Chapter 5

Some Basic Techniques of Group Theory

5.1 Groups Acting on Sets

In this chapter we are going to analyze and classify groups, and, if possible, break down complicated groups into simpler components. To motivate the topic of this section, let's look at the following result.

5.1.1 Cayley's Theorem

Every group is isomorphic to a group of permutations.

Proof. The idea is that each element g in the group G corresponds to a permutation of the set G itself. If $x \in G$, then the permutation associated with g carries x into gx. If $gx = gy$, then premultiplying by g^{-1} gives $x = y$. Furthermore, given any $h \in G$, we can solve $gx = h$ for x. Thus the map $x \to gx$ is indeed a permutation of G. The map from g to its associated permutation is injective, because if $gx = hx$ for all $x \in G$, then (take $x = 1$) $g = h$. In fact the map is a homomorphism, since the permutation associated with hg is multiplication by hg, which is multiplication by g followed by multiplication by h, $h \circ g$ for short. Thus we have an embedding of G into the group of all permutations of the set G. ♣

In Cayley's theorem, a group acts on itself in the sense that each g yields a permutation of G. We can generalize to the notion of a group acting on an arbitrary set.

5.1.2 Definitions and Comments

The group G *acts on the set* X if for each $g \in G$ there is a mapping $x \to gx$ of X into itself, such that

(1) $h(gx) = (hg)x$ for every $g, h \in G$

(2) $1x = x$ for every $x \in X$.

As in (5.1.1), $x \to gx$ defines a permutation of X. The main point is that the action of g is a permutation because it has an inverse, namely the action of g^{-1}. (Explicitly, the inverse of $x \to gx$ is $y \to g^{-1}y$.) Again as in (5.1.1), the map from g to its associated permutation $\Phi(g)$ is a homomorphism of G into the group S_X of permutations of X. But we do not necessarily have an embedding. If $gx = hx$ for all x, then in (5.1.1) we were able to set $x = 1$, the identity element of G, but this resource is not available in general.

We have just seen that a group action induces a homomorphism from G to S_X, and there is a converse assertion. If Φ is a homomorphism of G to S_X, then there is a corresponding action, defined by $gx = \Phi(g)x, x \in X$. Condition (1) holds because Φ is a homomorphism, and (2) holds because $\Phi(1)$ must be the identity of S_X. The kernel of Φ is known as the *kernel of the action*; it is the set of all $g \in G$ such that $gx = x$ for all x, in other words, the set of g's that fix everything in X.

5.1.3 Examples

1. (*The regular action*) Every group acts on itself by multiplication on the left, as in (5.1.1). In this case, the homomorphism Φ is injective, and we say that the action is *faithful*.

[Similarly, we can define an action on the right by $(xg)h = x(gh)$, $x1 = x$, and then G acts on itself by right multiplication. The problem is that $\Phi(gh) = \Phi(h) \circ \Phi(g)$, an antihomomorphism. The damage can be repaired by writing function values as xf rather than $f(x)$, or by defining the action of g to be multiplication on the right by g^{-1}. We will avoid the difficulty by restricting to actions on the left.]

2. (*The trivial action*) We take $gx = x$ for all $g \in G$, $x \in X$. This action is highly unfaithful.

3. (*Conjugation on elements*) We use the notation $g \bullet x$ for the action of g on x, and we set $g \bullet x = gxg^{-1}$, called the *conjugate of x by g*, for g and x in the group G. Since $hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$ and $1x1^{-1} = x$, we have a legal action of G on itself. The kernel is

$$\{g \colon gxg^{-1} = x \text{ for all } x\}, \text{ that is, } \{g \colon gx = xg \text{ for all } x\}.$$

Thus the kernel is the set of elements that commute with everything in the group. This set is called the *center* of G, written $Z(G)$.

4. (*Conjugation on subgroups*) If H is a subgroup of G, we take $g \bullet H = gHg^{-1}$. Note that gHg^{-1} is a subgroup of G, called the *conjugate subgroup of H by g*, since $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. As in Example (3), we have a legal action of G on the set of subgroups of G.

5. (*Conjugation on subsets*) This is a variation of the previous example. In this case we let G act by conjugation on the collection of all subsets of G, not just subgroups. The verification that the action is legal is easier, because gHg^{-1} is certainly a subset of G.

6. (*Multiplication on left cosets*) Let G act on the set of left cosets of a fixed subgroup H by $g \bullet (xH) = (gx)H$. By definition of set multiplication, we have a legitimate action.

7. (*Multiplication on subsets*) Let G act on all subsets of G by $g \bullet S = gS = \{gx \colon x \in S\}$. Again the action is legal by definition of set multiplication.

Problems For Section 5.1

1. Let G act on left cosets of H by multiplication, as in Example 6. Show that the kernel of the action is a subgroup of H.
2. Suppose that H is a proper subgroup of G of index n, and that G is a *simple group*, that is, G has no normal subgroups except G itself and $\{1\}$. Show that$G$ can be embedded in S_n.
3. Suppose that G is an infinite simple group. Show that for every proper subgroup H of G, the index $[G : H]$ is infinite.
4. Let G act on left cosets of H by multiplication. Show that the kernel of the action is
$$N = \bigcap_{x \in G} xHx^{-1}.$$
5. Continuing Problem 4, if K is any normal subgroup of G contained in H, show that $K \leq N$. Thus N is the largest normal subgroup of G contained in H; N is called the *core* of H in G.
6. Here is some extra practice with left cosets of various subgroups. Let H and K be subgroups of G, and consider the map f which assigns to the coset $g(H \cap K)$ the pair of cosets (gH, gK). Show that f is well-defined and injective, and therefore
$$[G : H \cap K] \leq [G : H][G : K].$$
Thus (Poincaré) the intersection of finitely many subgroups of finite index also has finite index.
7. If $[G : H]$ and $[G : K]$ are finite and relatively prime, show that the inequality in the preceding problem is actually an equality.
8. Let H be a subgroup of G of finite index n, and let G act on left cosets xH by multiplication. Let N be the kernel of the action, so that $N \trianglelefteq H$ by Problem 1. Show that $[G : N]$ divides $n!$.
9. Let H be a subgroup of G of finite index $n > 1$. If $|G|$ does not divide $n!$, show that G is not simple.

.

5.2 The Orbit-Stabilizer Theorem

5.2.1 Definitions and Comments

Suppose that the group G acts on the set X. If we start with the element $x \in X$ and successively apply group elements in all possible ways, we get

$$B(x) = \{gx \colon g \in G\}$$

which is called the *orbit* of x under the action of G. The action is *transitive* (we also say that G *acts transitively* on X) if there is only one orbit, in other words, for any $x, y \in X$, there exists $g \in G$ such that $gx = y$. Note that the orbits partition X, because they are the equivalence classes of the equivalence relation given by $y \sim x$ iff $y = gx$ for some $g \in G$.

The *stabilizer* of an element $x \in X$ is

$$G(x) = \{g \in G \colon gx = x\},$$

the set of elements that leave x fixed. A direct verification shows that $G(x)$ is a subgroup. This is a useful observation because any set that appears as a stabilizer in a group action is guaranteed to be a subgroup; we need not bother to check each time.

Before proceeding to the main theorem, let's return to the examples considered in (5.1.3).

5.2.2 Examples

1. The regular action of G on G is transitive, and the stabilizer of x is the subgroup $\{1\}$.

2. The trivial action is not transitive (except in trivial cases), in fact, $B(x) = \{x\}$ for every x. The stabilizer of x is the entire group G.

3. Conjugation on elements is not transitive (see Problem 1). The orbit of x is the set of *conjugates* gxg^{-1} of x, that is,

$$B(x) = \{gxg^{-1} \colon g \in G\},$$

which is known as the *conjugacy class* of x. The stabilizer of x is

$$G(x) = \{g \colon gxg^{-1} = x\} = \{g \colon gx = xg\},$$

the set of group elements that commute with x. This set is called the *centralizer* of x, written $C_G(x)$. Similarly, the centralizer $C_G(S)$ of an arbitrary subset $S \subseteq G$ is defined as the set of elements of G that commute with everything in S. (Here, we do need to check that $C_G(S)$ is a subgroup, and this follows because $C_G(S) = \bigcap_{x \in S} C_G(x)$.)

4. Conjugation on subgroups is not transitive. The orbit of H is $\{gHg^{-1} \colon g \in G\}$, the collection of conjugate subgroups of H. The stabilizer of H is

$$\{g \colon gHg^{-1} = H\},$$

which is called the *normalizer* of H, written $N_G(H)$. If K is a subgroup of G containing H, we have

$$H \trianglelefteq K \text{ iff } gHg^{-1} = H \text{ for every } g \in K$$

and this holds iff K is a subgroup of $N_G(H)$. Thus $N_G(H)$ is the largest subgroup of G in which H is normal.

