Queen Mary
University of London

**MTHM024/MTH714U** **Group Theory**

**Notes 8** **Autumn 2011**

---

# 8 Extension theory

In this section we tackle the harder problem of describing all *extensions* of a group $A$ by a group $H$; that is, all groups $G$ which have a normal subgroup (isomorphic to) $A$ with quotient $G/A$ isomorphic to $H$. As suggested, we will call the normal subgroup $A$.

We will assume in this chapter that $A$ is abelian. Later we will discuss briefly why we make this assumption.

We begin as in the preceding section of the notes. The group $G$ acts on $A$ by conjugation: that is, we have a homomorphism $\phi : G \to \mathrm{Aut}(A)$. Since $A$ is abelian, its action on itself by conjugation is trivial; that is, $A \leq \mathrm{Ker}(\phi)$. Now we have the following useful result, which can be regarded as a generalisation of the First Isomorphism Theorem:

**Proposition 8.1** *Let $\theta : G \to H$ be a group homomorphism, and suppose that $N$ is a normal subgroup of $G$ satisfying $N \leq \mathrm{Ker}(\theta)$. Then $\theta$ induces a homomorphism $\bar{\theta} : G/N \to H$.*

**Proof** Of course, we would like to define $(Ng)\bar{\theta} = g\theta$. We have to check that this is well-defined. So suppose that $Ng_1 = Ng_2$, so that $g_2(g_1)^{-1} \in N$. Then by assumption, $(g_2(g_1^{-1}))\theta = 1_H$, and so $g_1\theta = g_2\theta$, as required.

Now proving that $\bar{\theta}$ is a homomorphism is a routine check, which you should do for yourself.

In our case, $A \leq \mathrm{Ker}\,\phi$, so $\phi$ induces a homomorphism (which we will also call $\phi$, by abuse of notation) from $H \cong G/A$ to $\mathrm{Aut}(A)$.

Note that we are now in the same situation as the case where there is a complement: we have a homomorphism from $H$ to $\mathrm{Aut}(A)$. Now here are a few questions for you to think about:

- What goes wrong if $A$ is not abelian?
- Is it possible that the same extension gives rise to different homomorphisms (in the case where $A$ is abelian)? Is this possible in the case where $A$ has a complement in $G$?
- (much harder) Is there an extension of $A$ by $H$ in which we cannot define a homomorphism from $H$ to $\mathrm{Aut}(A)$ to describe the conjugation action? ($A$ has to be non-abelian and not complemented.)

Now we begin to describe the group $G$. First of all, since $G/A$ is isomorphic to $H$, we can label the cosets of $A$ in $G$ by elements of $H$ (their images under the homomorphism from $G/A$ to $H$). How do we describe the elements of $G$? For this, we need to choose a set of coset representatives. Let $r(h)$ be the representative of the coset corresponding to $H$. We can, and shall, assume that $r(1) = 1$ (use the identity as representative of the coset $A$). If there is a complement we could use its elements as coset representatives; but in general this is not possible. Note that we have

$$r(h)^{-1} a r(h) = a^h,$$

where $a^h$ is shorthand for the image of $A$ under the automorphism $h\phi$.

Now, for $h_1, h_2 \in H$, the element $r(h_1)r(h_2)$ lies in the coset labelled by $h_1h_2$, but it is not necessarily equal to $r(h_1h_2)$. So we define a "fudge factor" to give us the difference between these elements:

$$r(h_1)r(h_2) = r(h_1h_2)f(h_1,h_2)$$

where $f(h_1,h_2) \in A$. Thus $f$ is a function from $H \times H$ to $A$ (that is, it takes two arguments in $H$ and outputs an element of $A$).

