

# Math 551 – Algebra – Fall 2002

Richard Lyons  
Rutgers University  
New Brunswick, New Jersey, USA

## A. Groups

### 2. Group Actions

#### 2a. Definition of group action

The close connection between groups and permutations is captured in the fundamental idea of group actions. Most natural occurrences of groups, and most techniques for their analysis, derive from the fact that groups act on things.

**Definition-Lemma.** *Let  $G$  be a group and  $\Omega$  a set. A (group) action of  $G$  on  $\Omega$  is defined by either a) or b), which are equivalent:*

a) as a mapping

$$G \times \Omega \rightarrow \Omega, (g, \omega) \mapsto g\omega,$$

such that

1)  $1\omega = \omega$  for all  $\omega \in \Omega$ ;

2)  $g(h\omega) = (gh)\omega$  for all  $g, h \in G$  and all  $\omega \in \Omega$ ; or

b) as a homomorphism  $\phi : G \rightarrow \Sigma_\Omega$ .

Given an action in the sense of a), we may define

$$\phi(g)(\omega) = g\omega \text{ for each } g \in G, \omega \in \Omega.$$

The axioms 1) and 2) yield that  $\phi(g)\phi(h) = \phi(gh)$  and  $\phi(1) = id_\Omega$ , for all  $g, h \in G$ . In particular  $\phi(g)\phi(g^{-1}) = \phi(g^{-1})\phi(g) = \phi(1) = id_\Omega$ , so  $\phi(g) \in \Sigma_\Omega$  for each  $g \in G$ , and we have an action in the sense of b). Conversely, given  $\phi$  as in b), we may define  $g\omega$  by the displayed equation, and the equations  $\phi(g)\phi(h) = \phi(gh)$  and  $\phi(1) = id_\Omega$  yield the axioms 1) and 2) in a).

Group actions are an important source of subgroups:

**Definition.** *If  $G$  acts on  $\Omega$  and  $\omega \in \Omega$ , then the stabilizer of  $\omega$  in  $G$  is*

$$G_\omega = \{g \in G \mid g\omega = \omega\}.$$

It is an quick consequence of the definitions that  $G_\omega \leq G$ .

**Lemma.** If  $G$  acts on  $\Omega$ ,  $g \in G$  and  $\omega \in \Omega$ , then  $G_{g\omega} = {}^g G_\omega = gG_\omega g^{-1}$ .

**Proof.**  $x \in G_\omega$  implies  $(gxg^{-1})g\omega = gx\omega = g\omega$ , so  ${}^g x \in G_{g\omega}$ . Therefore  ${}^g G_\omega \leq G_{g\omega}$ . To get the reverse inclusion apply this this with  $g\omega$  and  $g^{-1}$  in place of  $\omega$  and  $g$ , yielding  ${}^{g^{-1}} G_{g\omega} \leq G_\omega$ , and conjugate by  $g$ .

Some important examples of group actions follow.

**Ex. A.** Let  $G \leq \Sigma_\Omega$ . Then  $G$  acts on  $\Omega$  via  $\sigma\omega = \sigma(\omega)$ .

**Ex. B.** Let  $G$  be a group. Then  $G$  acts on itself via  $gh = gh$ . This is the “left regular” action of  $G$ . There is also a “right regular” action, defined by  $gh = hg^{-1}$ . (The “products” on the left are the results of the action of a group element  $g$  on a set element  $h$ ; on the right, the products are from the multiplication in  $G$ .) In both actions  $G_h = 1$  for every  $h \in G$ .

**Ex. C.** Let  $G$  be a group. Then  $G$  acts on itself via conjugation:  $gx = {}^g x = gxg^{-1} = \text{Int}(g)x$ . This is a group action, with the additional property that for each  $g \in G$ , the mapping  $x \mapsto {}^g x$  is **an automorphism** of  $G$ . For each  $x \in G$ ,  $G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} =: C_G(x)$ , the centralizer of  $x$ .

**Ex. D.** Let  $G$  act on  $\Omega$ . Then there are several “induced” actions on sets associated with  $\Omega$ :

- on  $\mathfrak{P}(\Omega)$ , the set of all subsets of  $\Omega$  ( $g\Psi = \phi(g)(\Psi) = \{g\omega \mid \omega \in \Psi\}$ );
- on  $\Omega \times \Omega$  ( $g(\omega_1, \omega_2) = (g\omega_1, g\omega_2)$ );
- on the set of all equivalence relations on  $\Omega$  ( $\omega_1 [g \sim] \omega_2 \iff g^{-1}\omega_1 \sim g^{-1}\omega_2$ )

**Ex. E.** If  $G$  acts on  $\Omega$ , and  $\sim$  is an equivalence relation on  $\Omega$  which is preserved by  $G$  (i.e., such that  $\omega_1 \sim \omega_2$  implies  $g\omega_1 \sim g\omega_2$  for all  $g \in G$  and  $\omega_1, \omega_2 \in \Omega$ ), then  $G$  acts on the set  $\Omega / \sim$  of equivalence classes by  $g[\omega] = [g\omega]$ ,  $g \in G$ ,  $\omega \in \Omega$ . The preservation assumption ensures that this action is well-defined, and the action axioms are easily verified.

**Ex. F.** Let  $H \leq G$ . Then the left regular action of  $G$  (example B) preserves the equivalence relation  $\sim_H$  ( $x^{-1}y \in H$  implies  $(gx)^{-1}(gy) \in H$  for all  $x, y, g \in G$ ), so by example E  $G$  acts on the set of equivalence classes; in other words,

$$g(xH) = (gx)H \text{ defines an action of } G \text{ on } G/H.$$

## 2b. Transitive actions; counting principle

**Definition.** A group action of  $G$  on  $\Omega$  is transitive if and only if for every  $\omega, \omega' \in \Omega$  there exists  $g \in G$  such that  $g\omega = \omega'$ .

**Exercise.** Let  $G$  act transitively on  $\Omega$  and let  $\phi : G \rightarrow \Sigma_\Omega$  be the associated mapping. Then for any  $\omega \in \Omega$ ,

$$\ker(\phi) = \bigcap_{g \in G} {}^g G_\omega.$$

**Proposition.** *If  $H \leq G$ , then the action of  $G$  on  $G/H$  defined above is transitive, and the stabilizer of the point  $H \in G/H$  is the subgroup  $H$ :  $G_H = H$ .*

**Proof.**  $(g(g')^{-1})g'H = gH$ . Also  $gH = H \iff g \in H$ .  $\square$

It then follows that the stabilizer of  $gH \in G/H$  is  ${}^gH$ . Consequently the kernel of the associated homomorphism  $\phi : G \rightarrow \Sigma_{G/H}$  is

$$\ker \phi = \bigcap_{g \in G} G_{gH} = \bigcap_{g \in G} {}^gH.$$

**Theorem.** *(Classification of transitive actions) Suppose that  $G$  acts transitively on  $\Omega$ . Let  $\omega \in \Omega$  and set  $G_\omega = \{g \in G \mid g\omega = \omega\}$ . Then*

1)  $G_\omega \leq G$ .

