COHOMOLOGY AND CENTRAL SIMPLE ALGEBRAS

William Crawley-Boevey

These are the notes for an MSc course given in Leeds in Spring 1996. My idea was to give an introduction to lots of different kinds of cohomology theories, and their applications to central simple algebras.

Contents

Some References

Cartan & Eilenberg, Homological algebra.
Weibel, Introduction to homological algebra.
Maclane, Homology.
Hilton and Stammbach, A course in homological algebra.
Spanier, Algebraic topology.

§1. Chain complexes

1.1. SETTING. Let R be a ring. We'll consider left R-modules.
Recall that if $R=\mathbb{Z}$ then we're dealing with additive groups.
If R=field, we're dealing with vector spaces.

Maps $M \longrightarrow N$ will be R-module homomorphisms.
Write $\mathrm{Hom}(M,N)$ or $\mathrm{Hom}_R(M,N)$.
Recall that this is an additive group.
It is an R-module if R is commutative.

1.2. DEFINITION. A <u>chain</u> <u>complex</u> $C_\bullet$ consists of R-modules C_i ($i\in\mathbb{Z}$) and maps

$$\cdots \longrightarrow C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} C_{-1} \xrightarrow{\partial_{-1}} C_{-2} \longrightarrow \cdots$$

satisfying $\partial_{n-1}\partial_n = 0$ for all n.
The elements of C_n are called <u>chains</u> of <u>degree</u> n or n-<u>chains</u>.
Convention is that the map ∂_n STARTS at the module C_n.
The maps ∂_n are the <u>differential</u>.

Sloppy notation: the chain complex is C.
Each of the maps is denoted ∂.
Thus the condition is that $\partial^2 = 0$.

If C is a chain complex, then it's <u>homology</u> is defined by

$$H_n(C) = \frac{\mathrm{Ker}(\partial_n : C_n \longrightarrow C_{n-1})}{\mathrm{Im}(\partial_{n+1} : C_{n+1} \longrightarrow C_n)} = \frac{Z_n(C)}{B_n(C)}$$

It is an R-module.
Since $\partial^2=0$ it follows that $B_n(C) \subseteq Z_n(C)$.
The elements of $B_n(C)$ are n-<u>boundaries</u>.
The elements of $Z_n(C)$ are n-<u>cycles</u>.
If x is an n-cycle we write [x] for its image in $H_n(C)$.

A chain complex C is

- <u>acyclic</u> if $H_n(C) = 0$ for all n.
- <u>non-negative</u> if $C_n = 0$ for n<0.
- <u>bounded</u> if only finitely many nonzero C_n.

1.3. EXAMPLES. (1) If M is an R-module and $n\in\mathbb{Z}$ you get a chain complex

$$C : \cdots \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots$$

with M in degree n. Then

$$H_i(C) = \begin{cases} M & (i=n) \\ 0 & (i\neq n) \end{cases}$$

I'll sometimes call this complex M(in deg n).

(2) Have chain complex of $\mathbb{Z}$-modules

$$C : \ldots \longrightarrow 0 \longrightarrow \underset{\deg 1}{\mathbb{Z}} \xrightarrow{a} \underset{0}{\mathbb{Z}} \longrightarrow 0 \longrightarrow \ldots$$

then $H_0(C) = \mathbb{Z}/a\mathbb{Z}$, $H_1(C) = 0$.

More generally if $M \xrightarrow{f} N$ is a homomorphism of R-modules you get a complex

$$C : \ldots \longrightarrow 0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0 \longrightarrow \ldots$$

say with M in degree 1, N in degree 0. Then

$$H_0(C) = N/\mathrm{Im}(f) = \mathrm{Coker}\,(f)$$
$$H_1(C) = \mathrm{Ker}(f).$$

(3) Recall that an <u>exact</u> <u>sequence</u> is a sequence of modules and maps

$$L \longrightarrow M \longrightarrow \ldots \longrightarrow X \longrightarrow Y$$

in which the image of each map is the same as the kernel of next map. You get a chain complex

$$C : \ldots \longrightarrow 0 \longrightarrow L \longrightarrow M \longrightarrow \ldots \longrightarrow X \longrightarrow Y \longrightarrow 0 \longrightarrow \ldots$$

once you decide which degree to put any of the terms in.
Then $H_i(C) = 0$ except possibly at L and Y.
A <u>short</u> <u>exact</u> <u>sequence</u> is an exact sequence

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0.$$

It gives an acyclic complex.

1.4. DEFINITION. A <u>cochain</u> <u>complex</u> $C^{\bullet}$ consists of R-modules C^i ($i \in \mathbb{Z}$) and maps

$$\cdots \longrightarrow C^{-2} \xrightarrow{\partial^{-2}} C^{-1} \xrightarrow{\partial^{-1}} C^{0} \xrightarrow{\partial^{0}} C^{1} \xrightarrow{\partial^{1}} C^{2} \longrightarrow \cdots$$

satisfying $\partial^{n+1}\partial^{n}=0$. The elements of C^n are called <u>cochains</u> of <u>degree</u> n or n-<u>cochains</u>.

Its <u>cohomology</u> is defined by

$$H^n(C) = \frac{\mathrm{Ker}(\partial:C^n\longrightarrow C^{n+1})}{\mathrm{Im}(\partial:C^{n-1}\longrightarrow C^n)} = \frac{Z^n(C)}{B^n(C)}$$

The elements of $B^n(C)$ are n-<u>coboundaries</u>.
The elements of $Z^n(C)$ are n-<u>cocycles</u>.

REMARK. There is no difference between chain and cochain complexes, apart from numbering. If you’ve got a chain complex C you get a cochain complex by defining $C^n = C_{-n}$. We say that one is obtained from the other by <u>renumbering</u>.

Most complexes are zero on the left or the right, so do as a non-negative chain or cochain complex.

1.5. DEFINITION. Let C be a chain complex of left R-modules. If N is a left R-module then there is a cochain complex Hom(C,N) with

$\mathrm{Hom}(C,N)^n = \mathrm{Hom}(C_n,N)$
$\partial:\mathrm{Hom}(C,N)^n\longrightarrow \mathrm{Hom}(C,N)^{n+1}$ induced by the map $\partial:C_{n+1}\longrightarrow C_n$.

It is a complex of $\mathbb{Z}$-modules (or of R-modules if R is commutative).

The cohomology of this complex is denoted $H^n(C,N)$. It is the "cohomology of C with coefficients in N".

1.6. EXAMPLE. Even if a chain complex C is acyclic, it’s cohomology might not be zero. Let C be the acyclic complex of $\mathbb{Z}$-modules:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{2} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & 0 \\ & \text{deg} & 1 & & 0 & & -1 & & \end{array}$$

Have $\mathrm{Hom}(\mathbb{Z}/2,\mathbb{Z}) = 0$ and $\mathrm{Hom}(\mathbb{Z},\mathbb{Z}) \cong \mathbb{Z}$ so $\mathrm{Hom}(C,\mathbb{Z})$ is cochain complex

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{2} & \mathbb{Z} & \longrightarrow & 0 \\ \text{deg} & & -1 & & 0 & & 1 & & \end{array}$$

so $H^1(C,\mathbb{Z}) \cong \mathbb{Z}/2$ and the rest vanish.

1.7. EXAMPLE. Simplicial homology.

If $v_0,...,v_n$ are n+1 points in $\mathbb{R}^N$ which don't lie in an n-plane then the n-<u>simplex</u> with vertices $v_0,...,v_n$ is

$$[v_0,...,v_n] = \{\text{convex span of the } v_i\} = \{\textstyle\sum_{i=0}^n \lambda_i v_i \mid \lambda_i \geq 0,\ \sum \lambda_i = 1\}$$

A simplex s is a closed subset of $\mathbb{R}^N$. Its vertices are uniquely determined as the extremal points of s.

$$\{v_i\} = \{x \in s \mid \text{cannot write } x = 1/2(u+v) \text{ with } u,v \in s,\ u \neq v\}$$

0-simplex is a point

1-simplex is a line segment

2-simplex is a triangle

3-simplex is a tetrahedron

A <u>face</u> of a simplex is a simplex given by a subset of its vertices.

A <u>simplicial complex</u> in $\mathbb{R}^N$ is a finite collection K of simplices satisfying

(1) If $s \in K$ then so is every face of K.

