  under  $\sigma$ , say  $B_i$ . Consequently,  $\tau_j(y) = \sigma(y)$  for all  $y \in B_i$  (since  $y = \sigma^n(x) = \tau_j^n(x)$  for some  $n \in \mathbb{Z}$ ). Since  $\tau_j$  is a cycle it has only one nontrivial orbit (if  $\tau_j = (i_1, i_2, \dots, i_u)$  then the orbit is  $\{i_1, i_2, \dots, i_u\}$ ) and it must be that the orbit is  $B_i$ .

## Theorem I.6.3 (continued 5)

**Theorem I.6.3.** Every nonidentity permutation in  $S_n$  is uniquely (up to the order of the factors) a product of disjoint cycles, each of which has length at least 2.

**Proof (continued).** Therefore for  $y \notin B_i$  we have that  $y$  is not an element of the one orbit of  $\tau_j$  and so  $\tau_j(y) = y$  ( $y$  is fixed by  $\tau_j$  since  $y$  is not in the cycle  $\tau_j$ ). So  $\tau_j = \sigma_i$  where  $\sigma_i$  is as defined above. "A suitable inductive argument shows that  $r = t$ ." So, after rearrangement,  $\sigma_i = \tau_i$  for  $i = 1, 2, \dots, r$  and the representation of  $\sigma$  as a product of cycles is unique (except possibly for order).  $\square$

## Corollary I.6.4

**Corollary I.6.4.** The order of a permutation  $\sigma \in S_n$  is the least common multiple of the orders of its disjoint cycles.

**Proof.** Let  $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$  with  $\{\sigma_i \mid 1 \leq i \leq r\}$  the disjoint cycles. Since disjoint cycles commute,  $\sigma^m = \sigma_1^m \sigma_2^m \cdots \sigma_r^m$  for all  $m \in \mathbb{Z}$ . So  $\sigma^m = (1)$  (the identity) if and only if  $\sigma_i^m = (1)$  for  $1 \leq i \leq r$ . Now  $\sigma_i^m = (1)$  if and only if  $|\sigma_i|$  divides  $m$  by Theorem I.3.4(iv). Therefore  $\sigma^{\text{lcm}(|\sigma_1|, |\sigma_2|, \dots, |\sigma_r|)} = (1)$  and  $\sigma^k = (1)$  for no positive  $k < \text{lcm}(|\sigma_1|, |\sigma_2|, \dots, |\sigma_r|)$ . That is,  $|\sigma| = \text{lcm}(|\sigma_1|, |\sigma_2|, \dots, |\sigma_r|)$ .  $\square$

## Corollary I.6.5

**Corollary I.6.5.** Every permutation in  $S_n$  can be written as a product of (not necessarily disjoint) transpositions.

**Proof.** It suffices by Theorem I.6.3 to show that every cycle is a product of transpositions. For a 1-cycle,  $(x_1) = (x_1, x_2)(x_2, x_1)$ . For an  $r$ -cycle,

$$(x_1, x_2, \dots, x_r) = (x_1, x_r)(x_1, x_{r-1})(x_1, x_{r-2}) \cdots (x_1, x_3)(x_1, x_2).$$

□

## Theorem I.6.8

**Theorem I.6.8.** For each  $n \geq 2$ , let  $A_n$  be the set of all even permutations of  $S_n$ . Then  $A_n$  is a normal subgroup of  $S_n$  of index 2 and order  $|S_n|/2 = n!/2$ . Furthermore  $A_n$  is the only subgroup of  $S_n$  of index 2. The group  $A_n$  is called the *alternating group* on  $n$  letters.