2) *There exists a bijection  $\phi : G/G_\omega \rightarrow \Omega$  such that  $\phi(G_\omega) = \omega$  and for every  $g \in G$  and  $\Gamma \in G/G_\omega$ ,*

$$\phi(g\Gamma) = g\phi(\Gamma).$$

Thus the actions of  $G$  on  $G/G_\omega$  and  $\Omega$  are “isomorphic”.

**Proof.** If  $g\omega = \omega = h\omega$ , then  $(gh)\omega = g(h\omega) = g\omega = \omega$ , and also  $g^{-1}\omega = g^{-1}(g\omega) = (g^{-1}g)\omega = 1\omega = \omega$ . This proves 1).

Define  $\Phi : G \rightarrow \Omega$  by  $\Phi(g) = g\omega$ . The transitivity of  $G$  on  $\Omega$  implies that  $\Phi$  is surjective. For any  $g, h \in G$ ,

$$\Phi(g) = \Phi(h) \iff g\omega = h\omega \iff h^{-1}g\omega = \omega \iff h^{-1}g \in G_\omega \iff g \sim_{G_\omega} h.$$

So the fibers of  $\Phi$  are the left cosets of  $G_\omega$ . Therefore  $\Phi$  induces an injective mapping  $\phi : G/G_\omega \rightarrow \Omega$  such that  $\phi(gG_\omega) = \Phi(g) = g\omega$ . Since  $\Phi$  is surjective, so is  $\phi$ , so  $\phi$  is a bijection. Finally for any  $\Gamma = hG_\omega \in G/G_\omega$  we have

$$\phi(g\Gamma) = \phi(g(hG_\omega)) = \phi((gh)G_\omega) = (gh)\omega = g(h\omega) = g\phi(hG_\omega),$$

completing the proof.

**Corollary.** *(The counting principle, transitive case) Let  $G$  act transitively on  $\Omega$ . Then for any  $\omega \in \Omega$ ,*

$$|\Omega| = |G : G_\omega|.$$

**Ex. G.** Let  $I$  be a regular icosahedron and  $G = \text{Aut}(I)$ , the group of all its symmetries. Then  $G$  acts on  $I$ , and in particular on the set  $\Omega$  of the 12 vertices of  $I$ . The action is clearly transitive. The stabilizer  $G_\omega$  of a particular vertex  $\omega$  contains 5 rotations and 5 reflections, which permute the 5 faces containing  $\omega$  in the manner  $D_{10}$  permutes the 5 vertices of a regular pentagon. Therefore  $|G| = |G_\omega||I| = 10 \cdot 12 = 120$ . Furthermore,

$G$  also acts transitively on the set of 20 faces  $F$  (and  $G_F \cong D_6$ ), and on the set of 30 edges (the stabilizer of one being  $D_4 \cong Z_2 \times Z_2$ ).

Conjugation gives lots of examples of transitive actions. Let  $X$  be a subset (such as a subgroup) of  $G$  and let  $\Omega = \{^g X \mid g \in G\}$  be the set of all  $G$ -conjugates of  $X$ . Then  $G$  acts on  $\Omega$  by conjugation:  $g^h X = {}^{gh} X$ . We define  $N_G(X) = \{g \in G \mid {}^g X = X\}$ . This is the stabilizer in  $G$  of the element  $X \in \Omega$ . Thus the counting principle yields:

**Corollary.** *Let  $G$  be a group and  $X$  a subset of  $G$ . Then  $N_G(X)$  is a subgroup of  $G$  and the number of distinct  $G$ -conjugates of  $X$  is  $|G : N_G(X)|$ .*

Taking  $X$  to be a singleton  $X = \{x\}$ , we see that  $N_G(X)$  is the set of all elements of  $G$  which commute with  $x$ . This is called  $C_G(x)$ , the centralizer of  $x$  in  $G$ .

**Corollary.** *Let  $G$  be a group and  $x \in G$ . Then  $C_G(x)$  is a subgroup of  $G$  and the number of distinct  $G$ -conjugates of  $x$  is  $|G : C_G(x)|$ .*

Now we consider not necessarily transitive actions. Let  $G$  act on  $\Omega$ . Define a relation  $\equiv$  on  $\Omega$  by

$$\omega \equiv \omega' \iff \exists g \in G \text{ such that } g\omega = \omega'.$$

By properties 1), 2) and 3) in the definition of group action, this relation is reflexive, transitive and symmetric. So it is an equivalence relation. The equivalence classes are called **orbits**, more precisely **the  $G$ -orbits on  $\Omega$** . Notice that  $G$  acts transitively on each orbit.

**Theorem.** *(Counting principle, general case) Let  $G$  act on  $\Omega$ . Let the set of orbits be  $\{\Omega_i \mid i \in I\}$  and choose for each  $i \in I$  an arbitrary representative element  $\omega_i \in \Omega_i$ . Then*

$$|\Omega| = \sum_i |G : G_{\omega_i}|.$$

**Proof.**  $|\Omega| = \sum_i |\Omega_i| = \sum_i |G : G_{\omega_i}|$ , the first since the orbits partition  $\Omega$ , and the second by the transitive case of the counting principle.

**Exercise.** *Let  $V$  be a 4-dimensional vector space over a field  $k$ , and let  $G = GL(V)$ . Let  $\Omega$  be the set of all 2-dimensional subspaces of  $V$ .*

- a) *Show that  $G$  acts transitively on  $\Omega$ .*
- b) *Let  $W$  be a 2-dimensional subspace of  $V$ . Describe the subgroup  $G_W$  (choose an appropriate basis of  $V$  and identify which matrices lie  $G_W$ ).*
- c) *Describe the orbits of  $G_W$  on  $\Omega$ .*

## 2c. Class equation of a finite group; actions of groups of prime power order

An interesting application is the “class equation” of a group. Let  $G$  be any group, and consider  $G$  to act on itself by conjugation. The action is certainly not transitive (unless

$G = 1$ ), since  $\{1\}$  is an orbit. The orbits of this action are called the **conjugacy classes** of  $G$ . If  $C$  is a conjugacy class and  $x \in C$  then  $|C| = |G : C_G(x)|$  by the previous corollary. Thus if we choose a set of representatives  $\{g_i \mid i \in I\}$  for the conjugacy classes (i.e., a subset of  $G$  which consists of one element from each conjugacy class), the counting principle yields

$$|G| = \sum_{i \in I} |G : C_G(g_i)|.$$

It is customary to separate out the terms in this sum which are equal to 1; i.e., those for which  $C_G(g_i) = G$ . This condition is equivalent to  $g_i$  not having any conjugates in  $G$  other than itself, which is equivalent to  $g_i x = x g_i$  for all  $x \in G$ , i.e.,  $x \in Z(G)$ . Thus  $Z(G)$  consists of all the elements contributing 1 to the sum above. We have proved

**Theorem.** (*The Class Equation*) *Let  $G$  be a finite group. Then*

$$|G| = |Z(G)| + \sum_j |G : C_G(g_j)|,$$

where the sum is over a set of representatives for all the conjugacy classes of  $G$  except those in  $Z(G)$ . (Thus  $|G : C_G(g_j)| > 1$  for each term in the sum.)

