Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Notes 7 **Autumn 2011**

---

7 Semidirect product

7.1 Definition and properties

Let A be a normal subgroup of the group G. A *complement* for A in G is a subgroup H of G satisfying

- $HA = G$;
- $H \cap A = \{1\}$.

It follows that every element of G has a *unique* expression in the form ha for $h \in H$, $a \in A$. For, if $h_1 a_1 = h_2 a_2$, then

$$h_2^{-1} h_1 = a_2 a_1^{-1} \in H \cap A = \{1\},$$

so $h_2^{-1} h_1 = a_2 a_1^{-1} = 1$, whence $h_1 = h_2$ and $a_1 = a_2$.

We are going to give a general construction for a group with a given normal subgroup and a given complement. First some properties of complements.

Proposition 7.1 *Let H be a complement for the normal subgroup A of G. Then*

(a) $H \cong G/A$;

(b) if G is finite then $|A| \cdot |H| = |G|$.

Proof (a) We have

$$G/A = HA/A \cong H/H \cap A = H,$$

the first equality because $G = HA$, the isomorphism by the Third Isomorphism Theorem, and the second equality because $H \cap A = \{1\}$.

(b) Clear.

Example There are two groups of order 4, namely the cyclic group C_4 and the Klein group V_4. Each has a normal subgroup isomorphic to C_2; in the Klein group, this subgroup has a complement, but in the cyclic group it doesn't. (The complement would be isomorphic to C_2, but C_4 has only one subgroup isomorphic to C_2.)

If A is a normal subgroup of G, then G acts on A by conjugation; the map $a \mapsto g^{-1}ag$ is an automorphism of A. Suppose that A has a complement H. Then, restricting our attention to A, we have for each element of H an automorphism of A, in other words, a map $\phi : H \to \mathrm{Aut}(A)$. Now this map is an automorphism: for

- $(g\phi)(h\phi)$ maps a to $h^{-1}(g^{-1}ag)h$,
- $(gh)\phi$ maps a to $(gh)^{-1}a(gh)$,

and these two expressions are equal. We conclude that, if the normal subgroup A has a complement H, then there is a homomorphism $\phi : H \to \mathrm{Aut}(A)$.

Conversely, suppose that we are given a homomorphism $\phi : H \to \mathrm{Aut}(A)$. For each $h \in H$, we denote the image of $a \in A$ under $h\phi$ by a^h, to simplify the notation. Now we make the following construction:

- we take as set the Cartesian product $H \times A$ (the set of ordered pairs (h,a) for $h \in H$ and $a \in A$);
- we define an operation on this set by the rule

$$(h_1,a_1) * (h_2,a_2) = (h_1h_2, a_1^{h_2}a_2).$$

We will see the reason for this slightly odd definition shortly.

Closure obviously holds; the element $(1_H, 1_A)$ is the identity; and the inverse of (h,a) is $(h^{-1}, (a^{-1})^{h^{-1}})$. (One way round, we have

$$(h,a) * (h^{-1}, (a^{-1})^{h^{-1}}) = (hh^{-1}, a^{h^{-1}}(a^{-1})^{h^{-1}}) = (1_H, 1_N);$$

you should check the product the other way round for yourself.) What about the associative law? If $h_1,h_2,h_3 \in H$ and $a_1,a_2,a_3 \in N$, then

$$\begin{aligned}((h_1,a_1) * (h_2,a_2)) * (h_3,a_3) &= (h_1h_2, a_1^{h_2}a_2) * (h_3,a_3) = (h_1h_2h_3, (a_1^{h_2}a_2)^{h_3}a_3),\\ (h_1,a_1) * ((h_2,a_2) * (h_3,a_3)) &= (h_1,a_1) * (h_2h_3, a_2^{h_3}a_3) = (h_1h_2h_3, a_1^{h_2h_3}a_2^{h_3}a_3),\end{aligned}$$

and the two elements on the right are equal.

So we have constructed a group, called the *semi-direct product* of A by H using the homomorphism ϕ, and denoted by $A \rtimes_\phi H$. If the map ϕ is clear, we sometimes simply write $A \rtimes H$. Note that the notation suggests two things: first, that A is the normal subgroup; and second, that the semi-direct product is a generalisation of the direct product. We now verify this fact.