5. Conjugation on subsets is not transitive, and the orbit of the subset S is $\{gSg^{-1}\colon g \in G\}$. The stabilizer of S is the normalizer$N_G(S) = \{g\colon gSg^{-1} = S\}$.

6. Multiplication on left cosets is transitive; a solution of $g(xH) = yH$ for x is $x = g^{-1}y$. The stabilizer of xH is

$$\{g\colon gxH = xH\} = \{g\colon x^{-1}gx \in H\} = \{g\colon g \in xHx^{-1}\} = xHx^{-1},$$

the conjugate of H by x. Taking $x = 1$, we see that the stabilizer of H is H itself.

7. Multiplication on subsets is not transitive. The stabilizer of S is $\{g\colon gS = S\}$, the set of elements of G that permute the elements of S.

5.2.3 The Orbit-Stabilizer Theorem

Suppose that a group G acts on a set X. Let $B(x)$ be the orbit of $x \in X$, and let $G(x)$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is,

$$|B(x)| = [G\colon G(x)].$$

Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

Proof. If y belongs to the orbit of x, say $y = gx$. We take $f(y) = gH$, where $H = G(x)$ is the stabilizer of x. To check that f is a well-defined map of $B(x)$ to the set of left cosets of H, let $y = g_1x = g_2x$. Then $g_2^{-1}g_1x = x$, so $g_2^{-1}g_1 \in H$, i.e., $g_1H = g_2H$. Since g is an arbitrary element of G, f is surjective. If $g_1H = g_2H$, then $g_2^{-1}g_1 \in H$, so that $g_2^{-1}g_1x = x$, and consequently $g_1x = g_2x$. Thus if $y_1 = g_1x$, $y_2 = g_2x$, and $f(y_1) = f(y_2)$, then $y_1 = y_2$, proving f injective. ♣

Referring to (5.2.2), Example 3, we see that $B(x)$ is an orbit of size 1 iff x commutes with every $g \in G$, i.e., $x \in Z(G)$, the center of G. Thus if G is finite and we select one element x_i from each conjugacy class of size greater than 1, we get the *class equation*

$$|G| = |Z(G)| + \sum_i [G\colon C_G(x_i)].$$

We know that a group G acts on left cosets of a subgroup K by multiplication. To prepare for the next result, we look at the action of a *subgroup* H of G on left cosets of K. Since K is a left coset of K, it has an orbit given by $\{hK\colon h \in H\}$. The union of the sets hK is the set product HK. The stabilizer of K is not K itself, as in Example 6; it is $\{h \in H\colon hK = K\}$. But $hK = K(= 1K)$ if and only if $h \in K$, so the stabilizer is $H \cap K$.

5.2.4 Proposition

If H and K are subgroups of the finite group G, then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. The cosets in the orbit of K are disjoint, and each has $|K|$ members. Since, as remarked above, the union of the cosets is HK, there must be exactly $|HK|/|K|$ cosets in the orbit. Since the index of the stabilizer of K is $|H/H \cap K|$, the result follows from the orbit-stabilizer theorem. ♣

Problems For Section 5.2

1. Let σ be the permutation $(1,2,3,4,5)$ and π the permutation $(1,2)(3,4)$. Then $\pi\sigma\pi^{-1}$, the conjugate of σ by π, can be obtained by applying π to the symbols of σ to get $(2,1,4,3,5)$. Reversing the process, if we are given $\tau = (1,2)(3,4)$ and we specify that $\mu\tau\mu^{-1} = (1,3)(2,5)$, we can take $\mu = [\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{smallmatrix}]$. This suggests that two permutations are conjugate if and only if they have the same cycle structure. Explain why this works.
2. Show that if S is any subset of G, then the centralizer of S is a normal subgroup of the normalizer of S. (Let the normalizer $N_G(S)$ act on S by conjugation on elements.)
3. Let $G(x)$ be the stabilizer of x under a group action. Show that stabilizers of elements in the orbit of x are conjugate subgroups. Explicitly, for every $g \in G$ and $x \in X$ we have
$$G(gx) = gG(x)g^{-1}.$$
4. Let G act on the set X. Show that for a given $x \in X$, $\Psi(gG(x)) = gx$ is a well-defined injective mapping of the set of left cosets of $G(x)$ into X, and is bijective if the action is transitive.
5. Continuing Problem 4, let G act transitively on X, and choose any $x \in X$. Show that the action of G on X is essentially the same as the action of G on the left cosets of the stabilizer subgroup $G(x)$. This is the meaning of the assertion that"any transitive G-set is isomorphic to a space of left cosets". Give an appropriate formal statement expressing this idea.
6. Suppose that G is a finite group, and for every $x, y \in G$ such that $x \neq 1$ and $y \neq 1$, x and y are conjugate. Show that the order of G must be 1 or 2.
7. First note that if r is a positive rational number and k a fixed positive integer, there are only finitely many positive integer solutions of the equation
$$\frac{1}{x_1} + \cdots + \frac{1}{x_k} = r.$$

Outline of proof: If x_k is the smallest x_i, the left side is at most k/x_k, so $1 \leq x_k \leq k/r$ and there are only finitely many choices for x_k. Repeat this argument for the equation $\frac{1}{x_1} + \cdots + \frac{1}{x_{k-1}} = r - \frac{1}{x_k}$.

Now set $r = 1$ and let $N(k)$ be an upper bound on all the x_i's in all possible solutions. If G is a finite group with exactly k conjugacy classes, show that the order of G is at most $N(k)$.

5.3 Application To Combinatorics

The theory of group actions can be used to solve a class of combinatorial problems. To set up a typical problem, consider the regular hexagon of Figure 5.3.1, and recall the dihedral group D_{12}, the group of symmetries of the hexagon (Section 1.2).

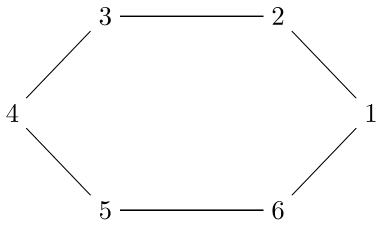

Figure 5.3.1

If R is rotation by 60 degrees and F is reflection about the horizontal line joining vertices 1 and 4, the 12 members of the group may be listed as follows.

$I =$ identity, $R = (1,2,3,4,5,6)$, $R^2 = (1,3,5)(2,4,6)$,
$R^3 = (1,4)(2,5)(3,6)$, $R^4 = (1,5,3)(2,6,4)$, $R^5 = (1,6,5,4,3,2)$
$F = (2,6)(3,5)$, $RF = (1,2)(3,6)(4,5)$, $R^2F = (1,3)(4,6)$
$R^3F = (1,4)(2,3)(5,6)$, $R^4F = (1,5)(2,4)$, $R^5F = (1,6)(2,5)(3,4)$.

(As before, RF means F followed by R.)

Suppose that we color the vertices of the hexagon, and we have n colors available (we are not required to use every color). How many distinct colorings are there? Since we may choose the color of any vertex in n ways, a logical answer is n^6. But this answer does not describe the physical situation accurately. To see what is happening, suppose we have two colors, yellow (Y) and blue (B). Then the coloring

$$C_1 = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ B & B & Y & Y & Y & B \end{matrix}$$

is mapped by RF to

$$C_2 = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ B & B & B & Y & Y & Y \end{matrix}$$

(For example, vertex 3 goes to where vertex 6 was previously, delivering the color yellow to vertex 6.) According to our counting scheme, C_2 is not the same as C_1. But imagine that we have two rigid necklaces in the form of a hexagon, one colored by C_1 and the other by C_2. If both necklaces were lying on a table, it would be difficult to argue that they are essentially different, since one can be converted to a copy of the other simply by flipping it over and then rotating it.

Let's try to make an appropriate mathematical model. Any group of permutations of a set X acts on X in the natural way: $g \bullet x = g(x)$. In particular, the dihedral group G acts on the vertices of the hexagon, and therefore on the set S of colorings of the vertices. The above discussion suggests that colorings in the same orbit should be regarded as equivalent, so the number of essentially different colorings is the number of orbits. The following result will help us do the counting.

5.3.1 Orbit-Counting Theorem

Let the finite group G act on the finite set X, and let $f(g)$ be the number of elements of X fixed by g, that is, the size of the set $\{x \in X : g(x) = x\}$. Then the number of orbits is

$$\frac{1}{|G|}\sum_{g\in G} f(g),$$

the average number of points left fixed by elements of G.

