The Geometry of Module Extensions*

Karl W. Gruenberg
School of Mathematical Sciences
Queen Mary College, University of London

1.

When we teach linear algebra to undergraduates, probably the first major result we prove is the following: if V is a vector space over a field and W is a subspace of V, then every basis of W can be extended to a basis of V. As a consequence, for W in V, there exists U in V so that $W \oplus U = V$.

These results really have nothing to do with the commutativity of the field. They remain true (with essentially the same proof) for vector spaces over a "non-commutative field" or division ring.

If we focus on the direct sum consequence above, then this holds over even more general coefficient rings. Explicitly, let R be a ring and consider the following property of modules over R:

$(*)$ Given an R-module V and a submodule W, then there exists a submodule U of V so that $W \oplus U = V$.

Every full matrix algebra over a division ring has this property $(*)$; and so (therefore) does every finite product of such rings. The surprise is that the converse is true: if R has the property $(*)$, then R must have the above structure. Such a ring is called semi-simple. This basic result was found in essence by Wedderburn in the first decade of the century, and in the general form by Artin in the twenties.

There is a useful restatement of $(*)$. Given an exact sequence of R-modules,

$$0 \longrightarrow W \longrightarrow V \xrightarrow{\pi} W' \longrightarrow 0,$$

we say the sequence splits if there is a homomorphism $\tau : W' \longrightarrow V$ so that $\tau\pi$ is the identity on W'. Then $V = W \oplus W'\tau$. Property $(*)$ is equivalent to the statement that every exact sequence of R-modules splits.

To understand the modules over a ring we need to know the simple modules, which form the building blocks of all modules, and to understand how the simple modules may be glued together. For semi-simple rings, the

---

* Lecture given to the Singapore Mathematical Society on 3 April 1987.

gluing process is irrelevant since then every module is a direct sum of simple modules. But for non semi-simple rings, there are usually many ways of gluing together two modules. The study of this is called extension theory.

The most important ring in mathematics is not semi-simple. I mean, of course, the ring of natural integers, Z. Let p be a prime and write $M = Z/pZ$. So M is a simple Z-module. A sequence

$$0 \longrightarrow M \longrightarrow V \longrightarrow M \longrightarrow 0$$

may or may not split: if $V = Z/p^2 Z$, then it is non-split. Suppose we enlarge the kernel:

$$0 \longrightarrow M \oplus M \longrightarrow E \longrightarrow M \longrightarrow 0.$$

A little experimentation shows that we must have $E \simeq V \oplus M$, with V as before. The same conclusion holds however large we make the kernel: if we use $M^{(k)}$ instead of $M^{(2)}$, then $E \simeq V \oplus M^{(k-1)}$.

What happens if we enlarge the image? Given

$$0 \longrightarrow M^{(k)} \longrightarrow E \longrightarrow M^{(2)} \longrightarrow 0,$$

we find $E \simeq W \oplus M^{(k-2)}$, where W arises in an extension

$$0 \longrightarrow M^{(2)} \longrightarrow W \longrightarrow M^{(2)} \longrightarrow 0.$$

There are various possibilities for W. (1) It could, of course, simply be $M^{(4)}$ (which happens if the sequence splits); (2) it could have the form $W \simeq U \oplus M$, where U arises in the non-split sequence

$$0 \longrightarrow M \longrightarrow U \longrightarrow M^{(2)} \longrightarrow 0;$$

or (3) W may have no direct summand M.

In this last case W is unique. To make this precise, we use the following general definition. Two extensions (exact sequences) of modules over an arbitrary ring

$$\begin{array}{c} 0 \longrightarrow A \longrightarrow E_1 \longrightarrow B \longrightarrow 0 \\ 0 \longrightarrow A \longrightarrow E_2 \longrightarrow B \longrightarrow 0 \end{array} \qquad (1)$$

are *isomorphic* if there exists an isomorphism $\varphi : E_1 \longrightarrow E_2$ so that φ induces the identity on B.

The module W in this case (3) above is uniquely determined to within an isomorphism. In case (2), there are various possibilities for U. We may view $M^{(2)}$ as a two dimensional vector space over the prime field Z/pZ and this has $p+1$ different one dimensional subspaces. Each such subspace yields some U and two different one-dimensional subspaces yield non-isomorphic extensions.

If we replace $M^{(2)}$ by $M^{(3)}, M^{(4)}, \ldots$, things get progressively more complicated. But there is a pattern behind it all as we shall see.

2.

We now make a fresh start. Let R be a given ring, B a fixed R-module and M a simple R-module. We are after the global structure of the totality of all extensions of the form

$$0 \longrightarrow M^{(k)} \longrightarrow E \longrightarrow B \longrightarrow 0$$

for $k \geq 0$.

To state the results we need some preparation. For an extension over B, meaning an exact sequence

$$0 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} B \longrightarrow 0, \tag{2}$$

we adopt the abbreviated notation $(A|E)$ and write its isomorphism class as $[A|E]$.

