Derivations and Stabilizing Automorphisms

Bennett Rennier
bennett@brennier.com

May 9, 2019

1 Derivations

The material for this section can be found in Hilton-Stammbach [1].

Definition 1. Let G be a group and let A be a G-module. A *derivation* (also known as a *crossed homomorphism*) is a function $d : G \to A$ such that

$$d(xy) = xd(y) + d(x)$$

We let $\mathrm{Der}(G, A)$ denote the set of all derivations and note that it forms an abelian group under pointwise addition in the image. We also note that $d(1) = 0$ as

$$d(1) = d(1 \cdot 1) = 1d(1) + d(1) = 2d(1).$$

Definition 2. An important class of derivations to look at are those of the form $d_a(x) = xa - a$ for some $a \in A$ which we call *principal derivations* (also known as *inner derivations*). We see these are indeed derivations as

$$\begin{aligned} d_a(x) + xd_a(y) &= xa - a + x(ya - a) \\ &= xa - a + xya - xa \\ &= xya - a \\ &= d_a(xy). \end{aligned}$$

We let $\mathrm{PDer}(G, A)$ denote the set of all principal derivations and note that these form of a subgroup of $\mathrm{Der}(G, A)$ as $d_a - d_b = d_{a-b}$.

Example 3. Now derivations are connected to semidirect products. Recall that if G is a group and A is a G-module, then their semidirect product $A \rtimes G$ comes equipped with maps i and p such that $0 \to A \xrightarrow{i} A \rtimes G \xrightarrow{p} G \to 1$ is exact. We can consider $i(A)$ as a $A \rtimes G$-module under the action of conjugation. That is

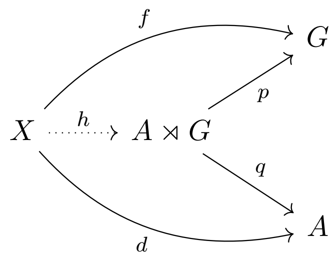
$$(b, x) \cdot (a, 1) \cdot (-x^{-1}b, x^{-1}) = (xa, 1),$$

which means we can consider A as a $A \rtimes G$-module under the action $(b, x).a = xa$. Note that we also have a projection map $q : A \rtimes G \to A$ where $q(a, x) = a$. This is projection is not a group homomorphism; however, it is a derivation as

$$\begin{aligned} q((a,x)\cdot(b,y)) &= q(a+xb, xy) \\ &= a + xb \\ &= q(a,x) + (a,x).b \\ &= q(a,x) + (a,x)\cdot q(b,y). \end{aligned}$$

In fact, we have following universal property of derivations in terms of semidirect products.

Proposition 4. Suppose that G is a group and A is a G-module. If we have a group homomorphism $f : X \to G$ and a derivation $d : X \to A$ (with A is regarded as an X-module using f), there is a unique group homomorphism $h : X \to A \rtimes G$ such that the following diagram commutes:



Conversely, every group homomorphism $h : X \to A \rtimes G$ induces a homomorphism $f : X \to G$ and a deriviation $d : X \to A$.

Proof. The proof is quite straightforward. We can simply define h to be $h(x) = (d(x), f(x))$ for all $x \in X$. We see that such an h is a group homomorphism as

$$\begin{aligned} h(x)h(y) &= (d(x), f(x))(d(y), f(y)) \\ &= (d(x) + d(y)f(x), f(x)f(y)) \\ &= (d(x) + xd(y), f(x)f(y)) \\ &= (d(xy), f(xy)) \\ &= h(xy). \end{aligned}$$

The converse is also quite easy; we can simply take $f = ph : X \to G$ and $d = qh : X \to A$. It is clear that f is a homomorphism as p and h are both homomorphisms. We see that d is a derivation as q is a derivation and so

$$\begin{aligned} d(xy) &= q(h(xy)) \\ &= q(h(x)h(y)) \\ &= h(x)\cdot q(h(y)) + q(h(x)) \\ &= h(x)\cdot d(y) + d(x) \\ &= p(h(x))d(y) + d(x) \\ &= f(x)d(y) + d(x) \\ &= xd(y) + d(x). \end{aligned}$$