(2) If $s,t \in K$ then their intersection is empty or is a face of s and t.

An <u>oriented simplicial complex</u> is a simplicial complex together with an ordering on its vertices. Can do this by labelling its vertices 1,2,3,...

If K is an oriented simplicial complex, its chain complex C = C(K) is defined as follows.

$$C_n = \begin{cases} \text{free } \mathbb{Z}\text{-module on the n-simplices in K} & (n\geq 0) \\ 0 & (n<0) \end{cases}$$

The map $\partial: C_n \longrightarrow C_{n-1}$ is defined by giving $\partial(s)$ for s an n-simplex.

If $s = [v_0,...,v_n]$ with $v_0<...<v_n$ in the chosen order.
Then $\partial(s) = \sum_{i=0}^{n} (-1)^i [v_0,...,\hat{v}_i,...,v_n]$.

Note that the signs depend on the ordering.

This is a chain complex, that is $\partial^2=0$. For example

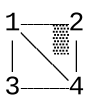
$$\partial^2[v_1,v_2,v_3,v_4] = \partial[v_2,v_3,v_4] - \partial[v_1,v_3,v_4] + \partial[v_1,v_2,v_4] - \partial[v_1,v_2,v_3]$$

$$\begin{aligned} = &\ \ \ ([v_3,v_4] - [v_2,v_4] + [v_2,v_3]) \\ &- ([v_3,v_4] - [v_1,v_4] + [v_1,v_3]) \\ &+ ([v_2,v_4] - [v_1,v_4] + [v_1,v_2]) \\ &- ([v_2,v_3] - [v_1,v_3] + [v_1,v_2]) \end{aligned}$$

$$= 0.$$

The simplicial homology of K is $H_n(C(K))$.
The simplicial cohomology of K with coefficients in N is $H^n(C(K),N)$.

REMARK. The naming of cycles and boundaries can be explained as follows.
Let K be a simplicial complex. For simplicity in $\mathbb{R}^2$.
A path along the edges gives an element of C_1.
The path is a cycle if it returns to its starting point.
The path is a boundary if you can fill in its interior with 2-simplices.

EXAMPLE. K is 

Then C_0 free on [1],[2],[3],[4]
C_1 free on [12],[13],[14],[24],[34]
C_2 free on [124]

$\partial([124]) = [24] - [14] + [12]$

$\partial([12]) = [2] - [1]$
$\partial([13]) = [3] - [1]$
$\partial([14]) = [4] - [1]$
$\partial([24]) = [4] - [2]$
$\partial([34]) = [4] - [3]$

$Z_0(C)$ is all of C_0.
$B_0(C)$ is linear combinations of these differences
$= \{\alpha[1]+\beta[2]+\gamma[3]+\delta[4] \mid \alpha+\beta+\gamma+\delta=0\}$
Thus $H_0(C) \cong \mathbb{Z}$.

$Z_1(C)$ = is set of $\alpha[12] + \beta[13] + \gamma[14] + \delta[24] + \varepsilon[34]$ with $\alpha,\ldots,\varepsilon\in\mathbb{Z}$ such that $(-\alpha-\beta-\gamma)[1] + (\alpha-\delta)[2] + (\beta-\varepsilon)[3] + (\gamma+\delta+\varepsilon)[4] = 0$.
$B_1(C)$ is set of $\zeta([24] - [14] + [12])$ with $\zeta,\eta\in\mathbb{Z}$.
Find that $Z_1(C) \cong B_1(C) \oplus \mathbb{Z}([34] - [14] + [13])$. Thus $H_1(C) \cong \mathbb{Z}$.

$Z_2(C) = 0$ so $H_2(C) = 0$.

1.8. EXAMPLE. de Rham cohomology.
Let U be an open subset of $\mathbb{R}^2$. Have chain complex

$$\begin{array}{ccccccccccc} \longrightarrow & 0 & \longrightarrow & \Omega^0 & \xrightarrow{d} & \Omega^1 & \xrightarrow{d} & \Omega^2 & \longrightarrow & 0 & \longrightarrow \ldots \\ & \text{deg} & & 0 & & 1 & & 2 & & & \end{array}$$

Ω^0 = set of smooth functions on U, that is functions $U \longrightarrow \mathbb{R}$ such that all partial derivatives of all orders exist and are continuous.
Ω^1 = set of differential 1-forms on U, symbols $\omega = p\,dx + q\,dy$ where p,q are smooth functions on U.
Ω^2 = set of differential 2-forms on U, symbols $h\,dx\,dy$ with h a smooth function on U.

If $f \in \Omega^0$ so f is a function on U then $df = \frac{\partial f}{\partial x}\,dx + \frac{\partial f}{\partial y}\,dy$.
If $\omega = p\,dx + q\,dy$ is a differential 1-form then $d\omega = (\frac{\partial q}{\partial x} - \frac{\partial p}{\partial y})\,dx\,dy$

This is a cochain complex since $\frac{\partial^2 f}{\partial x \partial y} = \frac{\partial^2 f}{\partial y \partial x}$.

Its differential d really is to do with differentiation.
de Rham cohomology of U is $H^n_{DR}(U) = H^n(\Omega^\bullet)$.

$Z^1(U) = \{\omega \in \Omega^1 \mid d\omega = 0\}$ is set of closed 1-forms.
$B^1(U) = \{df \mid f$ smooth function$\}$ is set of exact 1-forms.
$H^1_{DR}(U) = \{$closed 1-forms$\} / \{$exact ones$\}$

$H^1_{DR}(\mathbb{R}^2) = 0$ by Poincaré lemma.

$H^1_{DR}(\mathbb{R}^2\backslash 0) \neq 0$: can show $\omega = \dfrac{-y}{x^2+y^2}\,dx + \dfrac{x}{x^2+y^2}\,dy$ closed, but not exact.

Note that ω doesn't make sense as a 1-form on $\mathbb{R}^2$.

As a 1-form on $\mathbb{R}^2\backslash\{$y-axis$\}$ it does make sense and is exact.
Consider function f on $\mathbb{R}^2\backslash\{$y-axis$\}$, $f(x,y) = \tan^{-1}(y/x)$
(between $-\pi/2$ and $\pi/2$).
Then $df = \omega$.

de Rham cohomology generalizes to smooth manifolds. See
Fulton, Algebraic topology
Bott & Tu, Differential forms in algebraic topology

1.9. EXAMPLE. Singular homology.
Let X be a topological space. Let C_n be the free $\mathbb{Z}$-module with basis the set of continuous maps from an n-simplex to X.

The image of the map might look like a deformed simplex, but it might be singular, hence the name.

Can make the C_n into a chain complex.
Get singular homology and cohomology.

(1) Suppose K is a simplicial complex and |K| is union of its simplices. Then simplicial homology of K and singular homology of |K| coincide.

(2) Suppose U is open in $\mathbb{R}^2$, then singular cohomology with coefficients in $\mathbb{R}$ and de Rham cohomology coincide (de Rham's theorem).

Now a little theory about chain and cochain complexes.

1.10. DEFINITION. If C and D are chain complexes, then a <u>homomorphism</u> (or a <u>chain</u> <u>map</u>) $f:C \longrightarrow D$ is given by a homomorphism $f_n : C_n \longrightarrow D_n$ for each n, such that each square in the diagram is commutative

$$\begin{tikzcd}
\cdots \arrow[r, "\partial"] & C_{n+1} \arrow[r, "\partial"] \arrow[d, "f_{n+1}"'] & C_n \arrow[r, "\partial"] \arrow[d, "f_n"'] & C_{n-1} \arrow[r, "\partial"] \arrow[d, "f_{n-1}"'] & \cdots \\
\cdots \arrow[r, "\partial"] & C_{n+1} \arrow[r, "\partial"] & C_n \arrow[r, "\partial"] & C_{n-1} \arrow[r, "\partial"] & \cdots
\end{tikzcd}$$

If C and D are chain complexes then Hom(C,D) is an additive group.

The set of chain complexes together with their homomorphisms is a category. (If you are worried about what a category is, look it up).

There is also the notion of a cochain map of cochain complexes.
Note that if $C \longrightarrow D$ is a chain map and N is an R-module you get a cochain map $Hom(D,N) \longrightarrow Hom(C,N)$.

