Chapter 1

Group Theory

Partial class notes, draft of Tuesday 27th April, 2010, 9:48am.

1.1 The Alternating Groups

Let A_n be the alternating group of even permutations of $\{1, \ldots, n\}$. In this section we prove that A_n is simple for $n \geqslant 5$. The crux of the argument is finding a fixed point.

Lemma 1.1. *Let $g \in S_n$ be an even permutation. If g commutes with an odd permutation, then all permutations with the same cycle shape as g are conjugate in A_n.*

Proof. We know that all permutations with the same cycle shape as g are conjugate in S_n. Let k be an odd permutation that commutes with g. For any odd permutation h, the product hk is an even permutation, and we have

$$(hk)g(hk)^{-1} = hkgk^{-1}h^{-1} = hgkk^{-1}h^{-1} = hgh^{-1}$$

so any conjugate of g by an odd permutation is also a conjugate of g by an even permutation. Therefore, the permutations with the same cycle shape as g remain conjugate in A_n. ■

For example, $(1\,2)$ commutes with $(1\,2)(3\,4)$ and $(3\,4\,5)$, so all products of two disjoint 2-cycles are conjugate in A_4, and all 3-cycles are conjugate in A_5. However, in A_4 no odd permutation commutes with $(1\,2\,3)$, and the 3-cycles break up into two conjugacy classes. In A_5 no odd permutation commutes with $(1\,2\,3\,4\,5)$, and the 5-cycles break up into two conjugacy classes.

Lemma 1.2. *Any even permutation can be written as a product of 3-cycles.*

Proof. Write an even permutation as a product of 2-cycles. Consider the first pair of 2-cycles $(i\,j)(k\,\ell)$ in this product. If $j = k$ then $(i\,j)(k\,\ell) = (i\,\ell\,j)$ is a 3-cycle. Otherwise,

$$(i\,j)(k\,\ell) = (i\,j)(j\,k)\;(j\,k)(k\,\ell) = (i\,k\,j)(j\,\ell\,k)$$

is a product of two 3-cycles. Continuing with the remaining pairs, we express the even permutation as a product of 3-cycles. ■

For example, $(1\,2\,3\,4)(5\,6\,7\,8)$ is an even permutation. We can write

$$\begin{aligned}(1\,2\,3\,4)(5\,6\,7\,8) &= (1\,2)(1\,3)(1\,4)\;\;(5\,6)(5\,7)(5\,8)\\ &= (1\,2)(1\,3)\;\;(1\,4)(4\,5)\;\;(4\,5)(5\,6)\;\;(5\,7)(5\,8)\\ &= (1\,2\,3)(1\,5\,4)(4\,6\,5)(5\,7\,8)\end{aligned}$$

Corollary 1.3. *Let* N *be a normal subgroup of* A_n *for* $n \geqslant 5$. *If* N *contains either a* 3*-cycle or a product of two disjoint* 2*-cycles, then* $N = A_n$.

Proof. Suppose that after relabeling, N contains the permutation $(1\,2\,3)$. Because $(4\,5)$ commutes with $(1\,2\,3)$, by Lemma 1.1 all 3-cycles are conjugate in A_n, so they are all contained in N. By Lemma 1.2, every element of A_n is a product of 3-cycles, so $N = A_n$.

Now suppose that after relabeling, N contains the permutation $(1\,2)(3\,4)$. Because $(1\,2)$ commutes with $(1\,2)(3\,4)$, by Lemma 1.1 all products of two disjoint 2-cycles are conjugate in A_n, so they are all contained in N. In particular, N contains $(1\,2)(3\,5)$. The product

$$(1\,2)(3\,4)\;\;(1\,2)(3\,5) = (3\,4\,5)$$

is a 3-cycle, so again $N = A_n$. ■

Lemma 1.4. *Let* N *be a normal subgroup of* A_n *for* $n \geqslant 5$. *If* N *is not the identity subgroup, then* N *contains a nontrivial permutation that fixes some element of* $\{1, \ldots, n\}$.

Proof. Let $h \in N$ be a nontrivial permutation. If h has a fixed point, then we are done. Otherwise, write h as a product of disjoint cycles; if these cycles are of different lengths, then some power of h is a nontrivial permutation in N with a fixed point, and we are done.

Otherwise, h is a disjoint product of equal length cycles. Because N is closed under taking products, taking inverses, and conjugating by elements of A_n, we have $h\,gh^{-1}g^{-1} \in N$ for any $g \in A_n$. We show that for some choice of g, this product is a nontrivial permutation with a fixed point.