Proof. We use a standard combinatorial technique called "counting two ways". Let T be the set of all ordered pairs (g, x) such that $g \in G, x \in X$, and $gx = x$. For any $x \in X$, the number of g's such that $(g, x) \in T$ is the size of the stabilizer subgroup $G(x)$, hence

$$|T| = \sum_{x\in X} |G(x)|. \tag{1}$$

Now for any $g \in G$, the number of x's such that $(g, x) \in T$ is $f(g)$, the number of fixed points of g. Thus

$$|T| = \sum_{g\in G} f(g). \tag{2}$$

Divide (1) and (2) by the order of G to get

$$\sum_{x\in X} \frac{|G(x)|}{|G|} = \frac{1}{|G|}\sum_{g\in G} f(g). \tag{3}$$

But by the orbit-stabilizer theorem (5.2.3), $|G|/|G(x)|$ is $|B(x)|$,the size of the orbit of x. If, for example, an orbit has 5 members, then 1/5 will appear 5 times in the sum on the left side of (3), for a total contribution of 1. Thus the left side of (3) is the total number of orbits. ♣

We can now proceed to the next step in the analysis.

5.3.2 Counting the Number of Colorings Fixed by a Given Permutation

Let $\pi = R^2 = (1, 3, 5)(2, 4, 6)$. Since $\pi(1) = 3$ and $\pi(3) = 5$, vertices 1,3 and 5 have the same color. Similarly, vertices 2,4 and 6 must have the same color. If there are n colors available, we can choose the color of each cycle in n ways, and the total number of choices is n^2. If $\pi = F = (2, 6)(3, 5)$, then as before we choose 1 color out of n for each cycle, but in this case we still have to color the vertices 1 and 4. Here is a general statement that covers both situations.

If π has c cycles, *counting cycles of length 1*, then the number of colorings fixed by π is n^c.

To emphasize the need to consider cycles of length 1, we can write F as (2,6)(3,5)(1)(4). From the cycle decompositions given at the beginning of the section, we have one permutation (the identity) with 6 cycles, three with 4 cycles, four with 3 cycles, two with 2 cycles, and two with 1 cycle. Thus the number of distinct colorings is

$$\frac{1}{12}(n^6+3n^4+4n^3+2n^2+2n).$$

5.3.3 A Variant

We now consider a slightly different question. How many distinct colorings of the vertices of a regular hexagon are there if we are forced to color exactly three vertices blue and three vertices yellow? The group G is the same as before, but the set S is different. Of the 64 possible colorings of the vertices, only $\binom{6}{3}=20$ are legal, since 3 vertices out of 6 are chosen to be colored blue; the other vertices must be colored yellow. If π is a permutation of G, then within each cycle of π, all vertices have the same color, but in contrast to the previous example, we do not have a free choice of color for each cycle. To see this, consider $R^2=(1,3,5)(2,4,6)$. The cycle $(1,3,5)$ can be colored blue and $(2,4,6)$ yellow, or vice versa, but it is not possible to color all six vertices blue, or to color all vertices yellow. Thus $f(R^2)=2$. If $\pi=F=(2,6)(3,5)(1)(4)$, a fixed coloring is obtained by choosing one of the cycles of length 2 and one of the cycles of length 1 to be colored blue, thus producing 3 blue vertices. Consequently, $f(F)=4$. To obtain $f(I)$, note that all legal colorings are fixed by I, so $f(I)$ is the number of colorings of 6 vertices with exactly 3 blue and 3 yellow vertices, namely, $\binom{6}{3}=20$. From the cycle decompositions of the members of G, there are two permutations with $f=2$, three with $f=4$, and one with $f=20$; the others have $f=0$. Thus the number of distinct colorings is

$$\frac{1}{12}(2(2)+3(4)+20)=3.$$

Problems For Section 5.3

1. Assume that two colorings of the vertices of a square are equivalent if one can be mapped into the other by a permutation in the dihedral group $G=D_8$. If n colors are available, find the number of distinct colorings.
2. In Problem 1, suppose that we color the sides of the square rather than the vertices. Do we get the same answer?
3. In Problem 1, assume that only two colors are available, white and green. There are 16 unrestricted colorings, but only 6 equivalence classes. List the equivalence classes explicitly.
4. Consider a rigid rod lying on the x-axis from $x=-1$ to $x=1$, with three beads attached. The beads are located at the endpoints $(-1,0)$ and $(1,0)$, and at the center $(0,0)$. The beads are to be painted using n colors, and two colorings are regarded as equivalent if one can be mapped into the other by a permutation in the group $G=\{I,\sigma\}$, where σ is the 180 degree rotation about the vertical axis. Find the number of distinct colorings.

5. In Problem 4, find the number of distinct colorings if the color of the central bead is always black.

6. Consider the group of rotations of the regular tetrahedron (see Figure 5.3.2); G consists of the following permutations.

   (i) The identity;

   (ii) Rotations by 120 degrees, clockwise or counterclockwise, about an axis through a vertex and the opposite face. There are 8 such rotations (choose 1 of 4 vertices, then choose a clockwise or counterclockwise direction);

   (iii) Rotations by 180 degrees about the line joining the midpoints of two nontouching edges. There are 3 such rotations.

   Argue geometrically to show that there are no other rotations in the group, and show that G is isomorphic to the alternating group A_4.

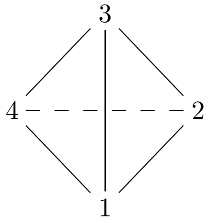

Figure 5.3.2

7. Given n colors, find the number of distinct colorings of the vertices of a regular tetrahedron, if colorings that can be rotated into each other are equivalent.

8. In Problem 7, assume that $n = 4$ and label the colors B,Y,W,G. Find the number of distinct colorings if exactly two vertices must be colored B.

9. The group G of rotations of a cube consists of the following permutations of the faces.

   (i) The identity.

   (ii) Rotations of ± 90 or 180 degrees about a line through the center of two opposite faces; there are $3 \times 3 = 9$ such rotations.

   (iii) Rotations of ± 120 degrees about a diagonal of the cube, i.e., a line joining two opposite vertices (vertices that are a maximal distance apart). There are 4 diagonals, so there are $4 \times 2 = 8$ such rotations.

   (iv) Rotations of 180 degrees about a line joining the midpoints of two opposite edges. There are 6 such rotations. (An axis of rotation is determined by selecting one of the four edges on the bottom of the cube, or one of the two vertical edges on the front face.)

   Argue geometrically to show that there are no other rotations in the group, and show that G is isomorphic to the symmetric group S_4.

10. If six colors are available and each face of a cube is painted a different color, find the number of distinct colorings.
11. Let G be the group of rotations of a regular p-gon, where p is an odd prime. If the vertices of the p-gon are to be painted using at most n colors, find the number of distinct colorings.
12. Use the result of Problem 11 to give an unusual proof of Fermat's little theorem.

5.4 The Sylow Theorems

Considerable information about the structure of a finite group G can be obtained by factoring the order of G. Suppose that $|G| = p^r m$ where p is prime, r is a positive integer, and p does not divide m. Then r is the highest power of p that divides the order of G. We will prove, among other things, that G must have a subgroup of order p^r, and any two such subgroups must be conjugate. We will need the following result about binomial coefficients.

5.4.1 Lemma

If $n = p^r m$ where p is prime, then $\binom{n}{p^r} \equiv m \bmod p$. Thus if p does not divide m, then it does not divide $\binom{p^r m}{p^r}$.

Proof. By the binomial expansion modulo p (see Section 3.4), which works for polynomials as well as for field elements, we have

$$(X+1)^{p^r} \equiv X^{p^r} + 1^{p^r} = X^{p^r} + 1 \bmod p.$$

Raise both sides to the power m to obtain

$$(X+1)^n \equiv (X^{p^r} + 1)^m \bmod p.$$

On the left side, the coefficient of X^{p^r} is $\binom{n}{p^r}$, and on the right side, it is $\binom{m}{m-1} = m$. The result follows. ♣

5.4.2 Definitions and Comments

Let p be a prime number. The group G is said to be a *p-group* if the order of each element of G is a power of p. (The particular power depends on the element.) If G is a finite group, then G is a p-group iff the order of G is a power of p. [The "if" part follows from Lagrange's theorem, and the "only if" part is a corollary to the Sylow theorems; see (5.4.5).]

If $|G| = p^r m$, where p does not divide m, then a subgroup P of G of order p^r is called a *Sylow p-subgroup* of G. Thus P is a p-subgroup of G of maximum possible size.

5.4.3 The Sylow Theorems

Let G be a finite group of order $p^r m$, where p is prime, r is a positive integer, and p does not divide m. Then

(1) G has at least one Sylow p-subgroup, and every p-subgroup of G is contained in a Sylow p-subgroup.