This has important consequences for finite groups; one cute one is the following:

**Theorem.** *Let  $G$  be a group such that  $|G|$  is a positive power of a prime. Then  $Z(G) \neq \{1\}$ .*

**Proof.** Let  $p$  be the prime. In the class equation,  $|G|$  as well as each term  $|G : C_G(g_j)|$  is a positive power of  $p$ , by Lagrange's Theorem. Therefore  $|Z(G)| \equiv 0 \pmod{p}$ . Certainly  $1 \in Z(G)$  so  $|Z(G)| \geq p$ . QED

Before giving an application of this we observe that virtually the same argument proves the following:

**Theorem.** *Let  $G$  be a finite group of order  $p^a$ ,  $p$  a prime, and suppose that  $G$  acts on the finite set  $\Omega$ . Define  $\text{Fix}_\Omega(G) = \{\omega \in \Omega \mid g\omega = \omega \ \forall g \in G\}$ . Then*

$$|\text{Fix}_\Omega(G)| \equiv |\Omega| \pmod{p}.$$

QED

Now for an application:

**Corollary.** *Let  $G$  be a group whose order is  $p^2$ ,  $p$  a prime. Then  $G$  is abelian (and is isomorphic either to  $Z_p \times Z_p$  or to  $Z_{p^2}$ ).*

**Proof.** We prove that  $G$  is abelian, i.e.,  $Z(G) = G$ , and leave the rest as an exercise. Assume by way of contradiction that  $Z(G) < G$ . We can choose  $g \in Z(G)$  with  $g \neq 1$  by

the theorem, and choose  $h \in G - Z(G)$ . Then  $|\langle g \rangle| = p$  and as  $\langle g, h \rangle$  properly contains  $\langle g \rangle$  and has order which divides  $p^2$ ,

$$G = \langle g, h \rangle.$$

But  $gh = hg$  and it quickly follows that any word in  $g$  and  $h$  commutes with any other, so that  $G$  is abelian.  $\square$

## 2d. Sylow's Theorem

A natural question is whether Lagrange's Theorem has a converse: i.e., given a group  $G$  and a divisor  $n$  of  $|G|$ , does  $G$  have a subgroup of order  $n$ ? The answer is definitely negative in general. As an example the symmetric group  $\Sigma_5$  has no subgroup  $H$  of order 30. Proof: if it did the action of  $\Sigma_5$  on  $\Sigma_5/H$  would yield a homomorphism  $\Sigma_5 \rightarrow \Sigma_{\Sigma_5/H} \cong \Sigma_4$ , whose kernel  $K$  would be the intersection of all the conjugates of  $H$ . In particular  $K \leq H$  and so  $|K| \leq 30$ . On the other hand,  $\Sigma_4$  has no element of order 5, so each element of  $x \in \Sigma_5$  of order 5 must satisfy  $\phi(x) = 1$  and hence lie in  $K$ . Hence  $K$  contains all 24 5-cycles of  $\Sigma_5$ . Then  $K$  contains  $(abcde)(acbde) = (ad)(ce)$  for all 5-cycles  $(abcde)$ , giving an additional 15 elements in  $K$ , which is absurd.

The best partial converse to Lagrange's Theorem is Sylow's Theorem; we begin with a baby version.

**Theorem 1.** *Let  $G$  be a finite group, and let  $p$  be a prime divisor of  $|G|$ . Then  $G$  possesses an element of order  $p$ .*

**Proof.** Define

$$\Omega = \{(g_1, g_2, \dots, g_p) \mid g_i \in G \ \forall i = 1, \dots, p \text{ and } g_1 g_2 \cdots g_p = 1\}.$$

Notice that this condition is equivalent to

$$g_p = (g_1 \cdots g_{p-1})^{-1},$$

and so for each  $g_1, \dots, g_{p-1} \in G$ , there is a unique  $p$ -tuple in  $\Omega$  starting with  $g_1, \dots, g_{p-1}$ . Therefore

$$|\Omega| = |G|^{p-1}.$$

Now let  $H = \langle h \rangle$  be a cyclic group of order  $p$ , and let  $H$  act on  $\Omega$  by  $h^i(g_1, g_2, \dots, g_p) = (g_{i+1}, g_{i+2}, \dots, g_{i+p})$ , where we interpret subscripts as having been reduced to their residue modulo  $p$  in the range between 1 and  $p$ . It is easy to check that this defines an action of  $H$  on  $\Omega$ . Therefore by the previous theorem,

$$\text{Fix}_\Omega(H) \equiv |\Omega| = |G|^{p-1} \equiv 0 \pmod{p}.$$

Notice that  $(1, 1, \dots, 1)$  is a fixed point of  $H$ , and so there exists another fixed point  $(z_1, z_2, \dots, z_p)$ . Since this point is fixed, we have  $z_1 = z_2 = \cdots = z_p$ . Therefore  $z_1 \neq 1$ , and the definition of  $\Omega$  yields  $z_1^p = 1$ .  $\square$

Using the class equation and quotient groups, we can prove the existence part of the full Sylow theorem.

**Definition.** Let  $G$  be a finite group and  $p$  a prime. Write  $|G| = p^a b$  with  $p$  not dividing  $b$ . Then a subgroup  $P$  of  $G$  is a Sylow  $p$ -subgroup of  $G$  if and only if  $|P| = p^a$ . We put

$$\text{Syl}_p(G) = \{P \mid P \text{ is a Sylow } p\text{-subgroup of } G\}.$$

**Theorem 2.** Let  $G$  be a finite group and  $p$  a prime. Then  $G$  possesses a Sylow  $p$ -subgroup.

**Proof.** The proof is by induction on  $|G|$ . The case  $|G| = 1$  (or even  $a = 0$ ) is trivial. Assume then that  $a > 0$  and consider the class equation of  $G$ . There are two cases.

Case 1. Some term  $|G : C_G(g_i)|$  is not divisible by  $p$ . Then  $|C_G(g_i)| = p^a b'$ . Since  $|G : C_G(g_i)| > 1$  (this is the way the class equation is sorted out), induction implies that  $C_G(g_i)$  has a Sylow  $p$ -subgroup, which is then a Sylow  $p$ -subgroup of  $G$ .