(I) The push-out and pull-back. These two easy constructions are quite general and were learnt by algebraists from the topologists.

Given (2) and a homomorphism $\alpha : A \longrightarrow C$, we construct the following picture:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & B & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow & & \| & & \\ 0 & \longrightarrow & C & \longrightarrow & H & \longrightarrow & B & \longrightarrow & 0 \end{array},$$

by setting $H = (C \oplus E)/N$, where N is the submodule generated by all $(a\alpha, -a\iota)$, $a \in A$. The lower sequence is called the *pushout* to $(A|E)$ via α and we shall denote it by $(A|E)\alpha$.

If we are given a homomorphism $\beta : C \longrightarrow B$, we produce the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & B & \longrightarrow & 0 \\ & & \Vert & & \uparrow & & \uparrow \beta & & , \\ 0 & \longrightarrow & A & \longrightarrow & L & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

where $L = \{(e,c) \in E \oplus C \mid e\pi = c\beta\}$. This is the *pull-back.*

(II) Products. Given extensions $(A_1|E_1)$, $(A_2|E_2)$, we construct the pull-back to

$$0 \longrightarrow A_1 \oplus A_2 \longrightarrow E_1 \oplus E_2 \longrightarrow B \oplus B \longrightarrow 0$$

via $\beta : B \longrightarrow B \oplus B$, $b\beta = (b,b)$. This is the product of the extensions and written $(A_1|E_1) \prod (A_2|E_2)$.

(III) $Ext(B,A)$. Two extensions, as in (1) above, are called *equivalent* if they are isomorphic and the isomorphism $\varphi : E_1 \longrightarrow E_2$ induces the identity on A. This is an equivalence relation on the totality of extensions over B with kernel A; we denote the set of all equivalence classes by $Ext(B,A)$ and the class containing $(A|E)$ by $\overline{(A|E)}$.

Given $(A|E_1)$, $(A|E_2)$, let $\alpha : A \oplus A \longrightarrow A$ be $(x,y) \longmapsto x + y$; define a binary operation $+$ on $Ext(B,A)$ by

$$\overline{(A|E_1)} + \overline{(A|E_2)} = \overline{((A|E_1) \prod (A|E_2))\alpha} \quad .$$

This makes $Ext(B,A)$ into an additive group. If $\varphi \in End_R A$, the R-endomorphism ring of A, then we define

$$\overline{(A|E)}\varphi = \overline{(A|E)\varphi}.$$

Now $Ext(B,A)$ is a module over $End_R A$.

We apply this with $M = A$. Since M is simple, $End_R M = D$ is a division ring. We are now exclusively interested in extensions of the form $(M^{(k)}|E)$. So without loss of clarity we may denote such an extension by $(k|E)$. If $(k|E)$ has no direct summand isomorphic to M, we call $(k|E)$ an *essential cover* (of B). This is equivalent to having $M^{(k)}$ contained in the

Frattini module of E: if W is a submodule of E so that $W + M^{(k)} = E$, then $W = E$.

Theorem *Every extension $(k|E)$ can be decomposed uniquely (to within an isomorphism) in the form*

$$(l|F) \prod S,$$

where $(l|F)$ is an essential cover and S is a split extension: $S = M^{(k-l)} \oplus B$.

This theorem allows us henceforth to focus our attention on essential covers. Now at last, the geometry promised in the title of this lecture enters the discussion.

Given $(k|E)$, define

$$(k|E)_M = \{ \overline{(k|E)\varphi} \mid \varphi \in Hom_R(M^{(k)}, M) \}.$$

Thus $(\ )_M$ is a mapping of extensions to subsets of $Ext(B,M)$. This mapping has some very nice properties:

(a) $(k|E)_M$ is a D-submodule of $Ext(B,M)$;

(b) $\left((k|E) \prod (l|F)\right)_M = (k|E)_M + (l|F)_M$;

(c) if $(k|E)$ is essential, then k is the dimension over D of $(k|E)_M$;

(d) $(k|E)_M \supset (l|F)_M$ if, and only if, there exists $(k|E) \longrightarrow (l|F)$.

(By $(k|E) \longrightarrow (l|F)$ we mean a diagram of the form

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M^{(k)} & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & M^{(l)} & \longrightarrow & F & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

.)

Clearly, $(\ )_M$ induces a mapping $[\ ]_M$ on the isomorphism classes of extensions.

Theorem $[\ ]_M$ *is a bijection of the set of all isomorphism classes of essential covers onto the set $\mathcal{P}$ of all finitely generated D-submodules of $Ext(B,M)$.*

Thus $\mathcal{P}$ is precisely the projective geometry on the D-space $Ext(B,M)$. The geometric containment relation corresponds to the existence of morphisms between the extensions (in the sense of (d) above). The theorem makes it plain that we have a unique maximal essential cover — the one corresponding to the ambient space $Ext(B,M)$ — provided this is finitely generated over D.