(2) Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \bmod p$ and n_p divides m.

(3) All Sylow p-subgroups are conjugate. Thus if we define an equivalence relation on subgroups by $H \sim K$ iff $H = gKg^{-1}$ for some $g \in G$, then the Sylow p-subgroups comprise a single equivalence class. [Note that the conjugate of a Sylow p-subgroup is also a Sylow p-subgroup, since it has the same number of elements p^r.]

Proof. (1) Let G act on subsets of G of size p^r by left multiplication. The number of such subsets is $\binom{p^r m}{p^r}$, which is not divisible by p by (5.4.1). Consequently, since orbits partition the set acted on by the group, there is at least one subset S whose orbit size is not divisible by p. If P is the stabilizer of S, then by (5.2.3), the size of the orbit is $[G : P] = |G|/|P| = p^r m/|P|$. For this to fail to be divisible by p, we must have $p^r||P|$, and therefore $p^r \le |P|$. But for any fixed $x \in S$, the map of P into S given by $g \to gx$ is injective. (The map is indeed into S because g belongs to the stabilizer of S, so that $gS = S$.) Thus $|P| \le |S| = p^r$. We conclude that $|P| = p^r$, hence P is a Sylow p-subgroup.

So far, we have shown that a Sylow p-subgroup P exists, but not that every p-subgroup is contained in a Sylow p-subgroup. We will return to this in the course of proving (2) and (3).

(2) and (3) Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$ and P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}, g \in P$. By (5.2.3), the size of any orbit divides $|P| = p^r$, hence is a power of p. Suppose that there is an orbit of size 1, that is, a Sylow p-subgroup $Q \in X$ such that $gQg^{-1} = Q$, and therefore $gQ = Qg$, for every $g \in P$. (There is at least one such subgroup, namely P.) Then $PQ = QP$, so by (1.3.6), $PQ = \langle P, Q, \rangle$, the subgroup generated by P and Q. Since $|P| = |Q| = p^r$ it follows from (5.2.4) that $|PQ|$ is a power of p, say p^c. We must have $c \le r$ because PQ is a subgroup of G (hence $|PQ|$ divides $|G|$). Thus

$$p^r = |P| \le |PQ| \le p^r, \text{ so } |P| = |PQ| = p^r.$$

But P is a subset of PQ, and since all sets are finite, we conclude that $P = PQ$, and therefore $Q \subseteq P$. Since both P and Q are of size p^r, we have $P = Q$. Thus there is only one orbit of size 1, namely $\{P\}$. Since by (5.2.3), all other orbit sizes are of the form p^c where $c \ge 1$, it follows that $n_p \equiv 1 \bmod p$.

Now let R be a p-subgroup of G, and let R act by multiplication on Y, the set of left cosets of P. Since $|Y| = [G : P] = |G|/|P| = p^r m/p^r = m$, p does not divide $|Y|$. Therefore some orbit size is not divisible by p. By (5.2.3), every orbit size divides $|R|$, hence is a power of p. (See (5.4.5) below. We are not going around in circles because (5.4.4) and (5.4.5) only depend on the existence of Sylow subgroups, which we have already established.) Thus there must be an orbit of size 1, say $\{gP\}$ with $g \in G$. If $h \in R$ then $hgP = gP$, that is, $g^{-1}hg \in P$, or equally well, $h \in gPg^{-1}$. Consequently, R is contained in a conjugate of P. If R is a Sylow p-subgroup to begin with, then R is a conjugate of P, completing the proof of (1) and (3).

To finish (2), we must show that n_p divides m. Let G act on subgroups by conjugation. The orbit of P has size n_p by (3), so by (5.2.3), n_p divides $|G| = p^r m$. But p cannot be a prime factor of n_p, since $n_p \equiv 1 \bmod p$. It follows that n_p must divide m. ♣

5.4.4 Corollary (Cauchy's Theorem)

If the prime p divides the order of G, then G has an element of order p.

Proof. Let P be a Sylow p-subgroup of G, and pick $x \in P$ with $x \neq 1$. The order of x is a power of p, say $|x| = p^k$. Then $x^{p^{k-1}}$ has order p. ♣

5.4.5 Corollary

The finite group G is a p-group if and only if the order of G is a power of p.

Proof. If the order of G is not a power of p, then it is divisible by some other prime q. But in this case, G has a Sylow q-subgroup, and therefore by (5.4.4), an element of order q. Thus G cannot be a p-group. The converse was done in (5.4.2). ♣

Problems For Section 5.4

1. Under the hypothesis of the Sylow theorems, show that G has a subgroup of index n_p.
2. Let P be a Sylow p-subgroup of the finite group G, and let Q be any p-subgroup. If Q is contained in the normalizer $N_G(P)$, show that PQ is a p-subgroup.
3. Continuing Problem 2, show that Q is contained in P.
4. Let P be a Sylow p-subgroup of the finite group G, and let H be a subgroup of G that contains the normalizer $N_G(P)$.
   (a) If $g \in N_G(H)$, show that P and gPg^{-1} are Sylow p-subgroups of H, hence they are conjugate in H.
   (b) Show that $N_G(H) = H$.
5. Let P be a Sylow p-subgroup of the finite group G, and let N be a normal subgroup of G. Assume that p divides $|N|$ and $|G/N|$, so that N and G/N have Sylow p-subgroups. Show that $[PN : P]$ and p are relatively prime, and then show that $P \cap N$ is a Sylow p-subgroup of N.
6. Continuing Problem 5, show that PN/N is a Sylow p-subgroup of G/N.
7. Suppose that P is the unique Sylow p-subgroup of G. [Equivalently, $P$is a normal Sylow p-subgroup of G; see (5.5.4).] Show that for each automorphism f of G, we have $f(P) = P$. [Thus P is a characteristic subgroup of G; see (5.7.1).]

8. The Sylow theorems are about subgroups whose order is a power of a prime p. Here is a result about subgroups of index p. Let H be a subgroup of the finite group G, and assume that $[G : H] = p$. Let N be a normal subgroup of G such that $N \leq H$ and $[G : N]$ divides $p!$ (see Section 5.1, Problem 8). Show that $[H : N]$ divides $(p - 1)!$.

9. Continuing Problem 8, let H be a subgroup of the finite group G, and assume that H has index p, where p is the smallest prime divisor of $|G|$. Show that $H \trianglelefteq G$.

5.5 Applications Of The Sylow Theorems

The Sylow theorems are of considerable assistance in the problem of classifying, up to isomorphism, all finite groups of a given order n. But in this area, proofs tend to involve intricate combinatorial arguments, best left to specialized texts in group theory. We will try to illustrate some of the basic ideas while keeping the presentation clean and crisp.

5.5.1 Definitions and Comments

A group G is *simple* if $G \neq \{1\}$ and the only normal subgroups of G are G itself and $\{1\}$. We will see later that simple groups can be regarded as building blocks for arbitrary finite groups. Abelian simple groups are already very familiar to us; they are the cyclic groups of prime order. For if $x \in G$, $x \neq 1$, then by simplicity (and the fact that all subgroups of an abelian group are normal), $G = \langle x \rangle$. If G is not of prime order, then G has a nontrivial proper subgroup by (1.1.4), so G cannot be simple.

The following results will be useful.

5.5.2 Lemma

If H and K are normal subgroups of G and the intersection of H and K is trivial (i.e., $\{1\}$), then $hk = kh$ for every $h \in H$ and $k \in K$.

Proof. We did this in connection with direct products; see the beginning of the proof of (1.5.2). ♣

5.5.3 Proposition

If P is a nontrivial finite p-group, then P has a nontrivial center.

Proof. Let P act on itself by conjugation; see (5.1.3) and (5.2.2), Example 3. The orbits are the conjugacy classes of P. The element x belongs to an orbit of size 1 iff x is in the center $Z(P)$, since $gxg^{-1} = x$ for all $g \in P$ iff $gx = xg$ for all $g \in P$ iff $x \in Z(P)$. By the orbit-stabilizer theorem, an orbit size that is greater than 1 must divide $|P|$, and therefore must be a positive power of p. If $Z(P) = \{1\}$, then we have one orbit of size 1, with all other orbit sizes $\equiv 0 \bmod p$. Thus $|P| \equiv 1 \bmod p$, contradicting the assumption that P is a nontrivial p-group. ♣

5.5.4 Lemma

P is a normal Sylow p-subgroup of G if and only if P is the unique Sylow p-subgroup of G.

