10 Group Structure: Extensions

10.1 Toward Classifying Finite Groups

For a fixed integer n, we attempt to identify all the groups of order n. In general, this is an extremely complex task, but we now have many of the construction tools handy and can at least handle many groups of small order. The Sylow theorems guarantee certain important subgroups and the Fundamental Homomorphism Theorem will allow us to build up from any normal subgroups we find.

We say G is an "extension of K by Q" if G has a normal subgroup K_0 isomorphic to K and G/K_0 is isomorphic to Q. Some groups are extensions of K by Q and have an additional property: there is a subgroup $Q_0 \leq G$ isomorphic to Q and $K_0 \cap Q_0 = \{1\}$. This is a special case ....

Let G be a group with nontrivial subgroups K and Q such that $KQ = G$ and $K \cap Q = \{1\}$. Then we say that Q is a **complement** of K in G. If both K and Q are normal in G then G is the internal direct product of K and Q and we write $G \cong K \times Q$. If one of the subgroups, say Q, is not normal, but the other is, we still have considerable information about G, for we know both K and $G/K \cong Q$. In this case, G is an extension of K by Q and furthermore, Q is visible in G. (This is a "split" extension.)

10.2 Semi-direct products

The Sylow theorems provide a great deal of information about finite groups. One more important concept is needed before we tackle the groups of small order (say, order less than 60.) We need the concept of semidirect product.

Let G be a group with subgroups Q, K such that

1. $G = KQ$,
2. $K \trianglelefteq G$
3. $K \cap Q = \{1\}$.

Then G is said to be a **semidirect product** of K and Q, written $K \rtimes Q$. (The little triangle in this notation implies that K is the normal subgroup.)

Note that if $G = K \rtimes Q$ then $G/K \cong Q$. If Q too is a normal subgroup then the elements of Q commute with the elements of K (show this!) and so G is just the direct product of K and Q. Thus the "semi" direct product is a generalization of the direct product.

If $G = K \rtimes Q$ then every element of G may be written in the form $g = kq$ where $k \in K, q \in Q$. Given $k \in K, q \in Q$, we know that $qkq^{-1} \in K$ and so the conjugation map $\phi_q : K \to K$ is an automorphism of K. This is worth stressing: *each* element of Q acts on K by conjugation. That is, given $G = K \rtimes Q$, we may identify q with the function $\phi_q : K \to K$ where $\phi_q(k) = qkq^{-1}$.

Thus we can construct G if we know the structure of K, the structure of Q, and if we know the automorphism group of K.

What if we don't know G? Suppose we are given K and Q and are asked to create all semidirect products $K \rtimes Q$? We may do this by recognizing that each element of Q, naturally identified with ϕ_q, must be further identified with an automorphism of Q. Therefore we need a map $\theta : Q \to Aut(K)$. If we can identify $\theta(q)$ for all $q \in Q$ then we will $define$ the group G by identifying ϕ_q with $\theta(q)$ and so, for all $q \in Q, k \in K$,

$$qkq^{-1} = \theta(q)(k).$$

Therefore $q \cdot k = [\theta(q)(k)] \cdot q$. More generally, given two elements $k_1 q_1$ and $k_2 q_2$ in G, we multiply them as follows:

$$(k_1 q_1)(k_2 q_2) = k_1(q_1 k_2)q_2 = k_1([\theta(q_1)(k_2)]q_1)q_2 = (k_1[\theta_{q_1}(k_2)])(q_1 q_2).$$

When θ is clearly defined, we will emphasize this by writing $G = K \rtimes_\theta Q$.