Proposition 7.2 *Let $\phi : H \to \mathrm{Aut}(A)$ map every element of H to the identity automorphism. Then $A \rtimes_\phi H \cong A \times H$.*

Proof The hypothesis means that $a^h = a$ for all $a \in A$, $h \in H$. So the rule for the group operation in $A \rtimes_\phi H$ simply reads

$$(h_1, a_1) * (h_2, a_2) = (h_1 h_2, a_1 a_2),$$

which is the group operation in the direct product.

Theorem 7.3 *Let G be a group with a normal subgroup A and a complement H. Then $G \cong A \rtimes_\phi H$, where ϕ is the homomorphism from H to $\mathrm{Aut}(A)$ given by conjugation.*

Proof As we saw, every element of G has a unique expression in the form ha, for $h \in H$ and $a \in A$; and

$$(h_1 a_1)(h_2 a_2) = h_1 h_2 (h_2^{-1} a_1 h_2) a_2 = (h_1 h_2)(a_1^{h_2} a_2),$$

where $a_1^{h_2}$ here means the image of a_1 under conjugation by h_2. So, if ϕ maps each element $h \in H$ to conjugation of A by h (an automorphism of A), we see that the map $ha \mapsto (h, a)$ is an isomorphism from G to $A \rtimes_\phi H$.

Example: Groups of order pq, where p and q are distinct primes. Let us suppose that $p > q$. Then there is only one Sylow p-subgroup P, which is therefore normal. Let Q be a Sylow q-subgroup. Then Q is clearly a complement for P; so G is a semi-direct product $P \rtimes_\phi Q$, for some homomorphism $\phi : Q \to \mathrm{Aut}(P)$.

Now $\mathrm{Aut}(C_p) \cong C_{p-1}$ (see below). If q does not divide $p-1$, then $|Q|$ and $|\mathrm{Aut}(P)|$ are coprime, so ϕ must be trivial, and the only possibility for G is $C_p \times C_q$. However, if q does divide $p-1$, then $\mathrm{Aut}(C_p)$ has a unique subgroup of order q, and ϕ can be an isomorphism from C_q to this subgroup. We can choose a generator for C_q to map to a specified element of order q in $\mathrm{Aut}(C_p)$. So there is, up to isomorphism, a unique semi-direct product which is not a direct product.

In other words, the number of groups of order pq (up to isomorphism) is 2 if q divides $p-1$, and 1 otherwise.

Why is $\mathrm{Aut}(C_p) \cong C_{p-1}$? Certainly there cannot be more than $p-1$ automorphisms; for there are only $p-1$ possible images of a generator, and once one is chosen, the automorphism is determined. We can represent C_p as the additive group of $\mathbb{Z}_p$, and then multiplication by any non-zero element of this ring is an automorphism of the additive group. So $\mathrm{Aut}(C_p)$ is isomorphic to the multiplicative group of $\mathbb{Z}_p$. The fact that this group is cyclic is a theorem of number theory (a generator for this cyclic group is called a *primitive root* mod p). We simply refer to Number Theory notes for this fact.

7.2 The holomorph of a group

Let A be any group. Take $H = \mathrm{Aut}(A)$, and let ϕ be the identity map from H to $\mathrm{Aut}(A)$ (mapping every element to itself). Then the semidirect product $A \rtimes_\phi \mathrm{Aut}(A)$ is called the *holomorph* of A.

Exercise Show that the holomorph of A acts on A in such a way that A acts by right multiplication and $\mathrm{Aut}(A)$ acts in the obious way (its elements are automorphisms of A, which are after all permutations!). Note that all automorphisms fix the identity element of A; in fact, $\mathrm{Aut}(A)$ is the stabiliser of the identity in this action of the holomorph.

Exercise Let G be a transitive permutation group with a regular normal subgroup A. Show that G is isomorphic to a subgroup of the holomorph of A.

Example Let A be the Klein group. Its autoorphism group is the symmetric group S_3. The holomorph $V_4 \rtimes S_3$ is the symmetric group S_4.