**Proof.** Let  $C$  be the multiplicative group on  $\{-1, 1\}$ . Define  $f : S_n \rightarrow C$  as  $f(\sigma) = \text{sgn}(\sigma)$ . We claim that  $f$  is an epimorphism. First, let  $\sigma, \tau \in S_n$ . If  $\sigma$  and  $\tau$  are both even or both odd, then  $\sigma\tau$  is even. If  $\sigma$  is even (respectively, odd) and  $\tau$  is odd (respectively, even) then  $\sigma\tau$  is odd (in all four claims, just count the transpositions in a representation of  $\sigma$  and  $\tau$ ). We then have in all four cases  $f(\sigma\tau) = f(\sigma)f(\tau)$  and  $f$  is a homomorphism. Also,  $f$  is onto since  $f((1, 2)) = -1$  and  $f((1, 2)(1, 2)) = 1$ . So  $f$  is an epimorphism.

## Theorem I.6.8 (continued)

**Theorem I.6.8.** For each  $n \geq 2$ , let  $A_n$  be the set of all even permutations of  $S_n$ . Then  $A_n$  is a normal subgroup of  $S_n$  of index 2 and order  $|S_n|/2 = n!/2$ . Furthermore  $A_n$  is the only subgroup of  $S_n$  of index 2. The group  $A_n$  is called the *alternating group* on  $n$  letters.

**Proof (continued).** Now  $\text{Ker}(f) = A_n$  (since 1 is the identity of the multiplicative group  $\{-1, 1\}$ ) and by Exercise I.2.9(a)  $A_n$  is a subgroup of  $S_n$ . By Theorem I.5.5,  $A_n$  is a normal subgroup of  $S_n$ . By the First Isomorphism Theorem (Corollary I.5.7),  $S_n/\text{Ker}(f) = S_n/A_n \cong \text{Im}(f) = C$  (this is where “onto” is used). So  $[S_n : A_n] = 2$  (the number of cosets of  $A_n$  in  $S_n$ ) and by Lagrange’s Theorem (Corollary I.4.6)  $|A_n| = |S_n|/2 = n!/2$ . By Exercise I.6.6,  $A_n$  is the unique subgroup of  $S_n$  of index 2. □

## Lemma I.6.11

**Lemma I.6.11.** Let  $r$  and  $s$  be distinct elements of  $\{1, 2, \dots, n\}$ . Then  $A_n$  (where  $n \geq 3$ ) is generated by the 3-cycles  $\{(r, s, k) \mid 1 \leq k \leq n, k \neq r, s\}$ .

**Proof.** For  $n = 3$ , the set of cycles is (WLOG)  $\{(1, 2, 3)\}$  and  $(1, 2, 3)^2 = (1, 3, 2)$ ,  $(1, 2, 3)^3 = (1)(2)(3)$ , and these are the three elements of  $A_3$ . Now for  $n > 3$ . Since  $A_n$  consists of all even permutations, then  $A_n$  is generated by all pairs of transpositions of the form  $(a, b)(c, d)$  (disjoint transpositions) and  $(a, d)(a, c)$  (transpositions sharing one element; if transpositions share two elements they are the same and the product is the identity) where  $a, b, c, d$  are distinct. Since  $(a, b)(c, d) = (a, c, b)(a, c, d)$  and  $(a, b)(a, c) = (a, c, b)$ , then the set of all 3-cycles generates all pairs of such transpositions and hence generates  $A_n$ .

## Lemma I.6.11 (continued 1)

**Lemma I.6.11.** Let  $r$  and  $s$  be distinct elements of  $\{1, 2, \dots, n\}$ . Then  $A_n$  (where  $n \geq 3$ ) is generated by the 3-cycles  $\{(r, s, k) \mid 1 \leq k \leq n, k \neq r, s\}$ .

**Proof (continued).** Next, recall that we started with given distinct  $r$  and  $s$ . Let  $a, b, c$  be distinct elements which are different from  $r$  and  $s$ . Then any 3-cycle of  $A_n$  must be of one of the following forms:

$(r, s, a)$ ,  $(r, a, s)$  (containing both  $r$  and  $s$  and sending  $r \mapsto s$  or  $s \mapsto r$ ),  
 $(r, a, b)$  (containing  $r$  and not  $s$ ),  
 $(s, a, b)$  (containing  $s$  and not  $r$ ), and  
 $(a, b, c)$  (containing neither  $r$  nor  $s$ ).