We consider each cycle length. Suppose that after relabeling, $h = (1\,2)(3\,4)\,k$, where k fixes the set $\{1, \ldots, 4\}$. In this case, we can choose $g = (1\,2\,3)$, which commutes with k:

$$(1\,2)(3\,4)\,k \;\; (1\,2\,3) \;\; k^{-1}\,(3\,4)(1\,2) \;\; (1\,3\,2) \;=\; (1\,4)(2\,3)$$

is a nontrivial permutation that fixes 5.

Suppose that after relabeling, $h = (1\,2\,3)(4\,5\,6)\,k$, where k fixes the set $\{1, \ldots, 6\}$. In this case, we can choose $g = (1\,4)(2\,5)$, which commutes with k:

$$(1\,2\,3)(4\,5\,6)\,k \;\; (1\,4)(2\,5) \;\; k^{-1}\,(4\,6\,5)(1\,3\,2) \;\; (2\,5)(1\,4) \;=\; (2\,5)(3\,6)$$

is a nontrivial permutation that fixes 1.

For the general case, suppose that after relabeling, $h = (1\,2\,3\,\ldots\,m)\,k$, where $m \geqslant 4$, and k fixes the set $\{1, \ldots, m\}$. In this case, we can choose $g = (1\,2\,3)$, which commutes with k:

$$(1\,2\,3\,\ldots\,m)\,k \;\; (1\,2\,3) \;\; k^{-1}\,(1\,m\,\ldots\,3\,2) \;\; (1\,3\,2) \;=\; (2\,m\,3)$$

is a nontrivial permutation that fixes 1. ■

The expression $hgh^{-1}g^{-1}$ is called a *commutator*; it measures the failure of g and h to commute. Commutators are a frequent object of study in algebra; one can for example construct the subgroup of all commutators of a group.

A different proof of this lemma uses the pigeonhole principle: If the non-identity elements of a subgroup $H < S_n$ have no fixed points, then $|H| \leqslant n$. For if g and h are distinction permutations of H, then they cannot agree on any element of $\{1, \ldots, n\}$, or else gh^{-1} will be a nontrivial permutation in H having that element as a fixed point.

The Klein four-group

$$K = \{\, (),\; (1\,2)(3\,4),\; (1\,3)(2\,4),\; (1\,4)(2\,4) \,\}$$

is a normal subgroup of A_4, and its nonidentity elements have no fixed points. However, for $n \geqslant 5$ one can show that each nonidentity conjugacy class in A_n is of order $\geqslant n$. Since a normal subgroup consists of entire conjugacy classes, establishing this bound gives an alternate proof of Lemma 1.4.

Theorem 1.5. *The alternating group A_n is simple for $n \geqslant 5$.*

Proof. Let N be a normal subgroup of A_n other than the identity subgroup. We want to show that $N = A_n$.

By Lemma 1.4, N contains a nontrivial permutation h with a fixed point. If $n = 5$, then h must either be 3-cycle or a product of two disjoint 2-cycles. By Corollary 1.3 we have $N = A_5$. This shows that A_5 is simple.

Otherwise, suppose that after relabeling, h fixes n. Let $A_{n-1} < A_n$ be the alternating group of even permutations of $\{1, \dots, n-1\}$, and let $H = N \cap A_{n-1}$. Then $h \in H$, so H is not the identity subgroup. Moreover, H is a normal subgroup of A_{n-1}. By induction, A_{n-1} is simple, so $H = A_{n-1}$. In particular, N contains the 3-cycle $(1\,2\,3)$, so again by Corollary 1.3 we have $N = A_n$. This shows that A_n is simple. ∎

1.2 The Sylow Theorems

Lemma 1.6. *Let* $f : G \to L$ *be a homomorphism between two finite groups with kernel* $N \lhd G$*, and let* $H < G$ *be a subgroup. If the orders* $|H|$ *and* $|L|$ *are relatively prime, then* $H \subseteq N$.

Proof. Consider the order of the image $f(H) < L$. Because $f(H)$ is a subgroup of L, its order divides the order of L. On the other hand, because $f(H)$ is a quotient of H, its order divides the order of H. Because the orders $|H|$ and $|L|$ are relatively prime, we conclude that $|f(H)| = 1$. In other words, f sends every element of H to the identity element of L, so H is contained in the kernel N of the map f. ∎

More generally, we can write the order of H as the product

$$|H| \;=\; |H \cap N| \cdot |f(H)|$$

with the restrictions that $|H \cap N|$ divides $|N|$, and $|f(H)|$ divides $|H|$.

