Group Theory **NOTES 4**
I. M. Isaacs Fall 2002

CYCLIC EXTENSIONS

Suppose that N is some "known" group. In this note, we discuss how to construct all possible groups G for which there exists a subgroup $N_1 \lhd G$, where $N_1 \cong N$ and G/N_1 is cyclic. (In the following, we identify N_1 with N and imagine that $N \lhd G$.)

First, we do the analysis, and then the synthesis. Suppose we have $N \lhd G$, where G/N is cyclic of order m. Then there is some coset gN that is a generating element for G/N and we know that $g^m N = (gN)^m = N$, and hence $g^m \in N$. (In fact, it is easy to see that m is the smallest positive integer such that $g^m \in N$. Write $a = g^m$, so a is some element of N.

Now conjugation by g in G induces an automorphism of N, and we let $\sigma \in \mathrm{Aut}(N)$ denote this automorphism, so that $x^g = x^\sigma$ for all $x \in N$.

We now have four items: the group N, the integer m the element $a \in N$ and the automorphism $\sigma \in \mathrm{Aut}(N)$. From these, our goal is to reconstruct the group G (up to isomorphism). But these four "ingredients" cannot be chosen arbitrarily; there are some compatibility conditions. For example, the element $a \in N$ is a power of g, and so g commutes with a and we have $a^\sigma = a^g = a$, and hence a must be a fixed point of σ. Also, since σ is the automorphism of N induced by g and $g^m = a$, we see that σ^m is the automorphism of N induced by a, and in particular, σ^m is an inner automorphism of N.

We now have four ingredients and two conditions, and it turns out that this is sufficient to reconstruct G. In fact, these determine G uniquely up to isomorphism. To summarize, the ingredients are

(a) A group N,

(b) A positive integer m,

(c) An element $a \in N$ and

(d) An automorphism $\sigma \in \mathrm{Aut}(N)$.

The conditions are

(1) $a^\sigma = a$ and

(2) σ^m is the inner automorphism of N induced by a.

Here is an example of how this can be used. Let N be a cyclic group of even order $2n$, let $m = 2$, let $a \in N$ be the unique element of order 2 and let σ be the map $x \mapsto x^{-1}$ on N. What results from this construction is a group G of order $4n$, where G has a cyclic subgroup N of order $2n$ and index 2. Also, there exists $g \in G - N$ of order 4 and $x^g = x^{-1}$ for $x \in N$. The group G is uniquely determined and is called the **generalized quaternion** group of order $4n$. We write $G = Q_{4n}$.

Let us compute some of the properties of this group. Since $G = N \cup Ng$, we see that if $u \in G$ is any element outside of the cyclic subgroup N, we can write $u = xg$, where $x \in N$. Now $u^2 = xgxg = xg^2(g^{-1}xg) = xg^2x^{-1} = g^2 = a$, where the penultimate equality follows since N is abelian. Since a has order 2, it follows that u has order 4, and this shows that all elements of $G - N$ have order 4, and thus a is the only involution in G. Note that the group Q_8 is the usual quaternion group.

Given our four ingredients satisfying two conditions, how do we prove that the group G exists? We can take the elements of G to be ordered pairs of the form (k, x), where $0 \leq k < m$ is an integer and $x \in N$. The multiplication rules are the following.

- $(i, x) \cdot (j, y) = (i + j, x^{\sigma^j} y)$ if $i + j < m$ and
- $(i, x) \cdot (j, y) = (i + j - m, a x^{\sigma^j} y)$ if $i + j \geq m$.

It is a routine (if somewhat tedious) calculation to check that this yields a group with the desired properties, where the element g is represented by the pair $(0, 1)$. (The first entry here is the number 0 and the second is the identity of N.) We omit this calculation since it is perhaps more instructive to see where the multiplication formulas listed above come from. If we go back to the group we want to get, we see that the full list of cosets of N in G is N, gN, g^2N, and so on, up to $g^{m-1}N$. Every element of G, therefore, is uniquely of the form $g^k x$, where $0 \leq k < m$ and $x \in N$, and this is the element we represent as the ordered pair (k, x). To see how these elements multiply, we compute

$$(g^i x)(g^j y) = g^i g^j (g^{-j} x g^j) y = g^{i+j} x^{\sigma^j} y \,,$$

since $x^g = x^\sigma$. If $i + j < m$, this agrees with the first of our multiplication formulas. If $i + j \geq m$, however, we see that $g^{i+j} = g^{i+j-m} a$, and this yields the second formula.

Starting with the trivial group, we ask which groups can, in theory at least, be constructed by repeated applications of this cyclic extension construction? It is easy to see that these are exactly the groups G for which there exist subgroups N_i such that

$$1 = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_r = G \,,$$

where each factor N_i / N_{i-1} is cyclic for $1 \leq i \leq r$. (Note that the subgroups N_i are all subnormal in G, but that they need not be normal.) These "constructible" groups are exactly the solvable groups, but recall that this is *not* the definition of solvable. That definition is that there exist *normal* subgroups K_i of G such that

$$1 = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = G \,,$$

where each factor K_i / K_{i-1} is abelian for $1 \leq i \leq r$. It is a good excercise to show that the "constructable" finite groups are exactly the solvable finite groups. We mention that a group is said to be **supersolvable** if there is a series of normal subgroups with cyclic factors. This property is strictly stronger than solvability and strictly weaker than nilpotence. (Exercise: Show that every nilpotent finite group is supersolvable.)