Now we are ready to examine the group $G$. Each element of $G$ has a unique representation in the form $r(h)a$ where $h \in H$ and $a \in A$. Said otherwise, there is a bijection between $H \times A$ (as a set) and $G$. What happens when we multiply two elements?

$$\begin{aligned} r(h_1)a_1r(h_2)a_2 &= r(h_1)r(h_2)a_1^{h_2}a_2 \\ &= r(h_1h_2)f(h_1,h_2)a_1^{h_2}a_2. \end{aligned}$$

At this point we are going to change our notation and write the group operation in $A$ as addition. So the product of $r(h_1)a_1$ and $r(h_2)a_2$ has coset representative $r(h_1h_2)$ and differs from it by the element $a_1^{h_2} + a_2 + f(h_1,h_2)$ of $A$. We will simplify notation in another way too. Instead of writing an element of $G$ as $r(h)a$, we will write it as the corresponding element $(h,a)$ of $H \times A$.

Before going on, let us look at a special case. What does it mean if $f(h_1,h_2)=0$ for all $h_1,h_2\in H$? This means that the chosen coset representatives require no fudge factor at all: $r(h_1)r(h_2)=r(h_1,h_2)$. This just means that $r$ is a homomorphism from $H$ to $G$, and its image is a complement for $A$. This is the semi-direct product case. So the function $f$ should measure how far we are from a semi-direct product. So it does, but things are a little more complicated ...

Here is another special case. In primary school you learned how to add two-digit numbers. What is $37+26$? You add 7 and 6, giving 13; you write down 3 and carry 1. Then you add 3 and 2 together with the carried 1 to get 6, so the answer is 63. If you did all your calculations mod 10 and didn't worry about carrying, the answer would be 53. Said another way, the sum of the elements $(3,7)$ and $(2,6)$ in $\mathbb{Z}_{10}\times\mathbb{Z}_{10}$ is $(5,3)$. But there is another extension of $\mathbb{Z}_{10}$ by $\mathbb{Z}_{10}$, namely $\mathbb{Z}_{100}$, which has a normal subgroup $A$ (consisting of the multiples of 10) isomorphic to $\mathbb{Z}_{10}$ with quotient group $\mathbb{Z}_{10}$. If we use $(a,x)$ to denote the element $10a+x$ (belonging to the coset of $A$ containing $x$), then $(3,7)+(2,6)=(6,3)$. The carried 1 is exactly what we described as a fudge factor before. So in this case

$$f(x,y)=\begin{cases}0 & \text{if } x+y\le 9,\\ 1 & \text{if } x+y\ge 10.\end{cases}$$

So you should think of the function $f$ as a generalisation of the rules for carrying in ordinary arithmetic, to any group extension with abelian normal subgroup and arbitrary quotient.

The function $f$ is not arbitrary, but must satisfy a couple of conditions. The fact that $r(1)=0$ shows that $f(1,h)=f(h,1)=0$ for all $h\in H$. (Remember that we are writing $A$ additively, so the identity is now 0.) Also, let's do the calculation for the associative law. To simplify matters I will just work it out for elements of the form $(h,0)$.

$$\begin{aligned}((h_1,0)(h_2,0))(h_3,0) &= (h_1h_2,f(h_1,h_2))(h_3,0)=(h_1h_2h_3,f(h_1,h_2)^{h_3}+f(h_1h_2,h_3)),\\ (h_1,0)((h_2,0)(h_3,0)) &= (h_1,0)(h_2h_3,f(h_2,h_3))=(h_1h_2h_3,f(h_1,h_2h_3)+f(h_2,h_3))\end{aligned}$$

So the function $f$ must satisfy

$$f(h_1,h_2)^{h_3}+f(h_1h_2,h_3)=f(h_1,h_2h_3)+f(h_2,h_3)$$

for all $h_1,h_2,h_3\in H$.

Accordingly, we make a definition. Let $A$ be an abelian group (written additively), and $H$ a group. Let a homomorphism $\phi:H\to\mathrm{Aut}(A)$ be given; write the image of $a$ under $h\phi$ as $a^h$. A *factor set* is a function $f:H\times H\to A$ satisfying

- $f(1,h)=f(h,1)=0$ for all $h\in H$;

- $(h_1,h_2)^{h_3} + f(h_1h_2,h_3) = f(h_1,h_2h_3) + f(h_2,h_3))$ for all $h_1,h_2,h_3 \in H$.