Example Let p be a prime and n a positive integer. Let A be the elementary abelian group of order p^n (the direct product of n copies of C_p). Show that $\mathrm{Aut}(A) = \mathrm{GL}(n,p)$. The holomorph of A is called the *affine group* of dimension n over $\mathbb{Z}_p$, denoted by $\mathrm{AGL}(n,p)$. **Exercise:** Write down its order.

Exercise A group G is called *complete* if it has the properties $Z(G) = \{1\}$ and $\mathrm{Out}(G) = \{1\}$. If G is complete, then

$$\mathrm{Aut}(G) = \mathrm{Inn}(G) \cong G/Z(G) = G,$$

in other words, a complete group is isomorphic to its automorphism group. Prove that, if G is complete, then the holomorph of G is isomorphic to $G \times G$.

Exercise Find a group G which is not complete but satisfies $\mathrm{Aut}(G) \cong G$.

7.3 Wreath product

Here is another very important example of a semidirect product. Let F and H be groups, and suppose that we are also given an action of H on the set $\{1,\ldots,n\}$. Then

there is an action of H on the group F^n (the direct product of n copies of F) by "permuting the coordinates": that is,

$$(f_1, f_2, \ldots, f_n)^h = (f_{1h}, f_{2h}, \ldots, f_{nh})$$

for $f_1, \ldots, f_n \in F$ and $h \in H$, where ih is the image of i under h in its given action on $\{1, \ldots, n\}$. In other words, we have a homomorphism ϕ from H to $\mathrm{Aut}(F^n)$. The semi-direct product $F^n \rtimes_\phi H$ is known as the *wreath product* of F by H, and is written $F \,\mathrm{wr}\, H$ (or sometimes as $F \wr H$).

Example Let $F = H = C_2$, where H acts on $\{1,2\}$ in the natural way. Then F^2 is isomorphic to the Klein group $\{1, a, b, ab\}$, where $a^2 = b^2 = 1$ and $ab = ba$. If $H = \{h\}$, then we have $a^h = b$ and $b^h = a$; the wreath product $F \,\mathrm{wr}\, H$ is a group of order 8. Prove that it is isomorphic to the dihedral group D_8 (see also below).

There are two important properties of the wreath product, which I will not prove here. The first shows that it has a "universal" property for imprimitive permutation groups.

Let G be a permutation group on Ω, (This means that G acts faithfully on Ω, so that G is a subgroup of the symmetric group on Ω, and assume that G acts imprimitively on Ω. Recall that this means there is an equivalence relation on Ω which is non-trivial (not equality or the universal relation) and is preserved by G. In this situation, we can produce two smaller groups which give information about G:

- H is the permutation group induced by G on the set of congruence classes, that is, the image of the action of G on the equivalence classes).
- Let Δ be a congruence class, and F the permutation group induced on Δ by its setwise stabiliser in G.

Theorem 7.4 *With the above notation, G is isomorphic to a subgroup of $F \,\mathrm{wr}\, H$.*

Example . The partition $\{\{1,2\},\{3,4\}\}$ of $\{1,2,3,4\}$ is preserved by a group of order 8, which is isomorphic to D_8. The two classes of the partition are permuted transitively by a group isomorphic to C_2; and the subgroup fixing $\{1,2\}$ setwise also acts on it as C_2. The theorem illustrates that $C_2 \,\mathrm{wr}\, C_2 \cong D_8$; we can write the elements down explicitly as permutations. With the earlier notation, $a = (1,2)$, $b = (3,4)$, and $H = (1,3)(2,4)$.

The other application concerns group extensions, a topic we return to in the next section of the notes. Let F and H be arbitrary groups. An *extension* of F by H refers to any group G which has a normal subgroup isomorphic to F such that the quotient is isomorphic to F.

Theorem 7.5 *Every extension of F by H is isomorphic to a subgroup of F wr H.*

Example There are two extensions of C_2 by C_2, namely C_4 and the Klein group V_4. We find them in the wreath product, using the earlier notation, as follows:

- $\langle ah \rangle = \langle (1,4,2,3) \rangle \cong C_4$ (note that $(ah)^2 = ahah = aa^h = ab$);
- $\langle ab, h \rangle = \langle (1,2)(3,4), (1,3)(2,4) \rangle \cong V_4$.