Some authors use the previous computation and so define the semidirect product as an operation on a set of ordered pairs: $K \rtimes_\theta Q := \{(h,q) : q \in Q, k \in K\}$ with operation

$$(k_1 q_1, k_2 q_2) = (k_1 \theta_{q_1}(k_2), q_1 q_2).$$

If we are to construct a group using $Aut(K)$ and a function $\theta : Q \to Aut(K)$ then for any $q_1, q_2 \in Q$ we require, by the associative law, that for all $k \in K$,

$$q_2(q_1 k q_1^{-1})q_2^{-1} = (q_2 q_1)k(q_2 q_1)^{-1},$$

in other words, $\theta_{q_2}\theta_{q_1} = \theta_{q_2 q_1}$. The function θ is therefore a group homomorphism from Q into the group of automorphisms of K.

This is important; we know how to build homomorphisms!

If θ is the trivial map, that is, $\theta(q) = 1_{Aut(K)}$ for all $q \in Q$, then the elements of Q commute with the elements of K and so $K \rtimes_\theta Q = K \times Q$.

If G is metabelian then there is a normal *abelian* subgroup K and G/K is also abelian. We will concentrate (in this course) on constructing some metabelian groups using semidirect products of abelian groups. We will be especially interested in two types of abelian groups, the cyclic groups C_n and the group $C_p^m = C_p \times C_p \times \ldots \times C_p$, the direct product of m copies of C_p, p a prime. The group C_p^m is said to be "elementary abelian".

Recall that if $K \cong C_n$ is cyclic then the automorphism group of K is isomorphic to $U(n)$, the group of units of n. If n is an odd prime power then $U(n)$ is cyclic and a generator of $U(n)$ is said to be a **primitive root** of n.

On the other hand, if K is an elementary abelian p-group, that is, if K is isomorphic to a direct product of m copies of C_p, then we may view K as a vector space over the field Z_p of p elements and so the automorphism group of K contains $GL_m(p)$, the set of nonsingular $m \times m$ matrices over Z_p. It turns out that the automorphism group of the C_p^m is *equal* to $GL_m(p)$. For example, since $GL_2(2)$ has order six, we know that the automorphism group of $C_2 \times C_2$ must have order six.

We will use these facts about automorphisms of abelian groups in the examples below.

Examples.

1. **Classify all groups of order $2p$, p a prime.**

   Let p be an odd prime and G a group of order $2p$. By the Sylow theorems, G has a normal subgroup of order p which is obviously cyclic. G also has at least one subgroup of order 2. Let K be the cyclic subgroup of order p and Q the subgroup of order 2.

   The automorphism group of Z_p is $U(p)$; this group has order $p-1$. We need a map θ from $Q = \{1, q\}$ into $U(p)$. Since q has order 2, q must map to either the identity automorphism or to the unique automorphism of order two. The unique element of $U(p)$ of order two is $-1 \equiv p-1 \mod p$.

   Therefore, either

   (a) $\theta(q) = 1$ and so, $\forall k \in K,\ \theta(q)(k) = k$,
   or

   (b) $\theta(q) = -1$ and so, $\forall k \in K,\ \theta(q)(k) = k^{-1}$

   We only have two choices for θ and so we only have two groups of order $2p$. The first is the direct product $C_p \times C_2$ and the second is $C_p \rtimes_{(\theta : k \mapsto k^{-1})} C_2$. The first groupis cyclic; the second group is the dihedral group.

2. **Find all groups of order 20.**

   Let G be a group of order 20. By Sylow's theorem, G has a normal cyclic group of order 5, call it $K :=< x >$. G also has at least one Sylow 2-subgroup, call it Q. There are two cases, depending on the isomorphism class of Q.

   (a) Q is cyclic, say $Q = \{1, y, y^2, y^3\}$.

   The integer 2 is a primitive root of 5; $< 2 >= U(5)$. $Aut(K)$ is isomorphic to $U(5) =< 2 >= \{1, 2, 2^2 = 4, 2^3 = 3\}$ We may identify the elements of $Aut(K)$ with the set $\{x \mapsto x^1, x \mapsto x^2, x \mapsto x^4, x \mapsto x^3\}$. Since $Aut(K)$ is cyclic of order four, we may map y to any element of $Aut(K)$. In particular, we have four choices for θ. They are: $\theta(y)(x) = x^j,\ j = 1, 2, 4, 3$. This then gives four choices for G.