Proof. By Sylow (3), the Sylow p-subgroups form a single equivalence class of conjugate subgroups. This equivalence class consists of a single element $\{P\}$ iff $gPg^{-1} = P$ for every $g \in G$, that is, iff $P \trianglelefteq G$. ♣

5.5.5 Proposition

Let G be a finite, nonabelian simple group. If the prime p divides the order of G, then the number n_p of Sylow p-subgroups of G is greater than 1.

Proof. If p is the only prime divisor of $|G|$, then G is a nontrivial p-group, hence $Z(G)$ is nontrivial by (5.5.3). Since $Z(G) \trianglelefteq G$ (see (5.1.3), Example 3), $Z(G) = G$, so that G is abelian, a contradiction. Thus $|G|$ is divisible by at least two distinct primes, so if P is a Sylow p-subgroup, then $\{1\} < P < G$. If $n_p = 1$, then there is a unique Sylow p-subgroup P, which is normal in G by (5.5.4). This contradicts the simplicity of G, so we must have $n_p > 1$. ♣

We can now derive some properties of groups whose order is the product of two distinct primes.

5.5.6 Proposition

Let G be a group of order pq, where p and q are distinct primes.

(i) If $q \not\equiv 1 \bmod p$, then G has a normal Sylow p-subgroup.

(ii) G is not simple.

(iii) If $p \not\equiv 1 \bmod q$ and $q \not\equiv 1 \bmod p$, then G is cyclic.

Proof. (i) By Sylow (2), $n_p \equiv 1 \bmod p$ and $n_p | q$, so $n_p = 1$. The result follows from (5.5.4).

(ii) We may assume without loss of generality that $p > q$. Then p cannot divide $q - 1$, so $q \not\equiv 1 \bmod p$. By (i), G has a normal Sylow p-subgroup, so G is not simple.

(iii) By (i), G has a normal Sylow p-subgroup P and a normal Sylow q-subgroup Q. Since P and Q are of prime order (p and q, respectively), they are cyclic. If x generates P and y generates Q, then $xy = yx$ by (5.5.2). [P and Q have trivial intersection because any member of the intersection has order dividing both p and q.] But then xy has order $pq = |G|$ (see Section 1.1, Problem 8). Thus $G = \langle xy \rangle$. ♣

We now look at the more complicated case $|G| = p^2q$. The combinatorial argument in the next proof is very interesting.

5.5.7 Proposition

Suppose that the order of the finite group G is p^2q, where p and q are distinct primes. Then G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup. Thus G is not simple.

Proof. If the conclusion is false then n_p and n_q are both greater than 1. By Sylow (2), n_q divides p^2, so $n_q = p$ or p^2, and we will show that the second case leads to a contradiction. A Sylow q-subgroup Q is of order q and is therefore cyclic. Furthermore, every element of Q except the identity is a generator of Q. Conversely, any element of order q generates a Sylow q-subgroup. Since the only divisors of q are 1 and q, any two distinct Sylow q-subgroups have trivial intersection. Thus the number of elements of G of order q is exactly $n_q(q-1)$. If $n_q = p^2$, then the number of elements that are *not* of order q is

$$p^2q - p^2(q-1) = p^2.$$

Now let P be any Sylow p-subgroup of G. Then $|P| = p^2$, so no element of P can have order q (the orders must be 1, p or p^2). Since there are only p^2 elements of order unequal to q available, P takes care of all of them. Thus there cannot be another Sylow p-subgroup, so $n_p = 1$, a contradiction. We conclude that n_q must be p. Now by Sylow (2), $n_q \equiv 1 \bmod q$, hence $p \equiv 1 \bmod q$, so $p > q$. But n_p divides q, a prime, so $n_p = q$. Since $n_p \equiv 1 \bmod p$, we have $q \equiv 1 \bmod p$, and consequently $q > p$. Our original assumption that both n_p and n_q are greater than one has led inexorably to a contradiction. ♣

Problems For Section 5.5

1. Show that every group of order 15 is cyclic.
2. If $G/Z(G)$ is cyclic, show that $G = Z(G)$, and therefore G is abelian.
3. Show that for prime p, every group of order p^2 is abelian.
4. Let G be a group with $|G| = pqr$, where p, q and r are distinct primes and (without loss of generality) $p > q > r$. Show that $|G| \geq 1 + n_p(p-1) + n_q(q-1) + n_r(r-1)$.
5. Continuing Problem 4, if G is simple, show that n_p, n_q and n_r are all greater than 1. Then show that $n_p = qr$, $n_q \geq p$ and $n_r \geq q$.
6. Show that a group whose order is the product of three distinct primes is not simple.
7. Let G be a simple group of order p^rm, where $r \geq 1$, $m > 1$, and the prime p does not divide m. Let $n = n_p$ be the number of Sylow p-subgroups of G. If $H = N_G(P)$, where P is a Sylow p-subgroup of G, then $[G : H] = n$ (see Problem 1 of Section 5.4). Show that P cannot be normal in G (hence $n > 1$), and conclude that $|G|$ must divide $n!$.
8. If G is a group of order $250,000 = 2^45^6$, show that G is not simple.

5.6 Composition Series

5.6.1 Definitions and Comments

One way to break down a group into simpler components is via a *subnormal series*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G.$$

"Subnormal" means that each subgroup G_i is normal in its successor G_{i+1}. In a *normal series*, the G_i are required to be normal subgroups of the entire group G. For convenience, the trivial subgroup $\{1\}$ will be written as 1.

Suppose that G_i is not a maximal normal subgroup of G_{i+1}, equivalently (by the correspondence theorem) G_{i+1}/G_i is not simple. Then the original subnormal series can be *refined* by inserting a group H such that $G_i \triangleleft H \triangleleft G_{i+1}$. We can continue refining in the hope that the process will terminate (it always will if G is finite). If all factors G_{i+1}/G_i are simple, we say that the group G has a *composition series.* [By convention, the trivial group has a composition series, namely $\{1\}$ itself.]

The Jordan-Hölder theorem asserts that if G has a composition series, the resulting *composition length* r and the *composition factors* G_{i+1}/G_i are unique (up to isomorphism and rearrangement). Thus all refinements lead to essentially the same result. Simple groups therefore give important information about arbitrary groups; if G_1 and G_2 have different composition factors, they cannot be isomorphic.

Here is an example of a composition series. Let S_4 be the group of all permutations of $\{1, 2, 3, 4\}$, and A_4 the subgroup of even permutations (normal in S_4 by Section 1.3, Problem 6). Let V be the four group (Section 1.2, Problem 6; normal in A_4, in fact in S_4, by direct verification). Let $\mathbb{Z}_2$ be any subgroup of V of order 2. Then

$$1 \triangleleft \mathbb{Z}_2 \triangleleft V \triangleleft A_4 \triangleleft S_4.$$

The proof of the Jordan-Hölder theorem requires some technical machinery.

5.6.2 Lemma

(i) If $K \trianglelefteq H \le G$ and f is a homomorphism on G, then $f(K) \trianglelefteq f(H)$.

(ii) If $K \trianglelefteq H \le G$ and $N \trianglelefteq G$, then $NK \trianglelefteq NH$.

(iii) If A, B, C and D are subgroups of G with $A \trianglelefteq B$ and $C \trianglelefteq D$, then $A(B \cap C) \trianglelefteq A(B \cap D)$, and by symmetry, $C(D \cap A) \trianglelefteq C(D \cap B)$.

(iv) In (iii), $A(B \cap C) \cap B \cap D = C(D \cap A) \cap D \cap B$.
Equivalently, $A(B \cap C) \cap D = C(D \cap A) \cap B$.

Proof. (i) For $h \in H, k \in K$, we have $f(h)f(k)f(h)^{-1} = f(hkh^{-1}) \in f(K)$.

(ii) Let f be the canonical map of G onto G/N. By (i) we have $NK/N \trianglelefteq NH/N$. The result follows from the correspondence theorem.

(iii) Apply (ii) with $G = B, N = A, K = B \cap C, H = B \cap D$.

(iv) The two versions are equivalent because $A(B \cap C) \le B$ and $C(D \cap A) \le D$. If x belongs to the set on the left, then $x = ac$ for some $a \in A, c \in B \cap C$, and x also belongs to D. But $x = c(c^{-1}ac) = ca^*$ for some $a^* \in A \trianglelefteq B$. Since $x \in D$ and $c \in C \leq D$, we have $a^* \in D$, hence $a^* \in D \cap A$. Thus $x = ca^* \in C(D \cap A)$, and since $x = ac$, with $a \in A \leq B$ and $c \in B \cap C \leq B$, $x \in C(D \cap A) \cap B$. Therefore the left side is a subset of the right side, and a symmetrical argument completes the proof. ♣

The diagram below is helpful in visualizing the next result.

$$\begin{array}{ccc} B & | & D \\ & | & \\ A & | & C \end{array}$$

To keep track of symmetry, take mirror images about the dotted line. Thus the group A will correspond to C, B to D, $A(B \cap C)$ to $C(D \cap A)$, and $A(B \cap D)$ to $C(D \cap B)$.