## Lemma I.6.11 (continued 2)

**Lemma I.6.11.** Let  $r$  and  $s$  be distinct elements of  $\{1, 2, \dots, n\}$ . Then  $A_n$  (where  $n \geq 3$ ) is generated by the 3-cycles  $\{(r, s, k) \mid 1 \leq k \leq n, k \neq r, s\}$ .

**Proof (continued).** We now write each of these 3-cycles in terms of the 3-cycles given in the statement of the theorem:

$$\begin{aligned}(r, s, a) &= (r, s, a) \\(r, a, s) &= (r, s, a)^2 \\(r, a, b) &= (r, s, b)(r, s, a)^2 \\(s, a, b) &= (r, s, b)^2(r, s, a) \\(a, b, c) &= (r, s, a)^2(r, s, c)(r, s, b)^2(r, s, a).\end{aligned}$$

So any 3-cycle (and hence any element of  $A_n$ , by the first paragraph) is generated by the set  $\{(r, s, k) \mid 1 \leq k \leq n, k \neq r, s\}$  where  $r$  and  $s$  were initially given.  $\square$

## Lemma I.6.12

**Lemma I.6.12.** If  $N$  is a normal subgroup of  $A_n$  (where  $n \geq 3$ ) and  $N$  contains a 3-cycle, then  $N = A_n$ .

**Proof.** Let  $r, s, c$  be distinct where  $(r, s, c)$  is a 3-cycle in  $N$ . Then for any  $k \neq r, s, c$  the 3-cycle  $(r, s, k) \in N$  since

$$\begin{aligned}(r, s, k) &= (r, s)(c, k)(r, s, c)^2(c, k)(r, s) \\ &= [(r, s)(c, k)](r, s, c)^2[(r, s)(c, k)]^{-1} \in N\end{aligned}$$

by Theorem I.5.1(iv) and Definition I.5.2. So for given  $r, s \in \{1, 2, \dots, n\}$  (given as the “first” two elements of the 3-cycle hypothesized to be in  $N$ ) we have all cycles of the form  $(r, s, k) \in N$  where  $k \neq r, s$ . By Lemma I.6.11, these 3-cycles generate  $A_n$  and  $N = A_n$ .  $\square$

## Theorem I.6.10

**Theorem I.6.10.** The alternating group  $A_n$  is simple if and only if  $n \neq 4$ .

**Proof.** Since  $|A_2| = 1$  and  $|A_3| = 3$ , then these groups have no proper subgroups and so are (vacuously) simple. In Exercise I.6.7 you are asked to show that  $N = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$  is a normal subgroup of  $A_4$  (or see my online [Supplement. The Alternating Groups  \$A\_n\$  are Simple for  \$n \geq 5\$](#)  for Introduction to Modern Algebra [MATH 4127/5127]). For  $n \geq 5$ , we show that if  $N$  is a nontrivial normal subgroup of  $A_n$  then  $N = A_n$  (and so  $A_n$  is simple) in five cases. We’ll explain below why these five cases are the only possible cases.

**Case 1.**  $N$  contains a 3-cycle. Then by Lemma I.6.12,  $N = A_n$ .

## Theorem I.6.10 (continued 1)

**Proof. Case 2.**  $N$  contains an element  $\sigma$  which, when written as a product of disjoint cycles (Theorem I.6.3), has at least one of the cycles of length  $r \geq 4$ . Say  $\sigma = (a_1, a_2, \dots, a_r)\tau$  (where  $\tau$  is disjoint from the  $r$ -cycle). Then  $(a_1, a_2, a_3) \in A_n$ , so denote it as  $\delta = (a_1, a_2, a_3)$ . Since  $\sigma \in N$  and  $N$  is normal, then  $\sigma^{-1} \in N$  and  $\delta\sigma\delta^{-1} \in N$  (Theorem I.5.4(iv)), so  $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ . But