Case 2.  $|G : C_G(g_i)| \equiv 0 \pmod{p}$  for all  $i$ . Since  $a > 0$ ,  $|G| \equiv 0 \pmod{p}$ , and so  $|Z(G)| \equiv 0 \pmod{p}$ . By the previous theorem,  $Z(G)$  contains an element  $x$  of order  $p$ . Set  $H = \langle x \rangle$ . Then  $|H| = p$  and  $H \triangleleft G$ . The group  $\overline{G} = G/H$  has order  $|G : H| = |G|/p = p^{a-1}b$  so by induction has a subgroup  $\overline{P}$  of order  $p^{a-1}$ . Set  $P = \{g \in G \mid gH \in \overline{P}\} = \pi_H^{-1}(\overline{P})$ . A routine argument shows that  $P \leq G$  and  $|P| = |H||\overline{P}| = p^a$ . □ QED

The remaining parts of Sylow's Theorem all concern

the action of  $G$  on  $\text{Syl}_p(G)$  by conjugation

and depend on the following exercise:

**Exercise.** Let  $H, K \leq G$ . Then  $HK \leq G$  if and only if  $HK = KH$ . Moreover, if  $H$  and  $K$  are finite then  $|HK||H \cap K| = |H||K|$ .

**Lemma.** Suppose that  $Q \leq G$ ,  $|Q| = p^r$  for some  $r$ , and  $P \in \text{Syl}_p(G)$ . Then  $Q$  fixes  $P$  (by conjugation) if and only if  $Q \leq P$ . Moreover if  $Q \in \text{Syl}_p(G)$ , then  $Q$  fixes  $P$  if and only if  $Q = P$ .

**Proof.** Obviously if  $Q \leq P$ , then for any  $g \in Q$ ,  $gP = P$ . Conversely if this equation holds, then  $gP = Pg$  for all  $g \in Q$ . Therefore  $QP = PQ$ . By the exercise, this implies that  $QP \leq G$ , and  $|QP| = |Q||P|/|Q \cap P|$  is a power of  $p$ . Since  $P \leq QP$  and  $|P| = p^a$ , this forces  $P = QP$ , whence  $Q \leq P$ . This proves the first statement. The second follows immediately since any two Sylow  $p$ -subgroups of  $G$  have the same size. □ QED

Now we are ready for:

**Sylow's Theorem.** Let  $G$  be a finite group and  $p$  a prime. Then

- 1)  $\text{Syl}_p(G) \neq \emptyset$ .
- 2) Any two elements of  $\text{Syl}_p(G)$  are conjugate.
- 3)  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$ .
- 4) For any  $P \in \text{Syl}_p(G)$ ,  $|\text{Syl}_p(G)| = |G : N_G(P)|$ .

5) Any subgroup of  $G$  whose order is a power of  $p$  lies in some element of  $\text{Syl}_p(G)$ .

**Proof.** Theorem 2 is part 1). Fix  $P \in \text{Syl}_p(G)$  and consider the action of  $P$  on  $\text{Syl}_p(G)$  by conjugation. By the lemma, there is a unique orbit of length 1; by the counting principle the other orbits have length divisible by  $p$ . Therefore  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$ , which is 3). In fact, let  $\Omega$  be any  $G$ -orbit (by conjugation) on  $\text{Syl}_p(G)$ , and consider the action of  $P$  on  $\Omega$ . If  $P \in \Omega$ , the same argument shows that  $|\Omega| \equiv 1 \pmod{p}$ . If  $P \notin \Omega$ , the same argument shows that  $|\Omega| \equiv 0 \pmod{p}$ . But the argument may be repeated, in the latter case, for any  $Q \in \Omega$ , and yields  $|\Omega| \equiv 1 \pmod{p}$ , contradiction. Therefore it is impossible that  $P \notin \Omega$ . Hence  $\Omega = \text{Syl}_p(G)$ , proving 2). The counting principle then implies 4). As for 5), consider the action of  $Q$  on  $\text{Syl}_p(G)$ . Every orbit has length 1 or length divisible by  $p$ . By 3), there must be an orbit  $\{R\}$  of length 1,  $R \in \text{Syl}_p(G)$ . By the lemma,  $Q \leq R$ .  $\square$

This unassuming result is unmatched for power in all of finite group theory.

As an example of its use we show:

**Proposition.** *There two isomorphism types of groups of cardinality 6, namely  $Z_6$  and  $\Sigma_3$ .*

**Proof.** These two groups of order 6 are not isomorphic since  $Z_6$  is abelian and  $\Sigma_3$  is not. Now let  $G$  be any group of order 6. We must show that either  $G \cong Z_6$  or  $G \cong \Sigma_3$ . Let  $P \in \text{Syl}_3(G)$ . By Sylow's theorem the number of Sylow 3-subgroups is  $|G : N_G(P)|$ , which divides  $|G : P| = 2$  and is congruent to 1 mod 3. Therefore  $P$  is the unique Sylow 3-subgroup, so  ${}^gP = P$  for all  $g \in G$ , i.e.  $P \triangleleft G$ . We have  $P = \langle x \rangle$  for some  $x \in G$  of order 3. Thus conjugation induces a homomorphism  $G \rightarrow \text{Aut}(P)$ ,  $g \mapsto \text{Int}(g)|_P$ . Notice that  $\text{Aut}(P) \cong Z_2$ ; the only nontrivial automorphism of  $P$  inverts every element of  $P$ .

Likewise by Sylow's Theorem there exists  $y \in G$  of order 2.

Thus we have  $x^3 = 1$ ,  $y^2 = 1$  and

$$\text{either } {}^yx = x \text{ or } {}^yx = x^{-1}.$$

In the first case  $(xy)^6 = x^6y^6 = 1$ , but  $(xy)^3 = y^3 = y \neq 1$  and  $(xy)^2 = x^2 \neq 1$ , so  $xy$  has order 6 and  $G \cong Z_6$ . In the second case, we have  $yx = x^{-1}y$ . But we showed above that the symmetry group  $D_6$  of an equilateral triangle a) has elements  $\sigma$  and  $\tau$  satisfying the same relations and b) as a result of these relations and nothing else, can be shown to consist of the elements  $\tau^i\sigma^j$ ,  $0 \leq i \leq 1$ ,  $0 \leq j \leq 2$ , and have a uniquely determined multiplication table. Therefore  $G \cong D_6$ . In particular taking  $G = \Sigma_3$ , a noncyclic group of order 6, we have  $\Sigma_3 \cong D_6$ .  $\square$

Essentially the same argument proves:

**Corollary.** *Let  $p$  and  $q$  be primes, with  $p > q$ . If  $p \not\equiv 1 \pmod{q}$ , then every group of order  $pq$  is cyclic. If  $p \equiv 1 \pmod{q}$ , then there are two isomorphism classes of groups of order  $pq$ , represented by  $Z_{pq}$  and a group  $G = \langle x, y \rangle$  with  $x^p = y^q = 1$  and  ${}^yx = x^i$ , where  $i$  is an integer such that  $i^q \equiv 1 \pmod{p}$ .*

**Proof.** Let  $G$  have order  $pq$ . Let  $P \in \text{Syl}_p(G)$  and  $Q \in \text{Syl}_q(G)$ . Choose generators  $x$  and  $y$  of  $P$  and  $Q$  respectively. Then  $|\text{Syl}_p(G)|$  divides  $q$  and is congruent to 1 mod  $p$ , so  $P \triangleleft G$  as  $q < p$ . Therefore we again get a homomorphism  $\phi : Q \rightarrow (\mathbf{Z}/p\mathbf{Z})^\times$ , the composite

$$Q \rightarrow \text{Aut}(P) \cong \text{Aut}(\mathbf{Z}_p) \cong (\mathbf{Z}/p\mathbf{Z})^\times$$

such that  $\phi(y) = [i]$ , where  ${}^y x = x^i$ . Thus we have

$$x^p = y^q = 1, {}^y x = x^i.$$

Moreover,  $1 = \phi(y^q) = [i]^q$  so  $i^q \equiv 1 \pmod{p}$ . If  $[i] = [1]$ , then  $xy = yx$  and  $G$  is cyclic as before. So we may assume that  $[i] \neq [1]$ . Then as  $Q$  has prime order,  $\ker \phi = 1$ , so  $\text{im } \phi$  is a subgroup of order  $q$ , whence  $q|p-1$  by Lagrange's Theorem, i.e.,  $p \equiv 1 \pmod{q}$ . This completes the proof if  $p \not\equiv 1 \pmod{q}$ .

To complete the proof, assume that  $p \equiv 1 \pmod{q}$ . We need to use the fact that in the group  $(\mathbf{Z}/p\mathbf{Z})^\times$ , there are exactly  $q$  solutions  $[i]$  of the equation  $[i]^q \equiv 1$ .

That there are as many as  $q$  holds by Sylow's Theorem for  $q$ . That there are no more holds since the polynomial  $t^q - 1$ , like any polynomial of degree  $q$  over any field, has at most  $q$  distinct roots in  $\mathbf{Z}/p\mathbf{Z}$ .

These  $q$  solutions form a (the) subgroup of  $(\mathbf{Z}/p\mathbf{Z})^\times$  of order  $q$ , so form the image of  $\phi$ . Therefore if we fix  $[i_0] \in \mathbf{Z}/p\mathbf{Z}$  such that  $i_0^q \equiv 1 \not\equiv 1 \pmod{p}$ , we may replace  $y$  by a suitable generator of  $\langle y \rangle$  in order to arrange that  ${}^y x = x^{i_0}$ . Then the relations  $x^p = y^q = 1$  and  ${}^y x = x^{i_0}$  determine in the usual way that every element of  $G$  has the form  $x^k y^j$  for unique  $0 \leq j < q$  and  $0 \leq k < p$ , and the multiplication table of  $G$  is uniquely determined:  $x^k y^j x^m y^\ell = x^{k+m i_0^j} y^{j+\ell}$ , with exponents reduced modulo  $p$ . Hence there are at most two isomorphism classes for  $G$ .

The only remaining point is to verify that a nonabelian group of order  $pq$  actually exists when  $p \equiv 1 \pmod{q}$ . Using the element  $[i_0] \in \mathbf{Z}/p\mathbf{Z}$  of multiplicative order  $q$ , we may realize such a group as the multiplicative group

$$\left\{ \left[ \begin{array}{cc} [i_0]^j & [a] \\ 0 & [i_0]^{-j} \end{array} \right] \mid 0 \leq j < q, [a] \in \mathbf{Z}/p\mathbf{Z} \right\}.$$

□

## 2e. Finite Symmetric Groups

Examples illustrating the previous results can be found in the symmetric groups. We have already been using standard notation for them, in particular the "product of cycles" notation for permutations. The notation

$$(12357)(46)$$

for example refers to the permutation in  $\Sigma_7$  taking 1 to 2, 2 to 3, 3 to 5, 5 to 7, and 7 to 1, and interchanging 4 and 6. Such notation is possible for any permutation in any symmetric group. We shall prove this intuitively obvious fact since in doing so we pass by some other useful concepts.

**Let**  $g \in \Sigma_\Omega$ . Let  $\Omega_1$  be an orbit of  $\langle g \rangle$  on  $\Omega$ , and suppose that  $|\Omega_1| = n$ . Then for any  $\omega \in \Omega_1$ , we have

$$\Omega_1 = \{\omega, g\omega, g^2\omega, \dots, g^{n-1}\omega\}.$$

**Proof.** For any  $\alpha \in \Omega$ ,  $\alpha = g^i\omega$  for some  $i$ , by transitivity. Moreover  $\alpha = g^j\omega$  if and only if  $g^{i-j} \in \langle g \rangle_\omega$ . Now  $G_\omega = \langle g^n \rangle$  for some  $n$ , and we may assume that  $n$  is the least positive integer with this property. Then we may write  $\alpha = g^i\omega$  with  $0 \leq i < n$ , and different such  $i$  give different  $g$ 's.

Alternatively we may quote the classification of transitive actions, which says that there is a bijection  $\Omega_1 \rightarrow \langle g \rangle / \langle g \rangle_\omega$  preserving the action of  $\langle g \rangle$  and mapping  $\omega$  to the trivial coset  $\langle g \rangle_\omega$ . Writing  $G_\omega = \langle g^n \rangle$  with  $n$  again the least such positive integer, we see that  $1, g, g^2, \dots, g^{n-1}$  represent the left cosets of  $\langle g \rangle$ . This implies the result. □

We write  $g|\Omega_1$  as the “ $n$ -cycle”

$$g|\Omega_1 = (\omega \ g\omega \ g^2\omega \ \dots \ g^{n-1}\omega). \quad 2A$$

**Definition.** A permutation  $g \in \Sigma_\Omega$  is a cycle if and only if  $\langle g \rangle$  has one orbit  $\Omega_1$  on which it acts by (2A), with  $n > 1$ , and  $g$  fixes every point of  $\Omega - \Omega_1$ .

Thus we do not consider the identity permutation to be a cycle.

We may use the same notation for the cycle  $g$ , with the convention that points of  $\Omega$  omitted in this symbolism are fixed by  $g$ .

**Definition.** Two permutations  $g, g' \in \Sigma_\Omega$  are disjoint if and only if each point of  $\Omega$  is fixed by at least one of them.