   Write $G =< x > \rtimes_j < y >$ as an abbreviation for $G =< x > \rtimes_\theta < y >$ where $\theta(y)(x) = x^j$.

   If $\theta(y)(x) = x^2$ then $\theta(y^{-1})(x) = (x^2)^{-1} = x^{-2} = x^3$. But in Q, the elements y and y^{-1} are indistinguishable; they both generate Q; there is an automorphism of Q which interchanges them. Thus $G =< x > \rtimes_2 < y >$ and $G =< x > \rtimes_3 < y >$ should be isomorphic groups. (They are.) So our four choices for θ only give three distinct (nonisomorphic) groups of the form $C_5 \rtimes C_4$. They are: $C_5 \rtimes_1 C_4 = C_5 \times C_4, C_5 \rtimes_2 C_4$, and $C_5 \rtimes_4 C_4 = C_5 \rtimes_{-1} C_4$.

   (b) Q is not cyclic. Then we may write $Q = \{1, y, z, yz\}$ where all the nonidentity elements have order two. Since no element of Q has order four then for any q in Q, $\theta(q)$ cannot have order four. Thus the automorphism $\theta(q)$ is either the identity automorphism or the automorphism which maps x to $x^4 = x^{-1}$.

   If $\theta(h) = 1$ then G is abelian; $G = (C_5) \rtimes_1 (C_2 \times C_2) = C_5 \times C_2 \times C_2$.

   If θ is not the trivial map then the kernel of θ is of size two, and we may suppose, without loss of generality, that the kernel of θ is $\{1, z\}$. This means $\theta(z)(x) = x, \theta(y)(x) = x^{-1}$, and $\theta(yz)(x) = x^{-1}$.

   This last group will be written $< x > \rtimes_{-1}(< y > \times < z >)$.

   So there are five groups of order twenty. They are, in the notation developed above:

   1. $C_5 \rtimes_{-1} C_4$,
   2. $C_5 \times C_4$,
   3. $C_5 \rtimes_2 C_4$,
   4. $C_5 \times_{-1} (C_2 \times C_2)$,
   5. $C_5 \times C_2 \times C_2$,

   (I have ordered these according to the SmallGroups catalogue in *GAP*.)

3. **Find all groups of order 28.**

   By the Sylow theorem, a group G of order 28 is an extension K by Q where $K =< x : x^7 = 1 >$ is cyclic of order 7 and Q is a group of order 4. Again, there are two cases, depending on the isomorphism class of Q.

   In this case (unlike the groups of order 20) the automorphism group of K has order six and so has no element of order four. Thus the only possible images of $\theta : Q \to Aut(K)$ are $\theta(Q) = \{1\}$ or $\theta(Q) = \{1, \sigma\}$ where $\sigma(x) = x^{-1}$.

   In an analysis similar to the work, above, we find four groups of order 28. They are:

   1. $C_7 \rtimes_{-1} C_4$,
   2. $C_7 \times C_4$,
   3. $C_7 \times_{-1} (C_2 \times C_2)$,

4. $C_7 \times C_2 \times C_2$,

(Again, I have ordered these according to the SmallGroups catalogue in *GAP*.)

4. **We classify all groups of order 12 with normal Sylow 3-subgroup.**

   (a) Let $K =< k >\cong C_3$ be the cyclic group of order three and $Q =< h >\cong C_4$ the cyclic group of order four. Which groups are of the form $K \rtimes Q$?

   Answer. $Aut(K)$ has order two so either $\theta(q)$ is trivial or $\theta(q)(k) = k^{-1}$. So there are two groups: $< k > \times < q >$ and $< k > \rtimes_{-1} < q >$.

   (b) Let $K =< k >\cong C_3$ be the cyclic group of order three and $Q = \{1, y, z, yz\}$ the noncyclic group of order four. Which groups are of the form $K \rtimes Q$?