5.6.3 Zassenhaus Lemma

Let A, B, C and D be subgroups of G, with $A \trianglelefteq B$ and $C \trianglelefteq D$. Then

$$\frac{A(B \cap D)}{A(B \cap C)} \cong \frac{C(D \cap B)}{C(D \cap A)}.$$

Proof. By part (iii) of (5.6.2), the quotient groups are well-defined. An element of the group on the left is of the form $ayA(B \cap C), a \in A, y \in B \cap D$. But $ay = y(y^{-1}ay) = ya^*$, $a^* \in A$. Thus $ayA(B \cap C) = ya^*A(B \cap C) = yA(B \cap C)$. Similarly, an element of the right side is of the form $zC(D \cap A)$ with $z \in D \cap B = B \cap D$. Thus if $y, z \in B \cap D$, then

$$yA(B \cap C) = zA(B \cap C) \text{ iff } z^{-1}y \in A(B \cap C) \cap B \cap D$$

and by part (iv) of (5.6.2), this is equivalent to

$$z^{-1}y \in C(D \cap A) \cap D \cap B \text{ iff } yC(D \cap A) = zC(D \cap A).$$

Thus if h maps $yA(B \cap C)$ to $yC(D \cap A)$, then h is a well-defined bijection from the left to the right side of Zassenhaus' equation. By definition of multiplication in a quotient group, h is an isomorphism. ♣

5.6.4 Definitions and Comments

If a subnormal series is refined by inserting H between G_i and G_{i+1}, let us allow H to coincide with G_i or G_{i+1}. If all such insertions are strictly between the "endgroups", we will speak of a *proper refinement*. Two series are *equivalent* if they have the same length and their factor groups are the same, up to isomorphism and rearrangement.

5.6.5 Schreier Refinement Theorem

Let $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$ and $1 = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_s = G$ be two subnormal series for the group G. Then the series have equivalent refinements.

Proof. Let $H_{ij} = H_i(H_{i+1} \cap K_j)$, $K_{ij} = K_j(K_{j+1} \cap H_i)$. By Zassenhaus we have

$$\frac{H_{i,j+1}}{H_{ij}} \cong \frac{K_{i+1,j}}{K_{ij}}.$$

(In (5.6.3) take $A = H_i$, $B = H_{i+1}$, $C = K_j$, $D = K_{j+1}$). We can now construct equivalent refinements; the easiest way to see this is to look at a typical concrete example. The first refinement will have r blocks of length s, and the second will have s blocks of length r. Thus the length will be rs in both cases. With $r = 2$ and $s = 3$, we have

$$1 = H_{00} \trianglelefteq H_{01} \trianglelefteq H_{02} \trianglelefteq H_{03} = H_1 = H_{10} \trianglelefteq H_{11} \trianglelefteq H_{12} \trianglelefteq H_{13} = H_2 = G,$$
$$1 = K_{00} \trianglelefteq K_{10} \trianglelefteq K_{20} = K_1 = K_{01} \trianglelefteq K_{11} \trianglelefteq K_{21} = K_2 = K_{02} \trianglelefteq K_{12} \trianglelefteq K_{22} = K_3 = G.$$

The corresponding factor groups are

$$H_{01}/H_{00} \cong K_{10}/K_{00},\ H_{02}/H_{01} \cong K_{11}/K_{01},\ H_{03}/H_{02} \cong K_{12}/K_{02}$$
$$H_{11}/H_{10} \cong K_{20}/K_{10},\ H_{12}/H_{11} \cong K_{21}/K_{11},\ H_{13}/H_{12} \cong K_{22}/K_{12}.$$

(Notice the pattern; in each isomorphism, the first subscript in the numerator is increased by 1 and the second subscript is decreased by 1 in going from left to right. The subscripts in the denominator are unchanged.) The factor groups of the second series are a reordering of the factor groups of the first series. ♣

The hard work is now accomplished, and we have everything we need to prove the main result.

5.6.6 Jordan-Hölder Theorem

If G has a composition series S (in particular if G is finite), then any subnormal series R without repetition can be refined to a composition series. Furthermore, any two composition series for G are equivalent.

Proof. By (5.6.5), R and S have equivalent refinements. Remove any repetitions from the refinements to produce equivalent refinements R_0 and S_0 without repetitions. But a composition series has no proper refinements, hence $S_0 = S$, proving the first assertion. If R is also a composition series, then $R_0 = R$ as well, and R is equivalent to S. ♣

Problems For Section 5.6

1. Show that if G has a composition series, so does every normal subgroup of G.
2. Give an example of a group that has no composition series.
3. Give an example of two nonisomorphic groups with the same composition factors, up to rearrangement.

Problems 4–9 will prove that the alternating group A_n is simple for all $n \geq 5$. (A_1 and A_2 are trivial and hence not simple; A_4 is not simple by the example given in (5.6.1); A_3 is cyclic of order 3 and is therefore simple.) In these problems, N stands for a normal subgroup of A_n.

4. Show that if $n \geq 3$, then A_n is generated by 3-cycles.
5. Show that if N contains a 3-cycle, then it contains all 3-cycles, so that $N = A_n$.
6. From now on, assume that N is a *proper* normal subgroup of A_n, and $n \geq 5$. Show that no permutation in N contains a cycle of length 4 or more.
7. Show that no permutation in N contains the product of two disjoint 3-cycles. Thus in view of Problems 4,5 and 6, every member of N is the product of an even number of disjoint transpositions.
8. In Problem 7, show that the number of transpositions in a nontrivial member of N must be at least 4.
9. Finally, show that the assumption that N contains a product of 4 or more disjoint transpositions leads to a contradiction, proving that $N = 1$, so that A_n is simple. It follows that a composition series for S_n is $1 \triangleleft A_n \triangleleft S_n$.
10. A *chief series* is a normal series without repetition that cannot be properly refined to another normal series. Show that if G has a chief series, then any normal series without repetition can be refined to a chief series. Furthermore, any two chief series of a given group are equivalent.
11. In a composition series, the factor groups G_{i+1}/G_i are required to be simple. What is the analogous condition for a chief series?

5.7 Solvable And Nilpotent Groups

Solvable groups are so named because of their connection with solvability of polynomial equations, a subject to be explored in the next chapter. To get started, we need a property of subgroups that is stronger than normality.

5.7.1 Definitions and Comments

A subgroup H of the group G is *characteristic* (in G) if for each automorphism f of G, $f(H) = H$. Thus f restricted to H is an automorphism of H. Consequently, if H is characteristic in G, then it is normal in G. If follows from the definition that if H is characteristic in K and K is characteristic in G, then H is characteristic in G. Another useful result is the following.

(1) If H is characteristic in K and K is normal in G, then H is normal in G.

To see this, observe that any inner automorphism of G maps K to itself, so restricts to an automorphism (not necessarily inner) of K. Further restriction to H results in an automorphism of H, and the result follows.

5.7.2 More Definitions and Comments

The *commutator subgroup* G' of a group G is the subgroup generated by all *commutators* $[x, y] = xyx^{-1}y^{-1}$. (Since $[x, y]^{-1} = [y, x]$, G' consists of all finite products of commutators.) Here are some basic properties.

(2) G' is characteristic in G.

This follows because any automorphism f maps a commutator to a commutator: $f[x,y] = [f(x), f(y)]$.

(3) G is abelian if and only if G' is trivial.

This holds because $[x,y] = 1$ iff $xy = yx$.

(4) G/G' is abelian. Thus forming the quotient of G by G', sometimes called *modding out by* G', in a sense "abelianizes" the group.

For $G'xG'y = G'yG'x$ iff $G'xy = G'yx$ iff $xy(yx)^{-1} \in G'$ iff $xyx^{-1}y^{-1} \in G'$, and this holds for all x and y by definition of G'.

(5) If $N \trianglelefteq G$, then G/N is abelian if and only if $G' \leq N$.

The proof of (4) with G' replaced by N shows that G/N is abelian iff all commutators belong to N, that is, iff $G' \leq N$.

The process of taking commutators can be iterated:

$$G^{(0)} = G,\ G^{(1)} = G',\ G^{(2)} = (G')',$$

and in general,

$$G^{(i+1)} = (G^{(i)})',\ i = 0, 1, 2, \dots .$$

Since $G^{(i+1)}$ is characteristic in $G^{(i)}$, an induction argument shows that each $G^{(i)}$ is characteristic, hence normal, in G.