A version of this formula is familiar from linear algebra: If $f : V \to W$ is a linear map of vector spaces with kernel N, and $U \subset V$ is a subspace, then

$$\dim U \;=\; \dim(U \cap N) \;+\; \dim f(U)$$

with the restrictions that $\dim(U \cap N) \leqslant \dim N$ and $\dim f(U) \leqslant \dim W$.

These two formulas look similar; how can we reconcile them? When H is an n-dimensional vector space over the finite field $\mathbb{F}_p$, both formulas apply: As a vector space, $\dim H = n$, while as an additive group, H is isomorphic to the direct product $C_p \times \cdots \times C_p$ of n copies of the cyclic group of order p, and

$|H| = p^n$. Here, multiplying orders has the same effect as adding dimensions, and the two formulas agree. We think of the first formula as conservation of order, and the second formula as conservation of dimension.

Corollary 1.7. *Let G be a group of order mn, where m and n are relatively prime. If H and N are subgroups of order m, and N is normal in G, then $H = N$.*

Proof. We apply Lemma 1.6, taking $L = G/N$: Consider the quotient map $G \to G/N$, with kernel N. The quotient G/N has order n, which is relatively prime to the order m of H. By Lemma 1.6, $H \subseteq N$. Because H and N have the same order, they are equal. ■

A refinement of Corollary 1.7 will be used in one proof of the Sylow theorems:

Corollary 1.8. *Let G be a group of order mn, where m and n are relatively prime. If H and K are subgroups of order m, and H is contained in the normalizer $N(K)$ of K, then $H = K$.*

Proof. We apply Corollary 1.7 to the subgroup $N(K)$: We have the chain of subgroups $K < N(K) < G$, so the order $|N(K)|$ divides the order $|G| = mn$, and is a multiple mn' of the order $|K| = m$. Therefore n' divides n. Thus $N(K)$ is a group of order mn', where m and n' are relatively prime. H and K are subgroups of $N(K)$ of order m, and K is normal in $N(K)$, so Corollary 1.7 applies. ■

Example 1.9. Let $K < S_n$ be a subgroup of the symmetric group, of odd order. Then K consists entirely of even permutations.

Proof. Consider the homomorphism $S_n \to C_2$ taking each permutation to its sign, an element of the multiplicative group $\{1, -1\}$. The kernel of this map is the alternating group A_n of even permutations. Because $|K|$ is relatively prime to 2, by Lemma 1.6 we have $K \subseteq A_n$. ■

Example 1.10. The Klein-4 subgroup

$$K \;=\; \{\,(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\,\} \;<\; A_4.$$

is the unique order 4 subgroup of A_4.

We know this to be true by listing the elements of A_4; every other element has order 3. Once we establish that K is normal in A_4, this also follows from the Sylow theorems: 4 is the maximal power of 2 dividing the order 12 of A_4, so all subgroups of order 4 in A_4 are conjugate. However, it is simpler to apply Corollary 1.7:

Proof. K is normal in A_4, because conjugation of permutations preserves shape, and K consists of the identity and all elements of A_4 having the same shape as $(1\,2)(3\,4)$. Because $|K| = 4$ and $|A_4| = 4 \cdot 3$ with 4 and 3 relatively prime, by Corollary 1.7 any subgroup $H < A_4$ of order 4 is equal to K. ∎

The next example illustrates how Corollary 1.8 will be applied in a proof of the Sylow theorems:

Example 1.11. Consider the subgroup

$$K \;=\; \{\, (), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3) \,\} \;<\; A_5.$$

Let $H < A_5$ be a subgroup of order 4, which fixes K under conjugation. Then $H = K$.

Proof. Our hypothesis states that for any $h \in H$ we have $hKh^{-1} = K$. In other words, H is contained in the normalizer $N(K)$ of K. The order $|A_5| = 4 \cdot 15$ with 4 and 15 relatively prime, so by Corollary 1.8 we have $H = K$. ∎

We will prove the second and third Sylow theorems by considering how a p-Sylow subgroup $P < G$ acts by conjugation on the set X of all conjugates of a p-Sylow subgroup $Q < G$. First, we explore this construction in examples:

Example 1.12. Consider the 2-Sylow subgroups

$$P = \{(), (1\,2)\}, \quad Q = \{(), (1\,3)\}, \quad R = \{(), (2\,3)\}$$

of the symmetric group S_3. Let $X = \{P, Q, R\}$ be the set of conjugates of Q. Then P acts on X by conjugation, and under this action X consists of the orbits $\{P\}$ and $\{Q, R\}$.