**Lemma.** If  $g$  and  $g'$  are disjoint permutations then  $gg' = g'g$ , and points in the support of  $g$  are moved by  $gg'$  just as they are moved by  $g$ .

**Proof.** Left to reader. □

Now we can prove

**Theorem.** Let  $g \in \Sigma_\Omega$ , with  $\Omega$  finite. Then there exist uniquely determined disjoint cycles  $g_1, \dots, g_r$  (except for their order) such that  $g = g_1 \dots g_r$ .

**Proof.** Let  $\Omega_1, \dots, \Omega_r$  be the nontrivial orbits of  $\langle g \rangle$  on  $\Omega$ , and let  $g_i$  be the permutation which agrees with  $g$  on  $\Omega_i$  and acts trivially on all other  $\Omega_j$ . Then  $g_i$  is a cycle by the first lemma, the  $g_i$  are obviously disjoint and  $g = g_1 \dots g_r$ . Conversely if  $g = h_1 \dots h_s$ , disjoint cycles, and we let  $\Omega'_i$  be the nontrivial orbit of  $h_i$  on  $\Omega$ , then it is clear that the  $\Omega'_i$  are the nontrivial orbits of  $g$  on  $\Omega$ , so that by reordering we have  $r = s$  and  $\Omega_i = \Omega'_i$ . Then  $h_i = g|\Omega_i = g_i$ . □

**Lemma.** *The order of an  $n$ -cycle is  $n$ . If  $g = g_1 \cdots g_r$  as in the previous theorem, with  $g_i$  being an  $n_i$ -cycle, then the order of  $g$  is the l.c.m. of  $n_1, \dots, n_r$ . □*

**Theorem.** *Two elements of  $\Sigma_\Omega$ ,  $\Omega$  finite, are conjugate in  $\Sigma_\Omega$  if and only if they have the same cycle shape.*

**Proof.** If  $h\alpha = \beta$ , then  $ghg^{-1}(g\alpha) = g\beta$ . Hence if  $h = (\alpha\beta\cdots)(\gamma\delta\cdots)\cdots$ , then  $ghg^{-1} = (g\alpha g\beta\cdots)(g\gamma g\delta\cdots)\cdots$ . So conjugate elements have the same cycle shape; conversely if two elements have the same cycle shape a permutation  $g$  exists carrying the points in one cycle shape to corresponding points in the other. □

Now of the  $3!$  elements of  $\Sigma_3$ , there are 2 3-cycles, 3 2-cycles and 1 identity element.

Of the  $4! = 24$  elements of  $\Sigma_4$ , there are 6 4-cycles, 8 3-cycles, 6 2-cycles, 3 elements of the form  $(ab)(cd)$ , and one identity element. The last four elements constitute the “Klein four-subgroup  $V = \{1, (12)(34), (13)(24), (14)(23)\}$ ”.

Of the  $5! = 120$  elements of  $\Sigma_5$ , there are 24 5-cycles, 30 4-cycles, 20 3-cycles, 10 2-cycles, 15 “Klein elements”  $(ab)(cd)$ , and 20 elements  $(abc)(de)$  of order 6.

It is not possible systematically to enumerate the subgroups of  $\Sigma_n$ ; if this were possible we would know all finite groups, by Cayley’s Theorem. However, there are very few subgroups of very small index. Taking  $\Omega = \{1, \dots, n\}$ , we of course have the point-stabilizers  $(\Sigma_\Omega)_\omega$ ,  $\omega \in \Omega$ ; clearly this is isomorphic to  $\Sigma_{\Omega - \{\omega\}}$  and its index is  $|\Omega| = n$ . The only other subgroup of index  $\leq n$  is the alternating group  $A_\Omega$ .

2-cycles are also called “transpositions”.

**Theorem.** *Let  $\Omega$  be a finite set. Then every element  $g \in \Sigma_\Omega$  is the product  $g = t_1 \cdots t_r$  of (not necessarily disjoint) transpositions. This decomposition is not unique, nor is  $r$ . However, the parity of  $r$  is uniquely determined by  $g$ , and accordingly  $g$  is called even or odd, and the sign  $\epsilon_g$  of  $g$  is defined as 1 or  $-1$ , respectively.*

**Proof.**  $(\alpha_1 \alpha_2 \cdots \alpha_r)(\alpha_r \alpha_{r+1}) = (\alpha_1 \alpha_2 \cdots \alpha_r \alpha_{r+1})$ . Hence an inductive argument shows that every cycle is the product of transpositions. But every element of  $\Sigma_\Omega$  is the product of cycles, proving the first statement.

For the uniqueness, we define  $o(x)$ , for  $x \in \Sigma_\Omega$ , to be the number of orbits (counting trivial orbits) of  $\langle x \rangle$  on  $\Omega$ . Thus  $x$  is the product of  $o(x)$  disjoint cycles (counting 1-cycles). The uniqueness follows immediately from the following lemma:

**Lemma.** *Let  $x \in \Sigma_\Omega$ , and let  $t$  be a transposition in  $\Sigma_\Omega$ . Then  $o(tx) \not\equiv o(x) \pmod{2}$ .*

Indeed this immediately implies that  $o(t_1 \cdots t_n) \equiv n + o(1) \pmod{2}$  if  $t_1, \dots, t_n$  are transpositions. Then if  $t_1 \cdots t_n = u_1 \cdots u_m$ , with the  $t$ ’s and  $u$ ’s all being transpositions, then  $n + o(1) \equiv m + o(1) \pmod{2}$ , so  $n \equiv m \pmod{2}$ .

The lemma follows directly from the easily computable facts that

$$\begin{aligned} (a_1 \cdots a_n b_1 \cdots b_m) \cdot (a_1 b_1) &= (a_1 b_2 \cdots b_m)(b_1 a_2 \cdots a_n) \text{ and} \\ (a_1 \cdots a_n)(b_1 \cdots b_m) \cdot (a_1 b_1) &= (a_1 b_2 \cdots b_m b_1 a_2 \cdots a_n) \end{aligned}$$

so that the number of disjoint cycles changes by one in either case.  $\square$

An alternative proof of uniqueness uses a natural representation of  $G = \Sigma_\Omega$ . Say  $\Omega = \{1, \dots, n\}$ . Let  $R = \mathbf{Z}[x_1, \dots, x_n]$  be the polynomial ring in  $n$  (commuting) indeterminates  $x_1, \dots, x_n$ . The action of  $G$  on  $\Omega$  yields an action of  $G$  on  $R$ :

$$\text{For } g \in G \text{ and } p \in R, \text{ define } (g \cdot p)(x_1, \dots, x_n) = p(x_{g^{-1}1}, \dots, x_{g^{-1}n}). \quad 2B$$

If we put  $q = g \cdot p$ , notice that  $h \cdot (g \cdot p)(x_1, \dots) = (h \cdot q)(x_1, \dots, x_n) = q(x_{h^{-1}1}, \dots) = p(x_{g^{-1}h^{-1}1}, \dots) = (hg) \cdot p(x_1, \dots, x_n)$ . (For  $i = h^{-1}1$  gets replaced by  $g^{-1}i = g^{-1}h^{-1}1$ , etc.) Thus

$$h \cdot (g \cdot p) = (hg) \cdot p, \quad 2C$$

whence we really have an action. Moreover, the multiplication in  $R$  is respected by this action:

$$g \cdot (pq) = (g \cdot p)(g \cdot q), \quad 2D$$

where the products are in the ring  $R$ , i.e., ordinary multiplication of polynomials. This is clear from the definition of the action.