□

Corollary 5. We note that in particular, if we take $X = G$ and $f = 1_G$, we have that the set of derivations from G to A is in one-to-one correspondence with group homomorphisms $f : G \to A \rtimes G$

where $pf = 1_G$, which are the lifts of the exact sequence $0 \to A \xrightarrow{i} A \rtimes G \xrightarrow{p} G \to 1$. This means that a lift $\ell : G \to A \rtimes G$ is a homomorphism if and only if $\ell(x) = (d(x), x)$ for some derivation d.

We can also use derivations to describe the first cohomology group $H^1(G, A)$. To show this connection, we first prove the following:

Theorem 6. The groups $\mathrm{Der}(G, A)$ and $\mathrm{Hom}_G(IG, A)$ are isomorphic under the map $\phi : \mathrm{Der}(G, A) \to \mathrm{Hom}_G(IG, A)$, where ϕ sends a derivation d to the homomorphism ϕ_d defined by $\phi_d(y - 1) = d(y)$.

Proof. Let $d : G \to A$ be a derivation; we want to show that $\phi_d = \phi(d)$ is a G-module homomorphism. We see this is the case as

$$\begin{aligned}\phi_d(x(y-1)) &= \phi_d((xy-1) - (x-1)) \\ &= d(xy) - d(x) \\ &= d(x) + xd(y) - d(x) \\ &= x \cdot \phi_d(y-1).\end{aligned}$$

To prove that this is an isomorphism, we construct an inverse. Let $\psi : \mathrm{Hom}_G(IG, A) \to \mathrm{Der}(G, A)$ be the map that sends a G-module homomorphism $f : IG \to A$ to the map $\psi_f : G \to A$ where $\psi_f(y) = f(y - 1)$. We see that ψ_f is a derivation as

$$\begin{aligned}\psi_f(xy) &= f(xy-1) \\ &= f(x(y-1) + (x-1)) \\ &= xf(y-1) + f(x-1) \\ &= x\psi_f(y) + \psi_f(x).\end{aligned}$$

Since we have that $\psi_{\phi_d}(y) = \phi_d(y-1) = d(y)$ and that $\phi_{\psi_f}(y-1) = \psi_f(y) = f(y-1)$, we see that these maps are indeed inverses. This proves that ϕ is an isomorphism. □

Corollary 7. There is an isomorphism

$$H^1(G, A) \simeq \frac{\mathrm{Der}(G, A)}{\mathrm{PDer}(G, A)}.$$

Proof. Recall that if we start with the short exact sequence $0 \to IG \xrightarrow{i} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0$, we can then apply Ext to the get the following long exact sequence:

$$\dots \longrightarrow \mathrm{Hom}_G(\mathbb{Z}G, A) \xrightarrow{i^*} \mathrm{Hom}_G(IG, A) \longrightarrow H^1(G, A) \longrightarrow \mathrm{Ext}^1(\mathbb{Z}G, A) \longrightarrow \dots$$

Since $\mathrm{Ext}^1(\mathbb{Z}G, A) = 0$ as $\mathbb{Z}G$ is projective, we have that $H^1(G, A) \simeq \mathrm{Hom}_G(IG, A)/\operatorname{im}(i^*)$. Furthermore, we have an isomorphism between $\mathrm{Hom}_G(\mathbb{Z}G, A)$ that sends the map $\phi : \mathbb{Z}G \to A$ to the element $\phi(1)$ where $\phi(x) = x\phi(1)$. Thus, the image of i^* are the maps of the form $\phi : IG \to A$ where $\phi(x) = xa$. We see then that $\phi(x - 1) = (x - 1)a = xa - a$, meaning the image of i^* are exactly the principal derivations from G to A. This proves that

$$H^1(G, A) \simeq \frac{\mathrm{Hom}_G(IG, A)}{\operatorname{im}(i^*)} \simeq \frac{\mathrm{Der}(G, A)}{\mathrm{PDer}(G, A)}.$$ □

Now, we can also use derivations to prove some useful things about the homology and cohomology of free groups.