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= [\tau^{-1}(a_1, a_r, a_{r-1}, \dots, a_3, a_2)] \\ &\quad (a_1, a_2, a_3)[(a_1, a_2, \dots, a_r)\tau](a_1, a_3, a_2) \\ &= (a_1, a_r, a_{r-1}, \dots, a_3, a_2)(a_1, a_2, a_3)(a_1, a_2, \dots, a_r) \\ &\quad (a_1, a_3, a_2) \text{ (since } \tau \text{ is disjoint from the others)} \\ &= (a_1, a_3, a_r)\end{aligned}$$

and so  $N$  contains the 3-cycle  $(a_1, a_3, a_r)$  and by Lemma I.6.12,  $N = A_n$ .

## Theorem I.6.10 (continued 3)

**Theorem I.6.10.** The alternating group  $A_n$  is simple if and only if  $n \neq 4$ .

**Proof. Case 4.**  $N$  contains an element  $\sigma$  which is the product of one 3-cycle and some 2-cycles. Say  $\sigma = (a_1, a_2, a_3)\tau$  where  $\tau$  is disjoint from the 3-cycle and  $\tau$  is a product of disjoint 2-cycles. Then  $\sigma^2 \in N$  and

$$\begin{aligned}\sigma^2 &= (a_1, a_2, a_3)\tau(a_1, a_2, a_3)\tau \\ &= (a_1, a_2, a_3)^2\tau^2 \\ &= (a_1, a_2, a_3)^2 \text{ (since } \tau \text{ consists of disjoint transpositions)} \\ &= (a_1, a_2, a_3)\end{aligned}$$

and so  $N$  contains the 3-cycle  $(a_1, a_2, a_3)$ . By Lemma I.6.12,  $N = A_n$ .

## Theorem I.6.10 (continued 2)

**Theorem I.6.10.** The alternating group  $A_n$  is simple if and only if  $n \neq 4$ .

**Proof Case 3.**  $N$  contains an element  $\sigma$  which is the product of disjoint cycles, at least two of which have length 3. So, say,  $\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)\tau$  (where  $\tau$  is disjoint from the two 3-cycles). Then  $(a_1, a_2, a_4) \in A_n$  so denote it  $\delta = (a_1, a_2, a_4)$ . As in Case 2,

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= [\tau^{-1}(a_4, a_6, a_5)(a_1, a_3, a_2)](a_1, a_2, a_4) \\ &\quad [(a_1, a_2, a_3)(a_4, a_5, a_6)\tau](a_1, a_4, a_2) \\ &= (a_1, a_4, a_2, a_6, a_3)\end{aligned}$$

and so  $N$  contains the 5-cycle  $(a_1, a_4, a_2, a_6, a_3)$ . By Case 2,  $N = A_n$ .

## Theorem I.6.10 (continued 4)

**Proof. Case 5.** Every element of  $N$  is the product of an even number of disjoint 2-cycles. Let  $\sigma \in N$  with  $\sigma = (a_1, a_2)(a_3, a_4)\tau$  where  $\tau$  is disjoint from the transpositions and  $\tau$  is a product of an even number of disjoint 2-cycles. Then  $(a_1, a_2, a_3) \in A_n$  so we denote it  $\delta = (a_1, a_2, a_3)$ . Then  $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$  as in Case 2. Now

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= [\tau^{-1}(a_3, a_4)(a_1, a_2)](a_1, a_2, a_3)[(a_1, a_2)(a_3, a_4)\tau](a_1, a_3, a_2) \\ &= (a_1, a_3)(a_2, a_4).\end{aligned}$$

Since  $n \geq 5$ , there is an element  $b$  distinct from  $a_1, a_2, a_3, a_4$ . Since  $\xi = (a_1, a_3, b) \in A_n$  and  $\zeta = (a_1, a_3)(a_2, a_4) \in N$  then  $\zeta(\xi\zeta\xi^{-1}) \in N$  as in Case 2. But

$$\begin{aligned}\zeta(\xi\zeta\xi^{-1}) &= [(a_1, a_3)(a_2, a_4)](a_1, a_3, b)[(a_1, a_2)(a_2, a_4)](a_1, b, a_3) \\ &= (a_1, a_3, b)\end{aligned}$$

and so  $N$  contains the 3-cycle  $(a_1, a_2, b)$ . By Lemma I.6.12,  $N = A_n$ .