The group G is said to be *solvable* if $G^{(r)} = 1$ for some r. We then have a normal series

$$1 = G^{(r)} \trianglelefteq G^{(r-1)} \trianglelefteq \cdots \trianglelefteq G^{(0)} = G$$

called the *derived series* of G.

Every abelian group is solvable, by (3). Note that a group that is both simple and solvable must be cyclic of prime order. For the normal subgroup G' must be trivial; if it were G, then the derived series would never reach 1. By (3), G is abelian, and by (5.5.1), G must be cyclic of prime order.

A nonabelian simple group G (such as $A_n, n \geq 5$) cannot be solvable. For if G is nonabelian, then G' is not trivial. Thus $G' = G$, and as in the previous paragraph, the derived series will not reach 1.

There are several equivalent ways to describe solvability.

5.7.3 Proposition

The following conditions are equivalent.

(i) G is solvable.

(ii) G has a normal series with abelian factors.

(iii) G has a subnormal series with abelian factors.

Proof. Since (i) implies (ii) by (4) and (ii) implies (iii) by definition of normal and subnormal series, the only problem is (iii) implies (i). Suppose G has a subnormal series

$$1 = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

with abelian factors. Since G/G_1 is abelian, we have $G' \leq G_1$ by (5), and an induction argument then shows that $G^{(i)} \leq G_i$ for all i. [The inductive step is $G^{(i+1)} = (G^{(i)})' \leq G_i' \leq G_{i+1}$ since G_i/G_{i+1} is abelian.] Thus $G^{(r)} \leq G_r = 1$. ♣

The next result gives some very useful properties of solvable groups.

5.7.4 Proposition

Subgroups and quotients of a solvable group are solvable. Conversely, if N is a normal subgroup of G and both N and G/N are solvable, then G is solvable.

Proof. If H is a subgroup of the solvable group G, then H is solvable because $H^{(i)} \leq G^{(i)}$ for all i. If N is a normal subgroup of the solvable group G, observe that commutators of G/N look like $xyx^{-1}y^{-1}N$, so $(G/N)' = G'N/N$. (Not G'/N, since N is not necessarily a subgroup of G'.) Inductively,

$$(G/N)^{(i)} = G^{(i)}N/N$$

and since N/N is trivial, G/N is solvable. Conversely, suppose that we have a subnormal series from $N_0 = 1$ to $N_r = N$, and a subnormal series from $G_0/N = 1$ (i.e., $G_0 = N$) to $G_s/N = G/N$ (i.e., $G_s = G$) with abelian factors in both cases. Then we splice the series of N_i's to the series of G_i's. The latter series is subnormal by the correspondence theorem, and the factors remain abelian by the third isomorphism theorem. ♣

5.7.5 Corollary

If G has a composition series, in particular if G is finite, then G is solvable if and only if the composition factors of G are cyclic of prime order.

Proof. Let G_{i+1}/G_i be a composition factor of the solvable group G. By (5.7.4), G_{i+1} is solvable, and again by (5.7.4), G_{i+1}/G_i is solvable. But a composition factor must be a simple group, so G_{i+1}/G_i is cyclic of prime order, as observed in (5.7.2). Conversely, if the composition factors of G are cyclic of prime order, then the composition series is a subnormal series with abelian factors. ♣

Nilpotent groups arise from a different type of normal series. We will get at this idea indirectly, and give an abbreviated treatment.

5.7.6 Proposition

If G is a finite group, the following conditions are equivalent, and define a *nilpotent group*. [Nilpotence of an arbitrary group will be defined in (5.7.8).]

(a) G is the direct product of its Sylow subgroups.

(b) Every Sylow subgroup of G is normal.

Proof. (a) implies (b): By (1.5.3), the factors of a direct product are normal subgroups.

(b) implies (a): By (5.5.4), there is a unique Sylow p_i-subgroup H_i for each prime divisor p_i of $|G|, i = 1, \dots, k$. By successive application of (5.2.4), we have $|H_1 \cdots H_k| = |H_1| \cdots |H_k|$, which is $|G|$ by definition of Sylow p-subgroup. Since all sets are finite, $G = H_1 \cdots H_k$. Furthermore, each $H_i \cap \prod_{j \neq i} H_j$ is trivial, because the orders of the H_i are powers of distinct primes. By (1.5.4), G is the direct product of the H_i. ♣

5.7.7 Corollary

Every finite abelian group and every finite p-group is nilpotent.

Proof. A finite abelian group must satisfy condition (b) of (5.7.6). If P is a finite p-group, then P has only one Sylow subgroup, P itself, so the conditions of (5.7.6) are automatically satisfied. ♣

We now connect this discussion with normal series. Suppose that we are trying to build a normal series for the group G, starting with $G_0 = 1$. We take G_1 to be $Z(G)$, the center of G; we have $G_1 \trianglelefteq G$ by (5.1.3), Example 3. We define G_2 by the correspondence theorem:

$$G_2/G_1 = Z(G/G_1)$$

and since $Z(G/G_1) \trianglelefteq G/G_1$, we have $G_2 \trianglelefteq G$. In general, we take

$$G_i/G_{i-1} = Z(G/G_{i-1}),$$

and by induction we have $G_i \trianglelefteq G$. The difficulty is that there is no guarantee that G_i will ever reach G. However, we will succeed if G is a finite p-group. The key point is that a nontrivial finite p-group has a nontrivial center, by (5.5.3). Thus by induction, G_i/G_{i-1} is nontrivial for every i, so $G_{i-1} < G_i$. Since G is finite, it must eventually be reached.

5.7.8 Definitions and Comments

A *central series* for G is a normal series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$ such that $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$ for every $i = 1, \dots, r$. (The series just discussed is a special case called the *upper central series.*) An arbitrary group G is said to be *nilpotent* if it has a central series. Thus a finite p-group is nilpotent, and in particular, every Sylow p-subgroup is nilpotent. Now a direct product of a finite number of nilpotent groups is nilpotent. (If G_{ij} is the i^{th} term of a central series of the j^{th} factor H_j, with $G_{ij} = G$ if the series has already terminated at G, then $\prod_j G_{ij}$ will be the i^{th} term of a central series for $\prod_j H_j$.) Thus a finite group that satisfies the conditions of (5.7.6) has a central series. Conversely, it can be shown that a finite group that has a central series satisfies (5.7.6), so the two definitions of nilpotence agree for finite groups.

Note that a nilpotent group is solvable. For if $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$, then the elements of G_i/G_{i-1} commute with each other since they commute with everything in G/G_{i-1}; thus G_i/G_{i-1} is abelian. Consequently, a finite p-group is solvable.

Problems For Section 5.7

1. Give an example of a nonabelian solvable group.
2. Show that a solvable group that has a composition series must be finite.
3. Prove directly (without making use of nilpotence) that a finite p-group is solvable.
4. Give an example of a solvable group that is not nilpotent.
5. Show that if $n \geq 5$, then S_n is not solvable.
6. If P is a finite simple p-group, show that P has order p.
7. Let P be a nontrivial finite p-group. Show that P has a normal subgroup N whose index $[P : N]$ is p.
8. Let G be a finite group of order $p^r m$, where r is a positive integer and p does not divide m. Show that for any $k = 1, 2, \dots, r$, G has a subgroup of order p^k.
9. Give an example of a group G with a normal subgroup N such that N and G/N are abelian, but G is not abelian. (If "abelian" is replaced by "solvable", no such example is possible, by (5.7.4).)
10. If G is a solvable group, its *derived length*, $\mathrm{dl}(G)$, is the smallest nonnegative integer r such that $G^{(r)} = 1$. If N is a normal subgroup of the solvable group G, what can be said about the relation between $\mathrm{dl}(G)$, $\mathrm{dl}(N)$ and $\mathrm{dl}(G/N)$?

5.8 Generators And Relations

In (1.2.4) we gave an informal description of the dihedral group via generators and relations, and now we try to make the ideas more precise.

5.8.1 Definitions and Comments

The *free group* G on the set S (or the *free group with basis* S) consists of all *words* on S, that is, all finite sequences $x_1 \cdots x_n$, $n = 0, 1, \dots$, where each x_i is either an element of S or the inverse of an element of S. We regard the case $n = 0$ as the *empty word* λ. The group operation is concatenation, subject to the constraint that if s and s^{-1} occur in succession, they can be cancelled. The empty word is the identity, and inverses are calculated in the only reasonable way, for example, $(stu)^{-1} = u^{-1}t^{-1}s^{-1}$. We say that G is *free on* S.