1.11. PROPOSITION. If $f:C \longrightarrow D$ is a chain map then for each n it induces a homomorphism on homology $H_n(f) : H_n(C) \longrightarrow H_n(D)$. (Thus H_n is a functor from category of chain complexes to category of modules.)

PROOF. An arbitrary element of $H_n(C)$ is of the form [x] with $x \in Z_n(C)$. Send it to $[f_n(x)]$ in $H_n(D)$.

1.12. THEOREM. Let $0 \longrightarrow C \xrightarrow{f} D \xrightarrow{g} E \longrightarrow 0$ be a short exact sequence of chain complexes, meaning that f and g are chain maps and for each n the maps

$$0 \longrightarrow C_n \xrightarrow{f_n} D_n \xrightarrow{g_n} E_n \longrightarrow 0$$

are a short exact sequence. Then there are connecting maps $c:H_n(E) \longrightarrow H_{n-1}(C)$ giving a long exact sequence

$$\ldots \longrightarrow H_{n+1}(E) \xrightarrow{c} H_n(C) \longrightarrow H_n(D) \longrightarrow H_n(E) \xrightarrow{c} H_{n-1}(C) \longrightarrow H_{n-1}(D) \longrightarrow \ldots$$

PROOF. Have diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C_{n+1} & \longrightarrow & D_{n+1} & \longrightarrow & E_{n+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_n & \longrightarrow & D_n & \xrightarrow{g} & E_n & \longrightarrow & 0 \\
 & & \downarrow & & \partial\downarrow & & \downarrow & & \\
0 & \longrightarrow & C_{n-1} & \xrightarrow{f} & D_{n-1} & \longrightarrow & E_{n-1} & \longrightarrow & 0
\end{array}$$

Define connecting map $H_n(E) \longrightarrow H_{n-1}(C)$ as follows.

Typical element of $H_n(E)$ is $[x]$ with $x \in Z_n(E)$.

Choose $y \in D_n$ with $g(y)=x$.

Then $g(\partial(y)) = \partial(g(y)) = \partial(x) = 0$.

Thus there is unique $z \in C_{n-1}$ with $f(z)=\partial(y)$.

Define $c([x]) = [z]$.

This doesn't depend on the choice of x or y.

Say $y, y' \in D_n$ have images $x, x' \in Z_n(E)$ with $[x]=[x']$.

Thus $g(y')-g(y) \in B_n(E)$.

Thus $g(y-y') = \partial g(u)$ for some $u \in D_{n+1}$

$= g\partial(u)$

Thus $y-y'-\partial(u) = f(v)$ for some $v \in C_n$.

Now if $f(z)=\partial(y)$ and $f(z')=\partial(y')$ then

$f(z-z') = \partial(y-y') = \partial(y-y'-\partial(u)) = \partial f(v) = f\partial(v)$.

Thus $z-z' = \partial v$.

Thus $[z] = [z']$ in $H_{n-1}(C)$.

Now $H_n(C) \longrightarrow H_n(D) \longrightarrow H_n(E) \xrightarrow{c} H_{n-1}(C) \longrightarrow H_{n-1}(D)$

Exact at $H_n(D)$:

Say $x \in Z_n(D)$ and $g(x) \in B_n(E)$.

Then there is $y \in D_{n+1}$ with $g(x) = \partial g(y) = g\partial y$.

Thus $x - \partial y = f(z)$ for some $z \in C_n$.

Now $f\partial z = \partial f(z) = \partial x - \partial^2 y = 0$.

Thus $z \in Z_n(C)$.

Then $[x] = [f(z)]$.

etc.

1.13. COROLLARY (Snake lemma). If you have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \theta\downarrow & & \phi\downarrow & & \psi\downarrow & & \\ 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \end{array}$$

you get an exact sequence

$$0 \longrightarrow \text{Ker } \theta \longrightarrow \text{Ker } \phi \longrightarrow \text{Ker } \psi \longrightarrow \text{Coker } \theta \longrightarrow \text{Coker } \phi \longrightarrow \text{Coker } \psi \longrightarrow 0$$

Consider $L \longrightarrow X$, $M \longrightarrow Y$ and $N \longrightarrow Z$ as chain complexes.

1.14. REFORMULATION. A short exact sequence of cochain complexes $0 \longrightarrow C \longrightarrow D \longrightarrow E \longrightarrow 0$ gives a long exact sequence

$$\ldots \longrightarrow H^{n-1}(E) \longrightarrow H^n(C) \longrightarrow H^n(D) \longrightarrow H^n(E) \longrightarrow H^{n+1}(C) \longrightarrow H^{n+1}(D) \longrightarrow \ldots$$

1.15. COROLLARY. If C is a chain complex of PROJECTIVE R-modules and $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence of R-modules then you get a long exact sequence in cohomology.

$$\ldots \longrightarrow H^{n-1}(C,N) \longrightarrow H^n(C,L) \longrightarrow H^n(C,M) \longrightarrow H^n(C,N) \longrightarrow H^{n+1}(C,N) \longrightarrow$$

PROOF. Since C_n is projective you get an exact sequence

$$0 \longrightarrow \text{Hom}(C_n,L) \longrightarrow \text{Hom}(C_n,M) \longrightarrow \text{Hom}(C_n,N) \longrightarrow 0.$$

(Recall this is one of the defining properties of projective modules. More later).

1.16. DEFINITION. If $f, f' : C \longrightarrow D$ are chain maps, then f and f′ are <u>homotopic</u> if for each n there are maps $h_n : C_n \longrightarrow D_{n+1}$ such that

$$f_n - f'_n = h_{n-1}\, \partial_n + \partial_{n+1}\, h_n.$$

Here all maps go $C_n \longrightarrow D_n$. The composites are

$$C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{h_{n-1}} D_n \quad \text{and} \quad C_n \xrightarrow{h_n} D_{n+1} \xrightarrow{\partial_{n+1}} D_n$$

The analogous notion for cochain maps $f,f':C\longrightarrow D$ is $h^n:C^n\longrightarrow D^{n-1}$ such that

$$f^n - f'^n = h^{n+1}\,\partial^n + \partial^{n-1}\,h^n.$$

1.17. PROPOSITION. If $f,f':C\longrightarrow D$ are homotopic then for each n they induce exactly the same map $H_n(C)\longrightarrow H_n(D)$.

PROOF. Say $[x]\in H_n(C)$, so $x\in Z_n(C)$. Then

$$\begin{aligned} H_n(f)([x]) - H_n(f')([x]) &= [f_n(x)] - [f'_n(x)] \\ &= [h_{n-1}\partial(x) + \partial h_n(x)] \\ &= [\partial h_n(x)] && \text{as } x \text{ is a cycle.} \\ &= 0 && \text{as } \partial h_n(x) \text{ is a boundary.} \end{aligned}$$

1.18. PROPOSITION. If $f,f':C\longrightarrow D$ are homotopic and N is an R-module, then the induced cochain maps $\mathrm{Hom}(D,N)\longrightarrow\mathrm{Hom}(C,N)$ are homotopic.

PROOF. A homotopy is given by maps $h_n:C_n\longrightarrow D_{n+1}$ such that

$$f_n - f'_n = h_{n-1}\,\partial_n + \partial_{n+1}\,h_n.$$

Let $h^n : \mathrm{Hom}(D,N)^n \longrightarrow \mathrm{Hom}(C,N)^{n-1}$ be $\mathrm{Hom}(h_{n-1},N)$.

$$\begin{array}{ccc} \mathrm{Hom}(D,N)^n & \longrightarrow & \mathrm{Hom}(C,N)^{n-1} \\ \cong & & \cong \\ \mathrm{Hom}(D_n,N) & & \mathrm{Hom}(C_{n-1},N) \end{array}$$

1.19. DEFINITION. A chain map $f:C\longrightarrow D$ is a <u>quasi-isomorphism</u> if for each n the map $H_n(C)\longrightarrow H_n(D)$ is an isomorphism.

A chain map $f:C\longrightarrow D$ is a <u>homotopy equivalence</u> if there is a chain map $g:D\longrightarrow C$ such that gf is homotopic to Id_D and fg is homotopic to Id_C.

If there is a homotopy equivalence we say that C and D are <u>homotopy equivalent</u>.