## Theorem I.6.10 (continued 5)

**Theorem I.6.10.** The alternating group  $A_n$  is simple if and only if  $n \neq 4$ .

**Proof (continued).** Now to see why at least one of Case 1–5 must hold, we consider writing the elements of  $N$  as disjoint products of cycles. Case 2 describes the situation in which there is a permutation which is the product of disjoint cycles, at least one of which has length 4 or greater. So if Case 2 does not hold, then all elements of  $N$  can be written as a disjoint product of cycles of lengths 2 and 3. Case 5 covers the case where  $N$  contains only permutations consisting of no 3-cycles but only 2-cycles (an even number since  $N \subset A_n$ ). Case 1 covers the case where  $N$  contains a permutation consisting of a single 3-cycle alone. Case 4 covers the case where  $N$  contains a permutation consisting of a single 3-cycle and a bunch of 2-cycles. Case 3 covers the case where  $N$  contains a permutation consisting of two or more 3-cycles. Therefore, in terms of decompositions of permutations into disjoint cycles and with an eye towards 3-cycles, if Case 2 does not hold then at least one of Case 1, 3, 4, 5 must hold.  $\square$

## Theorem I.6.13

**Theorem I.6.13.** For each  $n \geq 3$  the dihedral group  $D_n$  is a group of order  $2n$  whose generators  $a$  and  $b$  satisfy:

- (i)  $a^n = (1)$ ;  $b^2 = (1)$ ;  $a^k \neq (1)$  if  $0 < k < n$ ;
- (ii)  $ba = a^{-1}b$ .

Any group  $G$  which is generated by elements  $a, b \in G$  satisfying (i) and (ii) for some  $n \geq 3$  (with  $e \in G$  in place of (1)) is isomorphic to  $D_n$ .

**Proof.** First, with  $a = (1, 2, \dots, n)$  we have  $a^n = (1)$  and  $a^k \neq (1)$  for  $0 < k < n$ . Next,  $b$  fixes 1 so  $b^2$  fixes 1. For any  $1 < i \leq n$  we have  $b(i) = n + 2 - i$  and so  $b^2(i) = b(n + 2 - i) = n + 2 - (n + 2 - i) = i$ . So  $b^2 = (1)$ . So (i) holds.

## Theorem I.6.13 (continued 1)

**Proof (continued).** Next

$$\begin{aligned}
 ba &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} \\
 &\quad (1, 2, 3, \dots, n-1, n) \\
 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i-1 & \cdots & n-1 & n \\ n & n-1 & n-2 & n-3 & n-4 & \cdots & n+2-i & \cdots & 2 & 1 \end{pmatrix} \\
 &= (n, n-1, \dots, 3, 2, 1) \\
 &\quad \left( \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} \right) = a^{-1}b
 \end{aligned}$$

and (ii) holds.

## Theorem I.6.13 (continued 2)

**Proof (continued).** By Theorem I.2.8,

$$\begin{aligned}
 D_n &= \langle a, b \rangle = \{a^{m_1} b^{m_2} a^{m_3} b^{m_4} \cdots b^{m_k} \mid k \in 2\mathbb{Z}, k > 0, m_i \in \mathbb{Z}\} \\
 &= \{a^i b^j \mid i, j \in \mathbb{Z}\} \text{ by repeated application of (ii)} \\
 &= \{a^i b^j \mid 0 \leq i < n; j = 0, 1\} \text{ by (i)}.
 \end{aligned}$$