**Theorem 8.2** *Given an abelian group $A$, a group $H$, a homomorphism $\phi : H \to \mathrm{Aut}(A)$, and a factor set $f$, define an operation on $H \times A$ by the rule*

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

*Then $(H \times A, *)$ is a group; it is an extension of $A$ by $H$, where the action of $H$ on $A$ is given by $\phi$, and the "fudge factor" for a suitable choice of coset representatives by $f$.*

However, this is not the end of the story. Before we continue, let us make two simple observations.

**Proposition 8.3** *Given $A$, $H$ and $\phi$, the set of all factor sets is an abelian group, with operation given by*

$$(f+f')(h_1,h_2) = f(h_1,h_2) + f'(h_1,h_2).$$

We will denote this group by $\mathrm{FS}(A,H,\phi)$.

**Proposition 8.4** *If the chosen coset representatives form a complement for $A$ in $G$, then the corresponding factor set is identically zero.*

The reason why there is more to do lies in the choice of coset representatives. Suppose that the function $s$ defines another choice of coset representatives. The values $r(h)$ and $s(h)$ are in the same coset of $A$, so they differ by an element of $A$; say $s(h) = r(h)d(h)$, where $d$ is a function from $H$ to $A$. Since $r(1) = s(1) = 0$, we have $d(1) = 0$.

Let $f_r$ and $f_s$ be the factor sets corresponding to the coset representatives $r$ and $s$. Then

$$\begin{aligned} r(h_1h_2)d(h_1h_2)f_s(h_1,h_2) &= s(h_1h_2)f_s(h_1,h_2) \\ &= s(h_1)s(h_2) \\ &= r(h_1)d(h_1)r(h_2)d(h_2) \\ &= r(h_1)r(h_2)d(h_1)^{h_2}d(h_2) \\ &= r(h_1h_2)f_r(h_1,h_2)d(h_1)^{h_2}d(h_2). \end{aligned}$$

Reverting to additive notation, we see that

$$f_s(h_1,h_2) - f_r(h_1,h_2) = d(h_1)^{h_2} + d(h_2) - d(h_1h_2).$$

Now let $d$ be any *function* from $H$ to $A$ satisfying $d(1) = 0$, and define a function $\delta d : H \times H \to A$ by

$$\delta d(h_1, h_2) = d(h_1)^{h_2} + d(h_2) - d(h_1 h_2).$$

Then some calculation shows that $\delta d$ is a factor set. The special factor sets of this form are called *inner factor sets*.

Now at last we can summarise our conclusions.

**Theorem 8.5** *Let the abelian group $A$, the group $H$, and the map $\phi : H \to \mathrm{Aut}(A)$ be given.*

*(a) The factor sets form an abelian group $\mathrm{FS}(H,A,\phi)$, and the inner factor sets form a subgroup $\mathrm{IFS}(H,A,\phi)$ of $\mathrm{FS}(H,A,\phi)$.*

*(b) Two factor sets arise from different choices of coset representatives in the same extension if and only if their difference is an inner factor set.*

We define the *extension group* $\mathrm{Ext}(H,A,\phi)$ to be the quotient $\mathrm{FS}(H,A,\phi)/IFS(H,A,\phi)$. Now the elements of $\mathrm{Ext}(H,A,\phi)$ "describe" extensions of $A$ by $H$ with action $\phi$. In particular,

- the zero element of $\mathrm{Ext}(H,A,\phi)$ describes the semidirect product $A \rtimes_\phi H$;
- if $\mathrm{Ext}(H,A,\phi) = \{0\}$, then the only extension of $A$ by $H$ with action $\phi$ is the semi-direct product $A \rtimes_\phi H$.

We say that an extension of $A$ by $H$ *splits* if it is a semi-direct product; the last conclusion can be expressed in the form "if $\mathrm{Ext}(H,A,\phi) = \{0\}$ then any extension of $A$ by $H$ with action $\phi$ splits".