A chain complex C is <u>contractible</u> if it is homotopy equivalent to the zero complex.

Equivalent condition: Id_C is homotopic to 0_C.

Equivalent condition: there are maps $h_n : C_n \longrightarrow C_{n+1}$ with

$$Id_{C_n} = h_{n-1}\, \partial_n + \partial_{n+1}\, h_n$$

for all n. This is called a contracting homotopy.

WARNING. Don't confuse:
- Two morphisms $f, f' : C \longrightarrow D$ can be homotopic.
- Two complexes C,D can be homotopy equivalent.

1.20. PROPOSITION. If $f : C \longrightarrow D$ is a homotopy equivalence then it is a quasi-isomorphism.

PROOF. Clear.

1.21. PROPOSITION. A homotopy equivalence $f : C \longrightarrow D$ of chain complexes induces a homotopy equivalence of cochain complexes $Hom(D,N) \longrightarrow Hom(C,N)$. In particular $H^n(D,N) \cong H^n(C,N)$.

PROOF. Clear.

1.22. REMARK. The homotopy category K(R) has objects the chain complexes of R-modules, and

$Hom_{K(R)}(C,D)$ = homotopy equivalence classes of homomorphisms $C \longrightarrow D$.

(Often people use cochain complexes).

This defines a category since if $f, f' : C \longrightarrow D$ are homotopic and $g, g' : D \longrightarrow E$ are homotopic then so are gf and g'f'.

In this category the isomorphisms are the homotopy equivalences.

1.23. DEFINITION. Recall that a short exact sequence

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0.$$

is <u>split</u> if the following equivalent conditions hold

(1) f has a retraction, a map $r:M \longrightarrow L$ with $rf = Id_L$

(2) g has a section, a map $s:N \longrightarrow M$ with $gs = Id_N$

(3) Im(f) is a direct summand of M.

Considered as a chain complex, it is split if and only if it is contractible. More generally:

1.24. THEOREM. A chain complex C is contractible if and only if it is acyclic and all of the short exact sequences

$$0 \longrightarrow Z_n(C) \xrightarrow{i_n} C_n \xrightarrow{\partial_n} B_{n-1}(C) \longrightarrow 0$$

are split. (Here i_n is the inclusion).

PROOF. If C is contractible then it is quasi-isomorphic to the zero complex, so acyclic. Let h be the contracting homotopy. Let $s:B_{n-1}(C) \longrightarrow C_n$ be the restriction of $h_{n-1}:C_{n-1} \longrightarrow C_n$. If $x \in B_{n-1}(C)$ then

$$x = Id_{C_{n-1}}(x) = (h_{n-2}\,\partial_{n-1} + \partial_n\, h_{n-1})(x)$$

$$= \partial_n\, h_{n-1}(x)$$

$$= \partial_n\, s\,(x)$$

Thus s is a section for the short exact sequence.

Now suppose that C is acyclic and all the short exact sequences are split. Then for all n there are sections

$$s_{n-1} : B_{n-1}(C) \longrightarrow C_n.$$

If $x \in C_n$ then $x - s_{n-1}\partial_n x$ is in $Z_n(C) = B_n(C)$ so we can define a function $h_n:C_n \longrightarrow C_{n+1}$ by

$$h_n(x) = s_n\,(x - s_{n-1}\partial_n x).$$

Then

$$(h_{n-1}\,\partial_n + \partial_{n+1}\,h_n)(x) = s_{n-1}\,(\partial_n x - s_{n-2}\partial_{n-1}\partial_n x) + \partial_{n+1}s_n(x - s_{n-1}\partial_n x)$$

$$= s_{n-1}\,\partial_n x + \partial_{n+1}s_n x + (x - s_{n-1}\partial_n x) = x.$$

so h is a contracting homotopy.

§2. Extensions

Still we're dealing with left R-modules.

2.1. DEFINITION. Two short exact sequences $0\to L\to M\to N\to 0$ and $0\to L\to M'\to N\to 0$ are <u>equivalent</u> if there is a map $M\to M'$ giving a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & L & \longrightarrow & M' & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

By the snake lemma the map $M\to M'$ must be an isomorphism. It follows that equivalence is an equivalence relation.

2.2. PROPOSITION. Given a short exact sequence $\xi : 0\to L\to M\to N\to 0$ and a map $\theta : L\to L'$ there is a short exact sequence $\xi' : 0\to L'\to M'\to N\to 0$, the <u>pushout</u> of ξ <u>along</u> θ, unique up to equivalence, fitting into a commutative diagram

$$\begin{array}{cccccccccc} \xi: & 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & & \downarrow\theta & & \downarrow\phi & & \| & & \\ \xi': & 0 & \longrightarrow & L' & \xrightarrow[f']{} & M' & \xrightarrow[g']{} & N & \longrightarrow & 0 \end{array}$$

PROOF. Existence. Set $M' = (L'\oplus M)/\{(\theta(\ell),-f(\ell)) \mid \ell\in L\}$ and let the maps be the natural ones. Explicitly, $f'(\ell') = [(\ell',0)]$, $g'([(\ell',m)]) = g(m)$, $\phi(m) = [(0,m)]$. It is easy to check that the diagram is commutative and has exact rows.

Uniqueness. The sequence

$$0 \longrightarrow L \xrightarrow{\begin{pmatrix}\theta\\ -f\end{pmatrix}} L'\oplus M \xrightarrow{(f'\ \phi)} M' \longrightarrow 0$$

is exact by diagram chasing. It follows that M' is isomorphic to $(L'\oplus M)/\{(\theta(\ell),-f(\ell)) \mid \ell\in L\}$. This gives an equivalence between ξ' and the exact sequence we constructed above.

2.3. PROPOSITION. Given a short exact sequence $\xi : 0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ and a map $\psi : N'' \longrightarrow N$ there is a short exact sequence $\xi'' : 0 \longrightarrow L \longrightarrow M'' \longrightarrow N'' \longrightarrow 0$, the <u>pullback</u> of ξ <u>along</u> θ, unique up to equivalence, fitting into a commutative diagram

$$\begin{tikzcd}
\xi'': 0 \arrow[r] & L \arrow[r] \arrow[d, equal] & M'' \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d, "\psi"] & 0 \\
\xi : 0 \arrow[r] & L \arrow[r, "f"] & M \arrow[r, "g"] & N \arrow[r] & 0
\end{tikzcd}$$

PROOF. For existence set $M'' = \{(m,n'') \in M \oplus N'' \mid g(m) = \psi(n'')\}$, and for uniqueness show that $0 \longrightarrow M'' \longrightarrow M \oplus N'' \longrightarrow N \longrightarrow 0$ is exact.

2.4. PROPOSITION. The following properties of a module P are equivalent

(1) If $M \twoheadrightarrow N$ then any map $P \longrightarrow N$ lifts to a map $P \longrightarrow M$.

(2) $0 \longrightarrow \mathrm{Hom}(P,L) \longrightarrow \mathrm{Hom}(P,M) \longrightarrow \mathrm{Hom}(P,N) \longrightarrow 0$ is exact for any short exact sequence $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$.

(3) Any short exact sequence $0 \longrightarrow L \longrightarrow M \longrightarrow P \longrightarrow 0$ splits.

(4) P is isomorphic to a direct summand of a free module.

If these conditions hold then P is said to be <u>projective</u>. Moreover, every module is a quotient of a projective module.

PROOF. (1)$\Rightarrow$(2) For any P the sequence $0 \longrightarrow \mathrm{Hom}(P,L) \longrightarrow \mathrm{Hom}(P,M) \longrightarrow \mathrm{Hom}(P,N)$ is exact by diagram chasing.

(2)$\Rightarrow$(3) Can lift $\mathrm{Id}_P \in \mathrm{Hom}(P,P)$ to a map in $\mathrm{Hom}(P,M)$. This is a section for the map $M \longrightarrow P$.

(3)$\Rightarrow$(4) Choosing a generating set of P gives a surjection from a free module onto P. This splits.

(4)$\Rightarrow$(1) It suffices to show that a free module F has this lifting property. Look at the images in N of a basis of F, and lift these to M.

2.5. PROPOSITION. The following properties of a module I are equivalent

(1) If $L \hookrightarrow M$ then any map $L \longrightarrow I$ extends to a map $M \longrightarrow I$.