Theorem 8. If F is the free group over a set S, then its augmentation ideal IF is a free F-module over the set $S-1=\{s-1 : x\in S\}$.

Proof. Recall that IF is generated by the set $F-1$. Since F is generated by S, this means that IF is generated by $S-1$. Thus, if we have a set function $f : S-1\to M$ for some F-module M, then there's only one possible extension to $f : IF\to M$. By proving that we can always make such an extension, we can conclude that IF is a free F-module over the set $S-1$.

So, let M be a F-module and let $f : S-1\to M$ be some set function. Since F is free over the set S, we can define a homomorphism $\tilde{f} : F\to M\rtimes F$, where $\tilde{f}(s)=(f(s-1),s)$. Since this is a homomorphism, Corollary 5 proves that $d : F\to M$ where $d(s)=f(s-1)$ is a derivation. By Theorem 6, we have that $f'=\phi(d)$ is a F-module homomorphism from IF to M where $f'(s-1)=d(s)=f(s-1)$. This f' is the desired extension of f, concluding the proof. □

Corollary 9. If F is a free group, then

$$H^n(F,A)=0=H_n(F,B)$$

for any F-modules A and B and for all $n\geq 2$.

Proof. We recall that

$$H^n(F,A)=H^n(\mathrm{Hom}_G(F_*,A)).$$

where F_* is a projective resolution of F. Since IF and $\mathbb{Z}F$ are both free F-modules, we have that

$$\cdots\to 0\to 0\to IF\to\mathbb{Z}F\to\mathbb{Z}$$

is a free resolution of $\mathbb{Z}$. As this is also a projective resolution and $F_n=0$ for $n\geq 2$, we see that $H^n(F,A)=0$. Similarly, $H_n(F,A)=0$ for $n\geq 2$. □

We can find another way of representing derivations and the second cohomology group, which is the topic of the next section.

2 Stabilizing Automorphisms

The material for this section can be found in Rotman [2]; though, most of the proofs have been modified and simplified to fit into the framework of the previous section.

A concept that we will see is very related to derivations are stablizing automorphisms. To begin, let G be a group and let A be a G-module so that $0\to A\to E\to G\to 1$ is an extension. This means that if we choose a lift $\ell : G\to E$, then every element of $e\in E$ can be written as $e=a+\ell(x)$ for some $a\in A$ and $x\in G$.

Definition 10. Now a *Stabilizing Automorphism* of an extension $0\xrightarrow{i} A\to E\xrightarrow{p} G\to 1$ is an automorphism $\phi : E\to E$ such that the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle 1_G} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

We let $\mathrm{Stab}(G, A)$ be the group of all stablizing automorphisms. Surprisingly, we already have a pretty good idea about this group.

Proposition 11. Let G be a group, A be a G-module, and $0 \to A \to E \to G \to 1$ be an extension. Now if $\ell : G \to E$ is some lifting, then $\phi : E \to E$ is a stabilizing automorphism if and only if it has the form

$$\phi(a + \ell(x)) = a + d(x) + \ell(x)$$

where $d : G \to A$ is a derivation. Morever, this derivation d is independent of our choice of lifting ℓ.