What has this to do with even and odd permutations? The polynomial ring  $R$  contains an element  $\delta$  which “detects” evenness and oddness, namely

$$\delta(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j).$$

The key point is that if  $t$  is a transposition, then

$$t \cdot \delta = -\delta. \quad 2E$$

Indeed  $t$  permutes and changes the signs of the factors of  $\delta$ , and so  $t \cdot \delta = \pm\delta$ , where the sign is determined by whether the phenomenon  $i < j$  but  $ti > tj$  occurs an even or odd number of times. But if  $t$  interchanges  $k$  and  $l$  with  $k < l$ , then this phenomenon occurs only if  $i = k$  and  $j = l$ , or  $i = k$  and  $k < j < l$ , or  $j = l$  and  $k < i < l$ . This is an odd number of times, proving (2E).

Now (2C, D, E) imply that if  $g$  is the product of  $r$  transpositions, then

$$g\delta = (-1)^r \delta.$$

Thus we may define  $\epsilon_g$  by  $g\delta = \epsilon_g \delta$ , and the proof is complete.  $\square$

**Definition.**  $A_\Omega$  is the subgroup of  $\Sigma_\Omega$  consisting of all even permutations.

Thus  $\Sigma_\Omega = A_\Omega \cup A_\Omega t$  for any transposition  $t$ , so

$$|\Sigma_\Omega : A_\Omega| = 2$$

and  $A_\Omega \triangleleft \Sigma_\Omega$ .

In particular  $A_3 = \langle (123) \rangle \cong \mathbf{Z}_3$ . Also  $A_4$  has order 12, and has four Sylow 3-subgroups (exhausting the set of 8 elements of order 3). In addition the three elements of  $A_4$  of shape  $(ab)(cd)$  have order 2 and have the property that the product of any two distinct ones is the third one; so they form a subgroup  $V \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ , and

$$V \triangleleft \Sigma_4.$$

( $V$  can also be understood in the following only slightly different way. A set  $\Omega$  with 4 elements can be divided in half in exactly 3 ways. Let  $\Psi$  be the set of these three partitions of  $\Omega$ . Then  $\Sigma_\Omega$  obviously acts on  $\Psi$ ; indeed it acts transitively. We then get a homomorphism

$$\phi : \Sigma_\Omega \rightarrow \Sigma_\Psi$$

whose kernel is the set of all  $g \in \Sigma_\Omega$  leaving invariant each of the three partitions. It is easily checked that  $\ker \phi$  is exactly  $V$ , after identifying  $\Sigma_\Omega$  with  $\Sigma_4$ .)

The alternating and symmetric groups are highly non-abelian. For instance,  $A_4$  has no subgroup of order 6. One way to see this is to use Sylow's Theorem (applied to the presumed subgroup of order 6), and show that no elements of order 2 and 3 in  $A_4$  can generate a subgroup of order 6. Another is to assume that such a subgroup  $H$  exists, let  $P$  be a Sylow 3-subgroup of  $H$ . Then  $P$  is a Sylow 3-subgroup of  $A_4$ , and there are four of them, so  $|A_4 : N_{A_4}(P)| = 4 = |A_4 : P|$ , whence  $N_G(P) = P$ . On the other hand,  $|H : P| = 2$  so by Sylow's Theorem  $|H : N_H(P)|$  can only be 1, as it is 1 mod 3. Therefore  $H = N_H(P) \leq N_G(P) = P$ , a contradiction.

A fundamental fact about the alternating groups  $A_n$  is that they are simple for  $n \geq 5$ , and the only nontrivial normal subgroup of  $\Sigma_n$  is  $A_n$  (except for  $n = 4$ ;  $\Sigma_4$  has precisely two nontrivial normal subgroups,  $A_4$  and  $V$ ).

**Theorem.** *Suppose that  $n \geq 5$ . Then  $A_n$  is simple.*

**Corollary.** *Suppose that  $n \geq 5$ . Then the only nontrivial normal subgroup of  $\Sigma_n$  is  $A_n$ .*

A standard approach to proving this theorem is a) show that  $A_n$  is generated by all its 3-cycles (note that we can't use 2-cycles since they are odd permutations); b) show that all 3-cycles in  $A_n$  are conjugate in  $A_n$ ; c) show that if  $1 < N \triangleleft A_n$ , then an element of  $N$  whose support has minimum size is a 3-cycle. Then by c) and b),  $N$  contains all 3-cycles, so equals  $G$ , as desired. The dirtiest part of this is c), where one produces from an element  $g \in A_n$  which is not a 3-cycle another non-identity element  $h \in A_n$  which has smaller support, but is the product of powers of  $g$  and their conjugates.

Instead we give an inductive proof, still using the action of  $A_n$  on  $\Omega = \{1, \dots, n\}$  of course. This is a transitive action for which the stabilizer of a point is isomorphic to  $A_{n-1}$ .

To start the induction, observe that  $A_5$  has 15 "Klein" elements (those of shape  $(ab)(cd)e$ ), and they are all conjugate in  $A_5$ .  $A_5$  also has 20 3-cycles, and they too are all conjugate in  $A_5$ .  $A_5$  has 24 5-cycles, each of which is self-centralizing and so lies in a conjugacy class of size  $|A_5|/5 = 12$ . The class equation for  $A_5$  is therefore

$$60 = 1 + 15 + 20 + 12 + 12.$$

Now a normal subgroup  $N$  of  $A_5$  must consist of the identity and some of the other conjugacy classes, so  $|N|$  is a subsum of the above sum, containing the term 1. But no such subsum divides 60, other than the full sum or 1. Therefore  $N = 1$  or  $N = A_5$ .

For the induction step, we need to check that for  $n \geq 6$ , the action of  $A_n$  on  $\{1, \dots, n\}$  is 4-transitive in the following sense.