(2) $0 \longrightarrow \mathrm{Hom}(N,I) \longrightarrow \mathrm{Hom}(M,I) \longrightarrow \mathrm{Hom}(L,I) \longrightarrow 0$ is exact for any short exact sequence $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$.

(3) Any short exact sequence $0 \longrightarrow I \longrightarrow M \longrightarrow N \longrightarrow 0$ splits.

If these conditions hold then I is said to be <u>injective</u>. Moreover, every module embeds in an injective module.

PROOF. (1)⇒(2)⇒(3) dual to projectives.

(3)⇒(1). We have $0 \longrightarrow L \longrightarrow M \longrightarrow M/L \longrightarrow 0$. Construct pushout

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "f"] \arrow[d, "\theta"'] & M \arrow[r] \arrow[d, "g"] & M/L \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & I \arrow[r, shift left, "h"] & M' \arrow[r] \arrow[l, shift left, "r"] & M/L \arrow[r] & 0
\end{tikzcd}$$

Now h has a retraction r. Then $rgf = rh\theta = \theta$ so rg extends θ.

Last part omitted.

2.6. DEFINITION. If M is an R-module, then a <u>projective</u> <u>resolution</u> of M is an exact sequence

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

with the P_i projective modules. It is equivalent to give a non-negative chain complex $P_\bullet$ of projective modules and a quasi-isomorphism
$P_\bullet \longrightarrow M$(in deg 0)

$$\begin{tikzcd}
\arrow[r] & P_2 \arrow[r] \arrow[d] & P_1 \arrow[r] \arrow[d] & P_0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & {} \\
\arrow[r] & 0 \arrow[r] & 0 \arrow[r] & M \arrow[r] & 0 \arrow[r] & {}
\end{tikzcd}$$

Note that every module has many different projective resolutions.
Choose any surjection $P_0 \longrightarrow M$.
Then any surjection $P_1 \longrightarrow \mathrm{Ker}(P_0 \longrightarrow M)$.
Then any surjection $P_2 \longrightarrow \mathrm{Ker}(P_1 \longrightarrow P_0)$, etc.

If one fixes a projective resolution of M then the <u>syzygies</u> of M are the modules $\Omega^n M = \mathrm{Im}(\partial : P_n \longrightarrow P_{n-1})$ (and $\Omega^0 M = M$). Thus there are exact sequences

$$0 \longrightarrow \Omega^{n+1}M \longrightarrow P_n \longrightarrow \Omega^n M \longrightarrow 0.$$

An <u>injective resolution</u> of M is an exact sequence

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \cdots$$

with I^i injective.

2.7. THEOREM (Comparison Theorem). Any map of modules $f:M \longrightarrow M'$ can be lifted to a map of projective resolutions.

$$\begin{array}{ccccccccc}
\longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow 0 \\
& \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & & \downarrow f & \\
\longrightarrow & P'_2 & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & M' & \longrightarrow 0
\end{array}$$

Moreover, any two such lifts are homotopic as chain maps $P \longrightarrow P'$.

PROOF. Consider diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega^1 M & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
& & \downarrow \Omega^1 f & & \downarrow f_0 & & \downarrow f & & \\
0 & \longrightarrow & \Omega^1 M' & \longrightarrow & P'_0 & \longrightarrow & M' & \longrightarrow & 0
\end{array}$$

Now $P'_0 \twoheadrightarrow M'$ is onto and P_0 is projective so there is a map f_0 making the right hand square commute. Then by diagram chasing there is a map $\Omega^1 f$ making the left hand square commute.

Now the same argument gets f_1 and $\Omega^2 f$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega^2 M & \longrightarrow & P_1 & \longrightarrow & \Omega^1 M & \longrightarrow & 0 \\
& & \downarrow \Omega^2 f & & \downarrow f_1 & & \downarrow \Omega^1 f & & \\
0 & \longrightarrow & \Omega^2 M' & \longrightarrow & P'_1 & \longrightarrow & \Omega^1 M' & \longrightarrow & 0
\end{array}$$

etc.

To show that any two lifts are homotopic it is equivalent to show that any lift of the zero map $M \longrightarrow M'$ is homotopic to zero. Now

$$\begin{array}{ccccccccc}
\longrightarrow P_2 & \xrightarrow{\partial_2} & P_1 & \xrightarrow{\partial_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\
\downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & & \downarrow 0 & & \\
\longrightarrow P'_2 & \xrightarrow[\partial_2]{} & P'_1 & \xrightarrow[\partial_1]{} & P'_0 & \xrightarrow[\varepsilon]{} & M' & \longrightarrow & 0
\end{array}$$

Then $\varepsilon f_0 = 0$ so f_0 has image contained in $\Omega^1 M'$.
Now $P'_1 \twoheadrightarrow \Omega^1 M'$ is onto and P_0 is projective so f_0 lifts to a map $h_0 : P_0 \longrightarrow P'_1$.
Thus $f_0 = \partial_1 h_0$.

Now suppose we've constructed $h_0, h_1, \ldots, h_{n-1}$
with $f_i = \partial_{i+1} h_i + h_{i-1} \partial_i$ for $0 < i < n$.

Then $\partial_n (f_n - h_{n-1}\partial_n) = f_{n-1}\partial_n - \partial_n h_{n-1}\partial_n = (f_{n-1} - \partial_n h_{n-1})\partial_n$

If n=1 this is 0, and if n>1 it is $h_{n-2}\partial_{n-1}\partial_n$, so also zero.

Thus $f_n - h_{n-1}\partial_n$ has image contained in $\Omega^{n+1} M'$.
Thus it lifts to a map $h_n : P_n \longrightarrow P'_{n+1}$.

2.8. COROLLARY. If P and P′ are projective resolutions of M then there is a homotopy equivalence $f : P \longrightarrow P'$ such that the triangle

$$\begin{array}{ccc}
P & & \\
f\downarrow & \searrow & \\
P' & \longrightarrow & M(\text{in deg } 0)
\end{array}$$

commutes. Moreover f is unique up to homotopy.

PROOF. The identity map $M \longrightarrow M$ lifts to a chain map $f : P \longrightarrow P'$ and $g : P' \longrightarrow P$.
Now $gf : P \longrightarrow P$ is a lift of the identity map $M \longrightarrow M$, so is homotopic to Id_P.
Similarly $fg : P' \longrightarrow P'$ is homotopic to $Id_{P'}$.

The uniqueness of f up to homotopy is part of the Comparison Theorem.

2.9. DEFINITION. If M and N are R-modules then $\mathrm{Ext}^n(M,N)$ (or more precisely $\mathrm{Ext}^n_R(M,N)$) is defined as follows. Choose a projective resolution P of M and set $\mathrm{Ext}^n(M,N) = H^n(P,N)$. Thus if $\longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ is the projective resolution, then $\mathrm{Ext}^n(M,N)$ is the cohomology in degree n of the cochain complex $0 \longrightarrow \mathrm{Hom}(P_0,N) \longrightarrow \mathrm{Hom}(P_1,N) \longrightarrow \mathrm{Hom}(P_2,N) \longrightarrow \ldots$

$\mathrm{Ext}^n(M,N)$ is an additive group. If R is commutative it is an R-module.

This doesn't depend on the choice of projective resolution. If P′ is another projective resolution then there is a homotopy equivalence $f:P \longrightarrow P'$. This gives a homotopy equivalence of cochain complexes $\mathrm{Hom}(P',N) \longrightarrow \mathrm{Hom}(P,N)$. This is a quasi-isomorphism so induces isomorphisms on cohomology $H^n(P',N) \longrightarrow H^n(P,N)$. Moreover the homotopy equivalence f is unique up to homotopy, so the cochain map $\mathrm{Hom}(P',N) \longrightarrow \mathrm{Hom}(P,N)$ is unique up to homotopy. Thus the map $H^n(P',N) \longrightarrow H^n(P,N)$ is uniquely determined.

2.10. PROPOSITION. If $N \longrightarrow N'$ is a map there is a natural map $\mathrm{Ext}^n(M,N) \longrightarrow \mathrm{Ext}^n(M,N')$. If $M'' \longrightarrow M$ is a map there is a natural map $\mathrm{Ext}^n(M,N) \longrightarrow \mathrm{Ext}^n(M'',N)$.