Proof. Let $\phi : E \to E$ be a stabilizing automorphism and $\ell : G \to E$ be a lifting. Then by the diagram in Definition 10, it must be that $\phi(a) = a$ and that $p\phi = p$. We can use this second condition to see that $\phi(\ell(x)) = d(x) + \ell(y)$ for some function $d : G \to A$. Since we have that

$$x = p(\ell(x)) = p\phi(\ell(x)) = p(d(x) + \ell(y)) = y,$$

so it must be that $x = y$ and that

$$\phi(a + \ell(x)) = \phi(a) + \phi(\ell(x)) = a + d(x) + \ell(x).$$

Now before we prove that d must be a derivation, we will first prove that it is independent of our choice of ℓ. To do this, let $\ell' : G \to E$ be another lifting such that $\phi(a + \ell'(x)) = a + d'(x) + \ell'(x)$ for some function d'. Since $p\ell'(x) = x = p\ell(x)$, there there is some $k : G \to A$ such that $\ell'(x) = k(x) + \ell(x)$. We see then

$$\begin{aligned} d'(x) &= \phi(\ell'(x)) - \ell'(x) \\ &= \phi(k(x) + \ell(x)) - \ell'(x) \\ &= k(x) + d(x) + \ell(x) - \ell'(x) \\ &= d(x) + \ell'(x) - \ell'(x) \\ &= d(x). \end{aligned}$$

This proves that the function d is independent of our choice of lifting. Now we need only to show that d is indeed a derivation. Recall that there is a factor set $f : G \times G \to A$ where $\ell(x) + \ell(y) = f(x, y) + \ell(xy)$ for all $x, y \in G$. We see that

$$\begin{aligned} \phi(\ell(x) + \ell(y)) &= \phi(\ell(x)) + \phi(\ell(y)) \\ &= d(x) + (\ell(x) + d(y) - \ell(x)) + \ell(x) + \ell(y) \\ &= d(x) + xd(y) + \ell(x) + \ell(y) \\ &= d(x) + xd(y) + f(x, y) + \ell(xy). \end{aligned}$$

However, computed another way, we also see that

$$\begin{aligned} \phi(\ell(x) + \ell(y)) &= \phi(f(x, y) + \ell(xy)) \\ &= \phi(f(x, y)) + \phi(\ell(xy)) \\ &= f(x, y) + \phi(\ell(xy)) \\ &= f(x, y) + d(xy) + \ell(xy). \end{aligned}$$

Comparing these two, we obtain

$$d(x) + xd(y) + f(x, y) + \ell(xy) = f(x, y) + d(xy) + \ell(xy)$$

If we then cancel the $\ell(xy)$ on both sides, we rest of the terms all lie in the abelian group A, so we can rearrange as we like and cancel the $f(x,y)$ term to obtain that

$$d(xy) = d(x) + xd(y)$$

which proves that d is a derivation.

Now conversely, let ϕ be a map of the form $\phi(a + \ell(x)) = a + d(x) + \ell(x)$ where $d : G \to A$ is a derivation. We see that $\phi(a, 0) = a$ and that $p(\phi(a+\ell(x))) = p(a+d(x)+\ell(x)) = \ell(x) = p(a+\ell(x))$. Thus, the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \downarrow 1_A & & \downarrow \phi & & \downarrow 1_G & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \end{array}$$

If we let $f : G \times G \to A$ be the factor set such that $\ell(x) + \ell(y) = f(x,y) + \ell(xy)$, we can see that ϕ is a homomorphism as

$$\begin{aligned} \phi(a + \ell(x) + b + \ell(y)) &= \phi(a + b + f(x,y) + \ell(xy)) \\ &= (a + b + f(x,y)) + d(xy) + \ell(xy) \\ &= a + b + (d(x) + xd(y)) + f(x,y) + \ell(xy) \\ &= a + b + d(x) + (\ell(x) + d(y) - \ell(x)) + \ell(x) + \ell(y) \\ &= (a + d(x) + \ell(x)) + (b + d(y) + \ell(y)) \\ &= \phi(a + \ell(x)) + \phi(b + \ell(y)) \end{aligned}$$

This means we can apply the Five Lemma to deduce that ϕ is an isomorphism, and thus ϕ is a stablizing automorphism. □

We also see that not only are derivations and stabilizing automorphisms in a 1-1 correspondence, they are also isomorphic as groups, which we will now prove.