   Answer. In addition to the direct product, there is the group $K \rtimes_\theta Q$ where $\theta(y)(k) = k^{-1}$, $\theta(z)(k) = k$ and $\theta(zy)(k) = k^{-1}$.

Summary: we have found four groups of order 12 with normal Sylow 3-subgroup. On the other hand, if a group of order 12 does not have a normal Sylow 3-subgroup then it is isomorphic to A_4; this is an exercise. So there are, up to isomorphism, five different groups of order 12.

5. **Which groups are extensions of the Klein 4-group by a cyclic group of order 3?** Let $K \cong C_2 \times C_2$ be the noncyclic group of order four and $H \cong C_3$ the cyclic group of order three. Which groups are of the form $K \rtimes H$?

   Obviously we have the direct product $(C_2 \times C_2) \times C_3$. This occurs when the map θ is the trivial one. Is there a nontrivial homomorphism θ from C_3 into $Aut(C_2 \times C_2)$? Yes, for $Aut(C_2 \times C_2)$ is isomorphic to the symmetric group S_3 of order six. (Permute the elements $\{y, z, yz\}$ of $C_2 \times C_2$ in any way you wish.) So we could have $\theta(h)$ be the permutation (y, z, yz). Thus G is generated by elements h, y, and z where h has order three, y and z each have order two, and conjugation by h maps y to z, z to yz and yz to y.

   Thus we have two groups of order 12 of the form $(C_2 \times C_2) \rtimes C_3$.

6. **Create a nonabelian extension of $C_p \times C_p$ by C_p.**

   Note that in the group $GL_2(p)$, the matrix $Z := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order p.

   Let $K =< x, y : x^p = y^p = [x, y] = 1 >$ be a presentation of the elementary abelian group $C_p \times C_p$ and let $Q =< z : z^p = 1 >$ represent the complement to K in G. We need to define the "action" of z on the elements of K. Viewing K as a two-dimensional vector space, we will agree to define the action of z on K as the action of Z on K. What does this mean? Z maps $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ to $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. So conjugation by z will map x to x and y to xy. (Note the transition from additive notation (eg. $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$) to multiplicative notation (x^1y^1).) Since Z is not the identity matrix, the action of z will not be trivial, so our group will not be abelian.

   A presentation for this group is $< x, y, z : x^p = y^p = z^p = [x, y] = [x, z] = 1; zyz^{-1} = xy >$ (or, in full use of commutators, $< x, y, z : x^p = y^p = z^p = [x, y] = [x, z] = [z, y]x^{-1} = 1 >$.)

7. Can we construct a nonabelian extension of K, the elementary abelian group of order 8 by Q, a cyclic group of order 7? Yes. To do so, we need an element of $GL(3, 2)$ of order 7.

Exercises.

1. Give an example of a finite noncyclic group which is not a semidirect product. (Hint: look at your lattice diagrams from an earlier assignment. This exercise demonstrates that not every metabelian group can be constructed from semidirect products.)

2. The groups of order twelve are $C_{12}, C_6 \times C_2, A_4, D_6$, and $T \cong Q_6 =< x, y : x^6 = y^4 = 1, x^3 = y^2, yxy^{-1} = x^{-1} >$. In these notes on semidirect products, we used semidirect products to construct six groups of order 12. (See examples 4 and 5, above. Two of the groups are of the form $(C_2 \times C_2) \rtimes C_3$, and four are of the form $C_3 \rtimes H$ where H is a group of order four.) Match these six groups in the notes with the five groups listed above. (As always, a *defense* of your claims is necessary.)

3. In the notes on semidirect products, we constructed all five groups of order 20. From earlier work, we already know the following groups of order 20: $C_{20}, C_{10} \times C_2, D_{10}$, and $Q_{10} :=< x, y : x^{10} = y^4 = 1, x^5 = y^2, yxy^{-1} = x^{-1} >$. Match these four groups with the five in the notes. (Which group in the notes is new?)