PROOF. The first because if P is a projective resolution of M then $N \longrightarrow N'$ induces a chain map $\mathrm{Hom}(P,N) \longrightarrow \mathrm{Hom}(P,N')$.

The second because the map $M'' \longrightarrow M$ lifts to a chain map $P'' \longrightarrow P$ of projective resolutions, unique up to homotopy, so gives a cochain map $\mathrm{Hom}(P,N) \longrightarrow \mathrm{Hom}(P'',N)$, unique up to homotopy, so gives unique maps on Ext^n.

2.11. PROPOSITION. $\mathrm{Ext}^n(M,N\oplus N') \cong \mathrm{Ext}^n(M,N)\oplus\mathrm{Ext}^n(M,N')$ and $\mathrm{Ext}^n(M\oplus M',N) \cong \mathrm{Ext}^n(M,N)\oplus\mathrm{Ext}^n(M',N)$.

PROOF. If P is a projective resolution of M then $\mathrm{Hom}(P,N\oplus N') \cong \mathrm{Hom}(P,N)\oplus\mathrm{Hom}(P,N')$. If P′ is a projective resolution of M′ then $P\oplus P'$ is a projective resolution of $M\oplus M'$ and $\mathrm{Hom}(P\oplus P',N) \cong \mathrm{Hom}(P,N)\oplus\mathrm{Hom}(P',N)$.

2.12. LEMMA. We have

$$\mathrm{Ext}^n(M,N) \cong \begin{cases} 0 & (n<0) \\ \mathrm{Hom}(M,N) & (n=0) \\ \mathrm{Coker}(\mathrm{Hom}(P_{n-1},N) \xrightarrow{i_n^*} \mathrm{Hom}(\Omega^n M,N)) & (n>0) \end{cases}$$

where $0 \longrightarrow \Omega^n M \xrightarrow{i_n} P_{n-1} \longrightarrow \Omega^{n-1} M \longrightarrow 0$.

PROOF. If $n<0$ the claim is clear since $\mathrm{Hom}(P,N)$ is a non-negative cochain complex. We deal with the other cases together, writing $P_{-1} = 0$ and $i_0 : M \longrightarrow 0$. By definition $\mathrm{Ext}^n(M,N) = \mathrm{Ker}(\partial_{n+1}^*)/\mathrm{Im}(\partial_n^*)$ where

$$\mathrm{Hom}(P_{n-1},N) \xrightarrow{\partial_n^*} \mathrm{Hom}(P_n,N) \xrightarrow{\partial_{n+1}^*} \mathrm{Hom}(P_{n+1},N)$$

Thus $\mathrm{Ext}^n(M,N) \cong \mathrm{Coker}(\mathrm{Hom}(P_{n-1},N) \longrightarrow \mathrm{Ker}(\partial_{n+1}^*))$. Now there is an exact sequence $P_{n+1} \longrightarrow P_n \longrightarrow \Omega^n M \longrightarrow 0$ so an exact sequence

$$0 \longrightarrow \mathrm{Hom}(\Omega^n M,N) \longrightarrow \mathrm{Hom}(P_n,N) \longrightarrow \mathrm{Hom}(P_{n+1},N)$$

so $\mathrm{Ker}(\partial_{n+1}^*) \cong \mathrm{Hom}(\Omega^n M,N)$.

2.13. PROPOSITION. If X is a module then for any short exact sequence $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ you get a long exact sequence

$$\begin{aligned} 0 &\longrightarrow \mathrm{Hom}(X,L) \longrightarrow \mathrm{Hom}(X,M) \longrightarrow \mathrm{Hom}(X,N) \longrightarrow \\ &\longrightarrow \mathrm{Ext}^1(X,L) \longrightarrow \mathrm{Ext}^1(X,M) \longrightarrow \mathrm{Ext}^1(X,N) \longrightarrow \\ &\longrightarrow \mathrm{Ext}^2(X,L) \longrightarrow \ldots \end{aligned}$$

We call it the long exact sequence for $\mathrm{Hom}(X,-)$.

PROOF. This is the long exact sequence in cohomology for the chain complex P.

2.14. PROPOSITION. $\mathrm{Ext}^n(M,N) = 0$ for $n>0$ if either M is projective or N is injective.

PROOF. If M is projective you can use the projective resolution with $P_0 = M$, $P_n = 0$ for $n>0$.

If N is injective then the exact sequence $0 \longrightarrow \Omega^n M \xrightarrow{i_n} P_{n-1} \longrightarrow \Omega^{n-1} M \longrightarrow 0$ gives an exact sequence $0 \longrightarrow \mathrm{Hom}(\Omega^{n-1}M,N) \longrightarrow \mathrm{Hom}(P_{n-1},N) \longrightarrow \mathrm{Hom}(\Omega^n M,N) \longrightarrow 0$, so $\mathrm{Coker}(i_n^*) = 0$.

2.15. PROPOSITION. If $0 \longrightarrow N \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \ldots$ is an injective resolution of N then you can compute $\mathrm{Ext}^n(M,N)$ as the cohomology of the cochain complex $\mathrm{Hom}(M,I^\bullet)$

$$0 \longrightarrow \mathrm{Hom}(M,I^0) \longrightarrow \mathrm{Hom}(M,I^1) \longrightarrow \mathrm{Hom}(M,I^2) \longrightarrow \ldots$$

PROOF. Break the injective resolution into short exact sequences

$$\begin{array}{ccccccccc} & & N & & & & & & \\ & & \| & & & & & & \\ 0 & \longrightarrow & \mho^0 N & \longrightarrow & I^0 & \longrightarrow & \mho^1 N & \longrightarrow & 0 \\ 0 & \longrightarrow & \mho^1 N & \longrightarrow & I^1 & \longrightarrow & \mho^2 N & \longrightarrow & 0 \end{array}$$

etc. @ = cosyzygies = upside down Ω. You get long exact sequences

$$\begin{array}{l} 0 \longrightarrow \mathrm{Hom}(M,\mho^i N) \longrightarrow \mathrm{Hom}(M,I^i) \longrightarrow \mathrm{Hom}(M,\mho^{i+1}N) \longrightarrow \\ \quad \longrightarrow \mathrm{Ext}^1(M,\mho^i N) \longrightarrow 0 \longrightarrow \mathrm{Ext}^1(M,\mho^{i+1}N) \longrightarrow \\ \quad \longrightarrow \mathrm{Ext}^2(M,\mho^i N) \longrightarrow 0 \longrightarrow \ldots \end{array}$$

Thus $\mathrm{Ext}^n(M,N) \cong \mathrm{Ext}^{n-1}(M,\mho^1 N) \cong \ldots \cong \mathrm{Ext}^1(M,\mho^{n-1}N)$ (Dimension shifting)
$\cong \mathrm{Coker}(\mathrm{Hom}(M,I^{n-1}) \longrightarrow \mathrm{Hom}(M,\mho^n N))$

Now $0 \longrightarrow \mho^n N \longrightarrow I^n \longrightarrow I^{n+1}$ is exact, so
$0 \longrightarrow \mathrm{Hom}(M,\mho^n N) \longrightarrow \mathrm{Hom}(M,I^n) \longrightarrow \mathrm{Hom}(M,I^{n+1})$ exact.
The claim follows.

2.16. PROPOSITION. If Y is a module then for any short exact sequence $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ you get a long exact sequence

$$\begin{array}{l} 0 \longrightarrow \mathrm{Hom}(N,Y) \longrightarrow \mathrm{Hom}(M,Y) \longrightarrow \mathrm{Hom}(L,Y) \longrightarrow \\ \quad \longrightarrow \mathrm{Ext}^1(N,Y) \longrightarrow \mathrm{Ext}^1(M,Y) \longrightarrow \mathrm{Ext}^1(L,Y) \longrightarrow \\ \quad \longrightarrow \mathrm{Ext}^2(N,Y) \longrightarrow \ldots \end{array}$$

We call it the long exact sequence for Hom(-,Y).

PROOF. Use an injective resolution $I^\bullet$ of Y. The maps $L\longrightarrow M\longrightarrow N$ induce maps of cochain complexes $\mathrm{Hom}(N,I^\bullet)\longrightarrow\mathrm{Hom}(M,I^\bullet)\longrightarrow\mathrm{Hom}(L,I^\bullet)$. This is an exact sequence of cochain complexes since the I^n are injective. Now use the long exact sequence in cohomology.