Theorem 12. The group of stabilizing automorphisms $\mathrm{Stab}(G, A)$ is isomorphic to the group of derivations $\mathrm{Der}(G, A)$.

Proof. According to the previous proposition, if $\phi : E \to E$ is a stabilizing automorphism, then $\phi(a+\ell(x)) = a+d(x)+\ell(x)$ where d is a derivation and ℓ is any lifting. So, we let $\sigma : \mathrm{Stab}(G, A) \to \mathrm{Der}(G, A)$ be the map that sends a stabilizing automorphism to the derivation associated with it in this way. We see that if $\sigma(\phi) = d_1$ and $\sigma(\psi) = d_2$, then

$$\begin{aligned} (\psi \circ \phi)(a + \ell(x)) &= \psi(\phi(a + \ell(x))) \\ &= \psi(a + d_1(x) + \ell(x)) \\ &= \psi((a + d_1(x)) + \ell(x)) \\ &= (a + d_1(x)) + d_2(x) + \ell(x) \\ &= a + (d_1(x) + d_2(x)) + \ell(x). \end{aligned}$$

This shows that $\sigma(\psi \circ \phi) = d_1 + d_2$, proving that σ is a homomorphism. Since the previous proposition stated that this is a 1-1 correspondence, we have that σ is an isomorphism as desired. □

Remark. Surprisingly, this proves that even though the operation of the group $\text{Stab}(G, A)$ is function composition, it's actually an abelian group as $\text{Der}(G, A)$ is abelian. Moreover, this also implies that $\text{Stab}(G, A)$ does not depend on the extension E at all.

To continue the analogy with derivations, we'll show that principal derivations correspond with a nice subgroup of stablizing automorphism.

Definition 13. An *inner stablizing automorphism* $\phi : G \to E$ is a stabilizing automorphism such that for some $b \in A$, $\phi(a + \ell(x)) = -b + a + \ell(x) + b$. We denote the subgroup of inner stabilizing automorphisms as $\text{InnStab}(G, A)$.

Remark. As a correction to a subtle mistake in Rotman, it should be noted that the group of inner stabilizing automorphisms is not the same as the group $\text{Stab}(G, A) \cap \text{Inn}(E)$. Only stabilizing automorphisms that act by conjugation with an element of A are considered inner stabilizing automorphisms. In fact, we will provide an example to show that it is possible that $\text{InnStab}(G, A)$ is a proper subgroup of $\text{Stab}(G, A) \cap \text{Inn}(E)$. Consider the extension

$$0 \to Z(Q_8) \xrightarrow{\iota} Q_8 \xrightarrow{\pi} G \to 1$$

where Q_8 is the quaternion group of order 8, $Z(Q_8)$ is the center of Q_8 (i.e. $Z(Q_8) = \{-1, 1\}$), and $G = Q_8/Z(Q_8)$. Let $\phi : Q_8 \to Q_8$ be defined as conjugation by i, that is $\phi(x) = ix(-i)$. Since ϕ is the is the identity on $Z(Q_8)$ and $\phi(x) = ix(-i) \in \{x, -x\}$, we see that the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Z(Q_8) & \xrightarrow{\iota} & Q_8 & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow 1_{Z(Q_8)} & & \downarrow \phi & & \downarrow 1_G & & \\ 0 & \longrightarrow & Z(Q_8) & \xrightarrow{\iota} & Q_8 & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

This proves that $\phi \in \text{Stab}(G, Z(Q_8)) \cap \text{Inn}(Q_8)$. However, conjugation by an element of $Z(Q_8)$ is trivial since it is the center of Q_8. This means that $\text{InnStab}(G, Z(Q_8)) = \{1_{Q_8}\}$. Since ϕ is not the identity map, we have that $\text{InnStab}(G, Z(Q_8)) \subsetneq \text{Stab}(G, Z(Q_8)) \cap \text{Inn}(Q_8)$.