Now suppose that G is free on S, and we attempt to construct a homomorphism f from G to an arbitrary group H. The key point is that f is completely determined by its values on S. If $f(s_1) = a$, $f(s_2) = b$, $f(s_3) = c$, then

$$f(s_1 s_2^{-1} s_3) = f(s_1) f(s_2)^{-1} f(s_3) = ab^{-1}c.$$

Here is the formal statement, followed by an informal proof.

5.8.2 Theorem

If G is free on S and g is an arbitrary function from S to a group H, then there is a unique homomorphism $f \colon G \to H$ such that $f = g$ on S.

Proof. The above discussion is a nice illustration of a concrete example with all the features of the general case. The analysis shows both existence and uniqueness of f. A formal proof must show that all aspects of the general case are covered. For example, if $u = s_1 s_2^{-1} s_3$ and $v = s_1 s_2^{-1} s_4^{-1} s_4 s_3$, then $f(u) = f(v)$, so that cancellation of $s_4^{-1} s_4$ causes no difficulty. Specific calculations of this type are rather convincing, and we will not pursue the formal details. (See, for example, Rotman, An Introduction to the Theory of Groups, pp. 343–345.) ♣

5.8.3 Corollary

Any group H is a homomorphic image of a free group.

Proof. Let S be a set of generators for H (if necessary, take $S = H$), and let G be free on S. Define $g(s) = s$ for all $s \in S$. If f is the unique extension of g to G, then since S generates H, f is an epimorphism. ♣

Returning to (1.2.4), we described a group H using generators R and F, and relations $R^n = I$, $F^2 = I$, $RF = FR^{-1}$. The last relation is equivalent to $RFRF = I$, since $F^2 = I$. The words R^n, F^2 and $RFRF$ are called *relators*, and the specification of generators and relations is called a *presentation*. We use the notation

$$H = \langle R, F \mid R^n, F^2, RFRF \rangle$$

or the long form

$$H = \langle R, F \mid R^n = I, F^2 = I, RF = FR^{-1} \rangle.$$

We must say precisely what it means to define a group by generators and relations, and show that the above presentation yields a group isomorphic to the dihedral group D_{2n}. We start with the free group on $\{R, F\}$ and set all relators equal to the identity. It is natural to mod out by the subgroup generated by the relators, but there is a technical difficulty; this subgroup is not necessarily normal.

5.8.4 Definition

Let G be free on the set S, and let K be a subset of G. We define the group $\langle S \mid K\rangle$ as $G/\overline{K}$, where $\overline{K}$ is the smallest normal subgroup of G containing K.

Unfortunately, it is a theorem of mathematical logic that there is no algorithm which when given a presentation, will find the order of the group. In fact, there is no algorithm to determine whether a given word of $\langle S \mid K\rangle$ coincides with the identity. Logicians say that the word problem for groups is unsolvable. But although there is no general solution, there are specific cases that can be analyzed, and the following result is very helpful.

5.8.5 Von Dyck's Theorem

Let $H = \langle S \mid K\rangle$ be a presentation, and let L be a group that is generated by the words in S. If L satisfies all the relations of K, then there is an epimorphism $\alpha\colon H \to L$. Consequently, $|H| \ge |L|$.

Proof. Let G be free on S, and let i be the identity map from S, regarded as a subset of G, to S, regarded as a subset of L. By (5.8.2), i has a unique extension to a homomorphism f of G into L, and in fact f is an epimorphism because S generates L. Now f maps any word of G to the same word in L, and since L satisfies all the relations, we have $K \subseteq \ker f$. But the kernel of f is a normal subgroup of G, hence $\overline{K} \subseteq \ker f$. The factor theorem provides an epimorphism $\alpha\colon G/\overline{K} \to L$. ♣

5.8.6 Justifying a presentation

If L is a finite group generated by the words of S, then in practice, the crucial step in identifying L with $H = \langle S \mid K\rangle$ is a proof that $|H| \le |L|$. If we can accomplish this, then by (5.8.5), $|H| = |L|$. In this case, α is a surjective map of finite sets of the same size, so α is injective as well, hence is an isomorphism. For the dihedral group we have $H = \langle F, R \mid R^n, F^2, RFRF\rangle$ and $L = D_{2n}$. In (1.2.4) we showed that each word of H can be expressed as R^iF^j with $0 \le i \le n-1$ and $0 \le j \le 1$. Therefore $|H| \le 2n = |D_{2n}| = |L|$. Thus the presentation H is a legitimate description of the dihedral group.

Problems For Section 5.8

1. Show that a presentation of the cyclic group of order n is $\langle a \mid a^n\rangle$.
2. Show that the quaternion group (see (2.1.3, Example 4)) has a presentation $\langle a, b \mid a^4 = 1, b^2 = a^2, ab = ba^{-1}\rangle$.
3. Show that $H = \langle a, b \mid a^3 = 1, b^2 = 1, ba = a^{-1}b\rangle$ is a presentation of S_3.
4. Is the presentation of a group unique?

In Problems 5–11, we examine a different way of assembling a group from subgroups, which generalizes the notion of a direct product. Let N be a normal subgroup of G, and H an arbitrary subgroup. We say that G is the *semidirect product* of N by H if $G = NH$ and $N \cap H = 1$. (If $H \trianglelefteq G$, we have the direct product.) For notational convenience, the letter n, possibly with subscripts, will always indicate a member of N, and similarly h will always belong to H. In Problems 5 and 6, we assume that G is the semidirect product of N by H.

5. If $n_1h_1 = n_2h_2$, show that $n_1 = n_2$ and $h_1 = h_2$.
6. If $i\colon N \to G$ is inclusion and $\pi\colon G \to H$ is projection ($\pi(nh) = h$), then the sequence

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "i"] & G \arrow[r, "\pi"] & H \arrow[r] & 1 \end{tikzcd}$$

   is exact. Note that π is well-defined by Problem 5, and verify that π is a homomorphism. Show that the sequence *splits on the right*, i.e., there is a homomorphism $\psi\colon H \to G$ such that $\pi \circ \psi = 1$.
7. Conversely, suppose that the above exact sequence splits on the right. Since ψ is injective, we can regard H (and N as well) as subgroups of G, with ψ and i as inclusion maps. Show that G is the semidirect product of N by H.
8. Let N and H be arbitrary groups, and let f be a homomorphism of H into $\operatorname{Aut} N$, the group of automorphisms of N. Define a multiplication on $G = N \times H$ by

$$(n_1, h_1)(n_2, h_2) = (n_1 f(h_1)(n_2), h_1h_2).$$

   [$f(h_1)(n_2)$ is the value of the automorphism $f(h_1)$ at the element n_2.] A lengthy but straightforward calculation shows that G is a group with identity $(1, 1)$ and inverses given by $(n, h)^{-1} = (f(h^{-1})(n^{-1}), h^{-1})$. Show that G is the semidirect product of $N \times \{1\}$ by $\{1\} \times H$.
9. Show that every semidirect product arises from the construction of Problem 8.
10. Show by example that it is possible for a short exact sequence of groups to split on the right but not on the left.

    [If $h\colon G \to N$ is a left-splitting map in the exact sequence of Problem 6, then h and π can be used to identify G with the direct product of N and H. Thus a left-splitting implies a right-splitting, but, unlike the result for modules in (4.7.4), not conversely.]
11. Give an example of a short exact sequence of groups that does not split on the right.
12. (The Frattini argument, frequently useful in a further study of group theory.) Let N be a normal subgroup of the finite group G, and let P be a Sylow p-subgroup of N. If $N_G(P)$ is the normalizer of P in G, show that $G = N_G(P)N$ ($= NN_G(P)$ by (1.4.3)).[If $g \in G$, look at the relation between P and gPg^{-1}.]
13. Let $N = \{1, a, a^2, \dots, a^{n-1}\}$ be a cyclic group of order n, and let $H = \{1, b\}$ be a cyclic group of order 2. Define $f\colon H \to \operatorname{Aut} N$ by taking $f(b)$ to be the automorphism that sends a to a^{-1}. Show that the dihedral group D_{2n} is the semidirect product of N by H. (See Problems 8 and 9 for the construction of the semidirect product.)
14. In Problem 13, replace N by an infinite cyclic group

$$\{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}.$$

    Give a presentation of the semidirect product of N by H. This group is called the *infinite dihedral group* D_∞.

Concluding Remarks

Suppose that the finite group G has a composition series

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G.$$

If $H_i = G_i/G_{i-1}$, then we say that G_i is an *extension of* G_{i-1} *by* H_i in the sense that $G_{i-1} \trianglelefteq G_i$ and $G_i/G_{i-1} \cong H_i$. If we were able to solve the extension problem (find all possible extensions of G_{i-1} by H_i) and we had a catalog of all finite simple groups, then we could build a catalog of all finite groups. This sharpens the statement made in (5.6.1) about the importance of simple groups.