2.17. DEFINITION. For any short exact sequence $\xi:0\longrightarrow L\longrightarrow M\longrightarrow N\longrightarrow 0$ we define an element $\hat{\xi}\in\mathrm{Ext}^1(N,L)$ as follows. The long exact sequence for Hom(N,-) gives a map $\mathrm{Hom}(N,N)\longrightarrow\mathrm{Ext}^1(N,L)$ and $\hat{\xi}$ is the image of Id_N under this map.

2.18. LEMMA. Fix a projective resolution of N, giving exact sequences

$$0\longrightarrow\Omega^1 N\xrightarrow{i}P_0\xrightarrow{\varepsilon}N\longrightarrow 0$$

and

$$\mathrm{Hom}(P_0,L)\xrightarrow{i^*}\mathrm{Hom}(\Omega^1 N,L)\longrightarrow\mathrm{Ext}^1(N,L)\longrightarrow 0.$$

by Lemma. If $\xi:0\longrightarrow L\longrightarrow M\longrightarrow N\longrightarrow 0$ is a short exact sequence then you can find maps α,β giving a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \Omega^1 N \arrow[r] \arrow[d, "\alpha"] & P_0 \arrow[r, "\varepsilon"] \arrow[d, "\beta"] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & L \arrow[r] & M \arrow[r] & N \arrow[r] & 0.
\end{tikzcd}$$

Moreover, for any such commutative diagram the image of α in $\mathrm{Ext}^1(N,L)$ is equal to $\hat{\xi}$.

PROOF. Since P_0 is projective and $M\longrightarrow N$ is onto there is a map β. Then α exists by diagram chasing.

Now the map $\mathrm{Hom}(N,N)\longrightarrow\mathrm{Ext}^1(N,L)$ is the connecting map in cohomology for the exact sequence of cochain complexes

$$0\longrightarrow\mathrm{Hom}(P,L)\longrightarrow\mathrm{Hom}(P,M)\longrightarrow\mathrm{Hom}(P,N)\longrightarrow 0.$$

This starts

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}(P_0,L) & \longrightarrow & \mathrm{Hom}(P_0,M) & \longrightarrow & \mathrm{Hom}(P_0,N) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}(P_1,L) & \longrightarrow & \mathrm{Hom}(P_1,M) & \longrightarrow & \mathrm{Hom}(P_1,N) & \longrightarrow & 0
\end{array}$$

$\mathrm{Hom}(N,N) \cong H^0(P,N)$ with Id_N corresponding to the element $[\varepsilon]$ of $\mathrm{Hom}(P_0,N)$. Now β is a lifting of ε in $\mathrm{Hom}(P_0,M)$. Let γ be the corresponding element of $\mathrm{Hom}(P_1,L)$. Then the diagram

$$\begin{array}{ccccccccc}
 & & P_1 & \xrightarrow{\partial_1} & P_0 & \xrightarrow{\varepsilon} & N & \longrightarrow & 0 \\
 & & \downarrow\gamma & & \downarrow\beta & & \| & & \\
0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0.
\end{array}$$

commutes. Now the composition

$$\begin{array}{ccc}
P_2 & \longrightarrow & P_1 \\
 & & \downarrow \\
 & & L & \longrightarrow & M
\end{array}$$

is equal to

$$\begin{array}{ccccc}
P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 \\
 & & & & \downarrow \\
 & & & & M
\end{array}$$

so is zero. Now since $L\longrightarrow M$ is 1-1 the composition $P_2\longrightarrow P_1\longrightarrow L$ is zero. Thus γ induces a map $P_1/\mathrm{Im}(\partial_2)\longrightarrow L$, ie $\alpha:\Omega^1 N\longrightarrow L$.

2.19. THEOREM. The assignment $\xi \longmapsto \hat{\xi}$ induces a bijection between equivalence classes of short exact sequences $0\longrightarrow L\longrightarrow M\longrightarrow N\longrightarrow 0$ and elements of $\mathrm{Ext}^1(N,L)$.

PROOF. Two equivalent short exact sequences fit as the bottom two rows of a commutative diagram

$$\begin{array}{ccccccccc}
 & 0 & \longrightarrow & \Omega^1 N & \longrightarrow & P_0 & \longrightarrow & N & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle\alpha} & & \downarrow & & \| & & \\
\xi : & 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\
 & & & \| & & \downarrow & & \| & & \\
\xi' : & 0 & \longrightarrow & L & \longrightarrow & M' & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

so that ξ and ξ' give rise to the same map $P_1 \longrightarrow L$, and by the lemma $\hat{\xi} = \hat{\xi}'$.

Any element of $\mathrm{Ext}^1(N,L)$ arises as $\hat{\xi}$ by lifting the element to some $\alpha \in \mathrm{Hom}(\Omega^1 N, L)$ and then using the pushout construction to get ξ.

If two short exact sequences ξ, ξ' give the same element of $\mathrm{Ext}^1(N,L)$ then you have diagrams

$$\begin{array}{ccccccccc}
 & 0 & \longrightarrow & \Omega^1 N & \longrightarrow & P_0 & \xrightarrow{\varepsilon} & N & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \| & & \\
\xi : & 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

and

$$\begin{array}{ccccccccc}
 & 0 & \longrightarrow & \Omega^1 N & \longrightarrow & P_0 & \xrightarrow{\varepsilon} & N & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle\alpha'} & & \downarrow{\scriptstyle\beta'} & & \| & & \\
\xi' : & 0 & \longrightarrow & L & \longrightarrow & M' & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

with $\alpha' - \alpha$ in the image of the map $\mathrm{Hom}(P_0, L) \xrightarrow{i^*} \mathrm{Hom}(\Omega^1 N, L)$.
Say $\alpha' - \alpha = \phi \circ i$ with $\phi : P_0 \longrightarrow L$. Then you get a commutative diagram

$$\begin{array}{ccccccccc}
 & 0 & \longrightarrow & \Omega^1 N & \xrightarrow{i} & P_0 & \xrightarrow{\varepsilon} & N & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle\alpha'} & & \downarrow{\scriptstyle\beta + f\phi} & & \| & & \\
\xi : & 0 & \longrightarrow & L & \xrightarrow[f]{} & M & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

so by the uniqueness of pushouts, ξ and ξ' are equivalent.

2.20. EXAMPLE. The split exact sequences form one equivalence class, corresponding to the zero element of $\mathrm{Ext}^1(N,L)$. Exercise.

2.21. EXAMPLE. If $\xi : 0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ is exact and multiplication by $n \in \mathbb{Z}$ induces an automorphism of L then $n\hat{\xi}$ is represented by the exact sequence

$$0 \longrightarrow L \xrightarrow{fn^{-1}} M \xrightarrow{g} N \longrightarrow 0.$$

PROOF. There are α and β with

$$\begin{tikzcd}
 & 0 \arrow[r] & \Omega^1 N \arrow[r] \arrow[d, "\alpha"] & P_0 \arrow[r, "\varepsilon"] \arrow[d, "\beta"] & N \arrow[r] \arrow[d, equal] & 0 \\
\xi : & 0 \arrow[r] & L \arrow[r] & M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

then there is a diagram

$$\begin{tikzcd}
0 \arrow[r] & \Omega^1 N \arrow[r] \arrow[d, "n\alpha"] & P_0 \arrow[r, "\varepsilon"] \arrow[d, "\beta"] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & L \arrow[r, "fn^{-1}"'] & M \arrow[r, "g"'] & N \arrow[r] & 0
\end{tikzcd}$$

2.22. REMARK. The natural maps $\mathrm{Ext}^1(N,L) \longrightarrow \mathrm{Ext}^1(N,L')$ and $\mathrm{Ext}^1(N,L) \longrightarrow \mathrm{Ext}^1(N'',L)$ given by homomorphisms $L \longrightarrow L'$ and $N'' \longrightarrow N$ correspond to pushouts and pullbacks of short exact sequences.