Proposition 14. Let $0 \to A \to E \to G \to 1$ be an extension and let $\ell : G \to E$ be a lifting. Then $\phi : E \to E$ is an inner stablizing automorphism if and only if it has the form

$$\phi(a + \ell(x)) = a + d_b(x) + \ell(x)$$

where d_b is a principal derivation.

Proof. If $\phi : E \to E$ has the form $\phi(a + \ell(x)) = a + d_b(x) + \ell(x)$ for some principal derivation d_b, then ϕ we know from Proposition 11 that ϕ is a stabilizing automorphism. We also see that

$$\begin{aligned} \phi(a + \ell(x)) &= a + d_b(x) + \ell(x) \\ &= a + (xb - b) + \ell(x) \\ &= -b + a + xb + \ell(x) \\ &= -b + a + (\ell(x) + b - \ell(x)) + \ell(x) \\ &= -b + a + \ell(x) + b \end{aligned}$$

which proves that ϕ acts by conjugation, meaning that it is an inner stabilizing automorphism.

Conversely, suppose that ϕ is an inner stabilizing automorphism. Since ϕ is a stabilizing automorphism, we know it has the form $\phi(a + \ell(x)) = a + d(x) + \ell(x)$ for some derivation d.

Additionally, since ϕ is an inner automorphism, we know that for some $b \in A$ we have that $\phi(a+\ell(x)) = -b + (a+\ell(x)) + b$. We see that

$$\begin{aligned}\phi(a+\ell(x)) &= -b + a + \ell(x) + b \\ &= -b + a + \ell(x) + b - \ell(x) + \ell(x) \\ &= -b + a + xb + \ell(x) \\ &= a + (xb - b) + \ell(x) \\ &= a + d_b(x) + \ell(x),\end{aligned}$$

which completes the proof. □

Corollary 15. Since Theorem 12 and Proposition 14 state that $\mathrm{Stab}(G,A) \simeq \mathrm{Der}(G,A)$ and $\mathrm{InnStab}(G,A) \simeq \mathrm{PDer}(G,A)$ respectively, we can use Corollary 7 to reinterpret the first cohomology group as

$$H^1(G,A) \simeq \frac{\mathrm{Stab}(G,A)}{\mathrm{InnStab}(G,A)}.$$

Theorem 16. Let $0 \to A \to E \to G \to 1$ be a split extension and let C and C' both be complements of A in E. Then if $H^1(G,A) = \{0\}$, then C and C' are conjugate subgroups.

Proof. As $E = A \rtimes G$, we have liftings $\ell : G \to E$ and $\ell' : G \to E$ which have images C and C' respectively. By the Corollary 5, we have that $\ell(x) = (d(x), x)$ and $\ell'(x) = (d'(x), x)$ where $d, d' : G \to A$ are derivations. This means that $h(x) = \ell(x) - \ell'(x) = (d(x) - d'(x), 0)$ is a derivation. Since $H^1(G,A) = \{0\}$, it must be that $\mathrm{Der}(G,A) = \mathrm{PDer}(G,A)$. Thus, $h(x)$ is a principal derivation, that is, $h(x) = xa - a$ for some $a \in A$. This shows that

$$\begin{aligned}\ell(x) &= h(x) + \ell'(x) \\ &= (xa - a) + \ell'(x) \\ &= -a + \ell'(x) + a - \ell'(x) + \ell'(x) \\ &= -a + \ell'(x) + a.\end{aligned}$$

This proves that $\mathrm{im}(\ell) = C$ and $\mathrm{im}(\ell') = C'$ are conjugate subgroups. □

References

[1] Hilton Peter, Stammbach Urs. “A course in homological algebra.” Springer Science & Business Media – 2012. - Vol. 4 – P. 194-197.

[2] Rotman Joseph. “An introduction to homological algebra.” Springer Science & Business Media – 2008. - Vol. 1 – P. 514-518.