For example, if $R = Z$, $B = \mathcal{F}_p^{(n)}$, $M = \mathcal{F}_p$, then $D = \mathcal{F}_p$ and $dim_D Ext(B,M) = n$. The case we examined at the start was $n = 2$, the projective line.

3.

The above theory also applies to group extensions. To see how this comes about it is best to use a general method of passing from group extensions to module extensions, and back. Here is a brief description.

A surjective group homomorphism $\pi : E \longrightarrow G$ gives rise, by linearization, to a ring homomorphism $\pi : ZE \longrightarrow ZG$. In particular, if $G = 1$, then π is the usual augmentation map on ZE and the kernel is $(E-1)$, the ideal in ZE generated by all elements $e-1$, $e \in E$. In general, if A is the kernel of $E \longrightarrow G$, then the kernel of $ZE \longrightarrow ZG$ is the ideal in ZE generated by the augmentation ideal $(A-1)$ of A:

$$0 \longrightarrow (A-1)E \longrightarrow ZE \xrightarrow{\pi} ZG \longrightarrow 0.$$

Of course, $(E-1)\pi = (G-1)$, the augmentation ideal of G. We now obtain an exact sequence of ZG-modules by factoring out the action of A:

$$0 \longrightarrow (A-1)E/(E-1)(A-1) \longrightarrow (E-1)/(E-1)(A-1) \longrightarrow (G-1) \longrightarrow 0. \quad (3)$$

Here

$$A/A' \simeq (A-1)E/(E-1)(A-1)$$

via $aA' \longmapsto (a-1)+(E-1)(A-1)$ and the isomorphism is one of G-modules. Henceforth, assume A is abelian $(A' = 1)$.

Now suppose we are given an exact sequence of ZG-modules,

$$0 \longrightarrow A \longrightarrow V \xrightarrow{\varphi} (G-1) \longrightarrow 0.$$

We wish to construct a group extension over G with kernel A. Let GV be the split extension of V (normal) by G and let $\psi : GV \longrightarrow G(G-1)$ be the group homomorphism

$$(g, v) \longmapsto (g, v\varphi).$$

If $\theta : G \longrightarrow G(G-1)$ is $g \longmapsto (g, g-1)$, then θ is an embedding of G and $G\theta\psi^{-1} = E$ is a group giving the required extension

$$1 \longrightarrow A \longrightarrow E \xrightarrow{\psi\theta^{-1}} G \longrightarrow 1. \qquad (4)$$

These two constructions are, in a natural way, inverse to each other. They provide a dictionary for translating module theory to group theory, and vice versa.

If M is a simple G-module, then an essential cover of $(G-1)$ with kernel $M^{(k)}$ corresponds to a group extension E over G whose kernel $M^{(k)}$ is contained in the Frattini group of E (a Frattini extension). Moreover, we have a bijection between the isomorphism classes of Frattini extensions

$$1 \longrightarrow M^{(k)} \longrightarrow E \longrightarrow G \longrightarrow 1$$

and isomorphism classes of essential covers

$$0 \longrightarrow M^{(k)} \longrightarrow V \longrightarrow (G-1) \longrightarrow 0.$$

So these isomorphism classes of group extensions form a projective geometry on $Ext((G-1), M)$ over $D = End_G M$.

As a very simple example, let G be the direct product of two cyclic groups of order 2 and M the trivial G-module $Z/2Z$. Then $D = \mathcal{F}_2$ and $Ext((G-1), M)$ has dimension 3 over $\mathcal{F}_2$. We therefore have a projective plane with 7 points and 7 lines. If two points are commutative (correspond to commutative extension groups), then the line joining them is also commutative (it corresponds to the extension-theoretic product, by property (b) of the mapping $(\ )_M$). Hence there are exactly 3 commutative points. One sees quite easily that there are 3 dihedral points, whence the remaining point must be quaternion.

If G is a finite, but otherwise unrestricted group and M is any simple G-module, then $Ext((G-1), M)$ is certainly finitely generated over D and hence our theory ensures the existence of a unique maximal Frattini extension. This fact was first proved by Gaschütz in the early fifties (by a completely different method); when M is a trivial module the result essentially goes back to work of Schur in the early part of the century.

Relevant Litreature.

(1) M. Auslander, Functors and morphisms determined by objects, in *Representation Theory of Algebras* (ed. Robert Gordon), Lecture Notes 37 (1978), Dekker, pp 1–244.

(2) K.W. Gruenberg and K.W. Roggenkamp, Extension categories of groups and modules, I: Essential covers, *J. Algebra* 49 (1977), pp 564–594.

(3) K.W. Gruenberg and K.W. Roggenkamp, The geometry of homogeneous extension categories, *Proc. Arcata Conf. on Representation Theory*, Amer. Math. Soc., to appear.