Now let  $0 \leq i < n$  and  $j = 0$ . Then  $a^i b^j(1) = a^i(1) = 1 + i$  and  $a^i b^j(2) = a^i(2) = 2 + i$ . For  $0 \leq i < n$  and  $j = 1$ ,  $a^i b^j(1) = a^i b(1) = a^i(1) = 1 + i$  and  $a^i b^j(2) = a^i b(2) = a^i(n) = n + i$ . So if  $i \neq i'$  then  $a^i b^j(1) = 1 + i \neq 1 + i' = a^{i'} b^j(1)$ . If  $j = 0$  and  $j' = 1$  then for any  $i$

$$a^i b^j(2) = a^i(2) = 2 + i \neq n + i = a^i(n) = a^i b^1(2) = a^i b^{j'}(2).$$

So if either  $i \neq i'$  or  $j \neq j'$  then  $a^i b^j$  is different from  $a^{i'} b^{j'}$ . So  $\{a^i b^j \mid 0 \leq i < n; j = 0, 1\}$  consists of  $2n$  permutations and  $|D_n| = 2n$ .

## Theorem I.6.13 (continued 3)

**Proof (continued).** Next, suppose  $G$  is a group generated by  $a, b \in G$  and  $a, b$  satisfy (i) and (ii) for some  $n \geq 3$ . By Theorem I.2.8 and the argument above which uses (i) and (ii), we have that every element of  $G$  is of the form  $a^i b^j$  where  $0 \leq i < n$  and  $j = 0, 1$ . Denote the generators of  $D_n$  by  $a_1$  and  $b_1$  (to avoid confusion with the generators of  $G$ ). Define  $f : D_n \rightarrow G$  as  $f(a_1^i b_1^j) = a^i b^j$ . Then  $f$  is a homomorphism:

$$\begin{aligned} f(a_1^i b_1^j a_1^{i'} b_1^{j'}) &= f(a_1^{i-i'} b_1^{j+j'}) \text{ by (ii)} \\ &= a^{j-i'} b^{j+j'} = a^i b^j a^{i'} b^{j'} \text{ by (ii)} \\ &= f(a_1^i b_1^j) f(a_1^{i'} b_1^{j'}). \end{aligned}$$

Since each element of  $G$  is of the form  $a^i b^j$  where  $0 \leq i < n$  and  $j = 0, 1$  and each element of  $D_n$  is of the form  $a_1^i b_1^j$  where  $0 \leq i < n$  and  $j = 0, 1$ , then  $f$  is onto and  $f$  is an epimorphism.

## Theorem I.6.13 (continued 4)

**Theorem I.6.13.** For each  $n \geq 3$  the dihedral group  $D_n$  is a group of order  $2n$  whose generators  $a$  and  $b$  satisfy:

- (i)  $a^n = (1)$ ;  $b^2 = (1)$ ;  $a^k \neq (1)$  if  $0 < k < n$ ;
- (ii)  $ba = a^{-1}b$ .

Any group  $G$  which is generated by elements  $a, b \in G$  satisfying (i) and (ii) for some  $n \geq 3$  (with  $e \in G$  in place of (1)) is isomorphic to  $D_n$ .

**Proof (continued).** We now show that  $f$  is one to one (i.e., a monomorphism). We use Theorem I.2.3(i) and show that  $\text{Ker}(f) = \{e\} = \{(1)\}$ . Suppose  $a_1^i b_1^j \in \text{Ker}(f)$  or  $f(a_1^i b_1^j) = a^i b^j = e \in G$  with  $0 \leq i < n$  and  $j = 0, 1$ . ASSUME  $j = 1$  then  $a^i = b^{-1} = b$  and by (ii)  $a^{i+1} = a^i a = ba = a^{-1}b = a^{-1}a^i = a^{i-1}$  which implies  $a^2 = e$ . This CONTRADICTS (i) since  $n \geq 3$ . Therefore  $j = 0$  and  $e = a^i b^0 = a^i$  with  $0 \leq i < n$  which implies that  $i = 0$  by (i). Thus  $a_1^i b_1^j = a_1^0 b_1^0 = (1)$ . So  $\text{Ker}(f) = \{(1)\}$  and  $f$  is one to one. Therefore  $f$  is an isomorphism.  $\square$