**Definition.** Let  $G$  act on  $\Omega$  with  $|\Omega| \geq 4$ . Then  $G$  acts 4-transitively if and only if for any quadruple  $(\alpha, \beta, \gamma, \delta) \in \Omega \times \Omega \times \Omega \times \Omega$  such that  $\alpha, \beta, \gamma, \delta$  are pairwise distinct, and for any other such quadruple  $(\alpha', \beta', \gamma', \delta')$ , there is  $g \in G$  such that  $g\alpha = \alpha'$ ,  $g\beta = \beta'$ ,  $g\gamma = \gamma'$ , and  $g\delta = \delta'$ .

One may similarly define  $n$ -transitivity (if  $|\Omega| \geq n$ ), using  $n$ -tuples instead of quadruples.

**Lemma.** If  $G$  acts  $n$ -transitively on  $\Omega$ , then for each  $\omega \in \Omega$ ,  $G_\omega$  acts  $n - 1$ -transitively on  $\Omega - \{\omega\}$ .

**Proof** Left to reader.

**Lemma.** For  $n \geq 6$ ,  $A_n$  acts 4-transitively on  $\{1, \dots, n\}$ .

**Proof**  $\Sigma_n$  certainly does, and if  $g$  is taken in  $\Sigma_n$  and is odd, then  $g' = g\tau$  works just as well, where  $\tau$  is a transposition fixing  $\alpha, \beta, \gamma, \delta$ .

A group action of  $G$  on  $\Omega$  is called faithful if and only if the kernel of the corresponding mapping  $G \rightarrow \Sigma_\Omega$  is trivial. The action of  $A_n$  on  $\{1, \dots, n\}$  is certainly faithful.

**Lemma.** Suppose that  $G$  acts  $n$ -transitively and faithfully on  $\Omega$ ,  $n \geq 2$ . Let  $1 \neq N \triangleleft G$ . Then  $N$  acts transitively on  $\Omega$ . Moreover, if  $N_\alpha = 1$  for some  $\alpha \in \Omega$ , then the action of  $G$  on  $N - \{1\}$  by conjugation is  $n - 1$ -transitive.

**Proof** For any  $\omega \in \Omega$ , the  $N$ -orbit  $N \cdot \omega$  is mapped by  $g \in G$  as follows:

$$g \cdot (N \cdot \omega) = (gN) \cdot \omega = Ng \cdot \omega = N(g\omega)$$

Thus each  $g \in G$  permutes the set of  $N$ -orbits on  $\Omega$ . Suppose that there are two or more orbits  $\Omega_1, \Omega_2, \dots$ . Then  $|\Omega_i| > 1$  since otherwise  $N$  would act trivially on  $\Omega$ , so  $N = 1$  by faithfulness, contrary to assumption. Choose  $\alpha, \beta \in \Omega_1$  and  $\gamma \in \Omega_2$ . There is  $g \in G$  such that  $g\alpha = \alpha$  and  $g\beta = \gamma$ . Therefore  $g\Omega_1 = \Omega_1$  and  $g\Omega_1 = \Omega_2$ , a contradiction. Therefore there's only one orbit and  $N$  is transitive.

Next fix  $\alpha \in \Omega$  and suppose that  $N_\alpha = 1$ . We map

$$\phi : N \rightarrow \Omega, n \mapsto n\alpha,$$

and claim that  $\phi$  is a bijection. Since  $N$  is transitive  $\phi$  is onto. If  $n\alpha = n'\alpha$  then  $n^{-1}n' \in N_\alpha = 1$  so  $n = n'$ . We also claim that

the actions of  $G_\alpha$  on  $N$  (by conjugation) and  $\Omega$  are isomorphic via  $\phi$ ,

that is,  $\phi(gn) = g\phi(n)$  for all  $g \in G_\alpha$  and  $n \in N$ . Namely,  $\phi(gn) = \phi(gng^{-1}) = gng^{-1}\alpha = gn\alpha = g\phi(n)$ .

But the action of  $G_\alpha$  on  $\Omega - \{\alpha\}$  is  $n - 1$ -transitive, and so its action on  $N - \{1\}$  is  $n - 1$ -transitive as well.  $\square$

Now we complete the proof of the theorem. Suppose that  $n \geq 6$  and let  $G = A_n$ . Proceeding by contradiction suppose that  $N \triangleleft G$ , with  $N \neq 1$  and  $N \neq G$ . We reach a contradiction. Let  $\alpha \in \{1, \dots, n\} = \Omega$ . Then  $G_\alpha \cap N \triangleleft G_\alpha$ , as is easily checked (see the parallelogram law in the next section). Of course  $G_\alpha \cap N = N_\alpha$ , as is immediate from the definition of stabilizer. But  $G_\alpha \cong A_{n-1}$  is simple by induction. Therefore  $N_\alpha = G_\alpha$  or  $1$ . Also  $N$  is transitive on  $\Omega$ , so  $|N : N_\alpha| = n$ .

If  $N_\alpha = 1$ , then  $|N| = n$ . The previous lemma shows that  $G_\alpha$  acts 3-transitively on  $N - \{1\}$  by conjugation, since  $G$  is 4-transitive on  $\Omega$ . But this yields a contradiction since conjugation by an element is an automorphism, and so the image of two elements determines the image of their product. Specifically, choose distinct elements  $x, y \in N - \{1\}$  and let  $z = xy$ , so that  $z$  is distinct from  $x$  and  $y$ . As  $n \geq 6$  there is another element  $w \in N - \{1\}$ . By the 3-transitivity of  $G_\alpha$  there is  $g \in G_\alpha$  such that

$$gxg^{-1} = x, \quad gyg^{-1} = y, \quad gzg^{-1} = w.$$

However,  $gzg^{-1} = gxg^{-1}gyg^{-1} = xy = z \neq w$ , a contradiction.

Therefore  $G_\alpha = N_\alpha$ . Then  $|G : G_\alpha| = n = |N : N_\alpha| = |N : G_\alpha|$  and so  $N = G$ .  $\square$

**Proof of Corollary.** Suppose that  $n \geq 5$  and  $1 \neq N \triangleleft \Sigma_n$ . Now  $NA_n = A_nN$  so  $NA_n$  is a subgroup, hence equals  $\Sigma_n$  or  $A_n$ , and so  $|N : A_n \cap N| = |NA_n : A_n| = 1$  or  $2$ . Also  $N \cap A_n \triangleleft A_n$  so  $N \cap A_n = 1$  or  $A_n$  by the theorem. Accordingly  $|N| = 2$  or  $A_n \leq N$ . If  $|N| = 2$ , then  $N$  consists of a single (odd) element which must be the unique element of its cycle shape (as  $N \triangleleft G$ ). But clearly for each cycle shape (except for the identity element) there is more than one element of that cycle shape, contradiction. Therefore  $A_n \leq N$  so  $N = A_n$  or  $\Sigma_n$  as required.  $\square$