There is one important case where this holds.

**Theorem 8.6 (Schur's Theorem)** *Suppose that $A$ is an abelian group and $H$ a group satisfying $\gcd(|A|,|H|) = 1$, Then any extension of $A$ by $H$ splits.*

**Proof** Let $m = |A|$ and $n = |H|$. Now if $f$ is any factor set, then $mf(h_1,h_2) = 0$ for any $h_1, h_2 \in H$; in other words, $mf = 0$ in $\mathrm{FS}(H,A,\phi)$, and so $m\overline{f} = 0$ in $\mathrm{Ext}(H,A,\phi)$, where $\overline{f}$ is the image of $f$ in FS / IFS.

We now show that $nf$ is an inner factor set. Define a function $d : H \to A$ by

$$d(h) = \sum_{h_1 \in H} f(h_1, h).$$

Consider the equation

$$f(h_1,h_2)^{h_3} + f(h_1h_2,h_3) = f(h_1,h_2h_3) + f(h_2,h_3)).$$

Sum this equation over $h_1 \in H$; we obtain

$$d(h_2)^{h_3} + d(h_3) = d(h_2h_3) + nf(h_2,h_3),$$

where we obtain $d(h_3)$ in the second term because $h_1h_2$ runs through $H$ as $h_1$ does. Thus,

$$nf(h_2,h_3) = d(h_2)^{h_3} + d(h_3) - d(h_2h_3),$$

which asserts that $nf$ is an inner derivation.

Now this says that $n\overline{f} = 0$ in $\mathrm{Ext}(H,A,\phi)$.

Our hypothesis says that $\gcd(m,n) = 1$. By Euclid's algorithm, there exist integers $a$ and $b$ such that $am + bn = 1$. Now, calculating in $\mathrm{Ext}(H,A,\phi)$,

$$\overline{f} = (am+bn)\overline{f} = a(m\overline{f}) + b(n\overline{f}) = 0.$$

Since $f$ was arbitrary, we have $\mathrm{Ext}(H,A,\phi) = \{0\}$.

In fact, a more general result is true. Zassenhaus improved Schur's theorem by showing that it is not necessary to assume that $A$ is abelian, as long as one of $A$ and $H$ is soluble. Now if the orders of $A$ and $H$ are coprime, then at least one of them is odd; and Feit and Thompson showed that any group of odd order is soluble. So we can say that if $\gcd(|A|,|H|) = 1$, then any extension of $A$ by $H$ splits, with no extra conditions on $A$ or $H$. This is known as the *Schur–Zassenhaus Theorem*.

Let us calculate $\mathrm{Ext}(C_2,C_2,\phi)$, where $\phi$ is the trivial homomorphism. Let $f$ be a factor set. Let $H = \{1,h\}$ and $A = \{0,a\}$. We have $f(1,1) = f(1,h) = f(h,1) = 0$, so there are two possible factor sets: we can have $f(h,h) = 1$ or $f(1,1) = a$.

What about inner factor sets? The function $d$ satisfies $d(1) = 0$; so we have

$$\delta d(h,h) = d(h) + d(h) - d(0) = 0,$$

So there is only one possible inner factor set.

Thus, $\mathrm{Ext}(C_2,C_2) = FS(C_2,C_2)/IFS(C_2,C_2) \cong C_2$, and there are just two extensions of $C_2$ by $C_2$. Of course we have known this all along; the only extensions are $C_4$ and $C_2 \times C_2$. Nevertheless, calculating factor sets and inner factor sets can easily be done by computer, so it is quite practical to decide what the possible extensions are.

There is one further problem, which we will not address (and causes a lot of difficulty in the theory). Non-isomorphic extensions correspond to different elements of the Ext group; but sadly, the converse is not true. Different elements of *Ext* may yield isomorphic groups. For example, $\mathrm{Ext}(C_p,C_p) = C_p$, but there are only two non-isomorphic extensions ($C_{p^2}$ and $C_p \times C_p$), not $p$ of them.