Pushouts is easy exercise. Pullbacks are complicated. Given a short exact sequence $\xi : 0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ and a map $\psi : N'' \longrightarrow N$ let ξ'' be the pullback. Fix projective resolutions of N and N''. You get a diagram

$$\begin{tikzcd}
 & 0 \arrow[rr] & & \Omega^1 N'' \arrow[rr] \arrow[d, "\Omega^1\psi"] \arrow[ddl, "\alpha''"'] & & P''_0 \arrow[rr, "\varepsilon"] \arrow[d, "\psi_0"] \arrow[ddl, "\beta''"'] & & N'' \arrow[rr] \arrow[d, "\psi"] \arrow[ddl, equal] & & 0 \\
 & 0 \arrow[rr] & & \Omega^1 N \arrow[rr] \arrow[ddl, "\alpha"'] & & P_0 \arrow[rr] \arrow[ddl, "\beta"'] & & N \arrow[rr] \arrow[ddl, equal] & & 0 \\
\xi'' : 0 \arrow[rr] & & L \arrow[rr] \arrow[d, equal] & & M'' \arrow[rr] \arrow[d, "\phi"] & & N'' \arrow[rr] \arrow[d, "\psi"] & & 0 & \\
\xi : 0 \arrow[rr] & & L \arrow[rr, "f"'] & & M \arrow[rr, "g"'] & & N \arrow[rr] & & 0 &
\end{tikzcd}$$

The rows ξ and ξ'' are a pullback diagram.
There are maps θ, ϕ as in the Comparison Theorem.
There are maps α, β by Lemma.

Recall that by construction $M'' = \{(m,n'')\in M\oplus N'' \mid g(m)=\psi(n'')\}$.
Define β'' by $\beta''(p) = (\beta(\psi_0(p)),\varepsilon(p))$ for $p\in P''_0$.
Then there is a unique α making the diagram commute.

Now α induces the element $\hat{\xi}$ in $\mathrm{Ext}^1(N,L)$ by Lemma.

By definition the natural map $\mathrm{Ext}^1(N,L)\longrightarrow\mathrm{Ext}^1(N'',L)$ induced by θ sends $\hat{\xi}$ to the element of $\mathrm{Ext}^1(N'',L)$ induced by $\alpha\circ\Omega^1\psi \in \mathrm{Hom}(\Omega^1 N'',L)$.

But $\alpha\circ\Omega^1\psi = \alpha''$, and the element of $\mathrm{Ext}^1(N'',L)$ that this induces is $\hat{\xi}''$.

2.23. EXAMPLE. If $n\neq 0$ then the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ has projective resolution

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.$$

Then $\mathrm{Hom}(P,N)$ is the cochain complex

$$\begin{array}{ccccccccc} & & & \text{deg } 0 & & \text{deg } 1 & & & \\ \ldots & \longrightarrow 0 & \longrightarrow & \mathrm{Hom}(\mathbb{Z},N) & \xrightarrow{n^*} & \mathrm{Hom}(\mathbb{Z},N) & \longrightarrow & 0 \longrightarrow & \ldots \\ & & & \cong & & \cong & & & \\ & & & N & \xrightarrow{n} & N & & & \end{array}$$

Thus $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},N) = \{x\in N \mid nx = 0\}$,
$\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z},N) \cong N/nN$
$\mathrm{Ext}^i(\mathbb{Z}/n\mathbb{Z},N) = 0$ for $i\geq 2$.

For example $\mathrm{Ext}^1(\mathbb{Z}/3\mathbb{Z},\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$. The three equivalence classes of short exact sequences are represented by

$$0 \longrightarrow \mathbb{Z} \xrightarrow{3} \mathbb{Z} \xrightarrow{\text{nat}} \mathbb{Z}/3\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z} \xrightarrow{-3} \mathbb{Z} \xrightarrow{\text{nat}} \mathbb{Z}/3\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow 0.$$

2.24. REMARK. Quote two facts about $\mathbb{Z}$-modules.
FACT 1. Any submodule of a free $\mathbb{Z}$-module is free.
Consequences:

(a) any projective $\mathbb{Z}$-module is free

(b) any module M has a projective resolution $0 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$

Thus $\mathrm{Ext}^n(M,N)=0$ for all $n\geq 2$.

FACT 2. A $\mathbb{Z}$-module N is injective if and only if it is divisible, that is, for all nonzero $n\in\mathbb{Z}$ and all $x\in N$ there is $x'\in N$ with $nx' = x$.

Clearly N injective implies divisible, for $\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z},N) = 0$ so $nN = N$, which implies divisible.

Conversely, if N is divisible and M is f.g. $\mathbb{Z}$-module then M is a direct sum of copies of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. Then calculation shows that $\mathrm{Ext}^1(M,N) = 0$.

The claim is that this holds for all M, so all exact sequences $0\longrightarrow N\longrightarrow E\longrightarrow M\longrightarrow 0$ split, so N is injective.

2.25. EXAMPLE. Let $R = \mathbb{Z}/p^2\mathbb{Z}$ with p prime. Thus an R-module is an additive group M with $p^2M = 0$. The R-module $\mathbb{Z}/p\mathbb{Z}$ has projective resolution

$$\longrightarrow \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

To compute $\mathrm{Ext}^n_R(\mathbb{Z}/p\mathbb{Z},M)$ have cochain complex

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}(\mathbb{Z}/p^2\mathbb{Z},M) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}/p^2\mathbb{Z},M) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}/p^2\mathbb{Z},M) & \longrightarrow & \dots \\ & & \cong & & \cong & & \cong & & \\ & & M & \xrightarrow{p} & M & \xrightarrow{p} & M & \xrightarrow{p} & \end{array}$$

Thus for $n>0$ have $\mathrm{Ext}^n(\mathbb{Z}/p\mathbb{Z},M) \cong \{x\in M \mid px=0\} / pM$.

For example $\mathrm{Ext}^n(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$.

2.26. PROPOSITION. Let M be a module and $n\geq 0$. The following are equivalent

(1) There is a projective resolution $0\longrightarrow P_n\longrightarrow \dots\longrightarrow P_0\longrightarrow M\longrightarrow 0$.

(2) $\mathrm{Ext}^{n+1}(M,N) = 0$ for all modules N.

The <u>projective</u> <u>dimension</u> of M is the smallest integer n with this property (or ∞ if there is none).

The <u>global</u> <u>dimension</u> of the ring R is the maximum of the projective dimensions of its modules.

PROOF. (1)⇒(2) is trivial.
(2)⇒(1). If P is a projective resolution then you have an exact sequence

$$0 \longrightarrow \Omega^n M \longrightarrow P_{n-1} \longrightarrow P_{n-2} \longrightarrow \dots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

and it suffices to prove that $\Omega^n M$ is projective, for then this exact sequence is a projective resolution as required. For this it suffices to prove that $\mathrm{Ext}^1(\Omega^n M,N) = 0$ for all N. Now use dimension shifting.
$0 \longrightarrow \Omega^n M \longrightarrow P_{n-1} \longrightarrow \Omega^{n-1} M \longrightarrow 0$ gives

$$\longrightarrow \underset{=0}{\mathrm{Ext}^1(P_{n-1},N)} \longrightarrow \mathrm{Ext}^1(\Omega^n M,N) \longrightarrow \mathrm{Ext}^2(\Omega^{n-1} M,N) \longrightarrow \underset{=0}{\mathrm{Ext}^2(P_{n-1},N)} \longrightarrow$$

so $\mathrm{Ext}^1(\Omega^n M,N) \cong \mathrm{Ext}^2(\Omega^{n-1} M,N)$. Similarly get

$$\mathrm{Ext}^2(\Omega^{n-1} M,N) \cong \mathrm{Ext}^3(\Omega^{n-2} M,N) \cong \dots \cong \mathrm{Ext}^{n+1}(\Omega^0 M,N) = 0.$$

2.27. EXAMPLES. (1) R has global dimension 0 if and only if R is semisimple artinian.

- If semisimple artinian then all modules are semisimple, so all short exact sequences are split, so gl dim 0.

- If global dimension zero then every left ideal is a direct summand of R, which implies that R is semisimple artinian.

(2) $\mathbb{Z}$ has global dimension 1.

(3) $\mathbb{Z}/p^2\mathbb{Z}$ has global dimension ∞.

2.28. EXAMPLE. If R is a ring then gl.dim R[x] = gl.dim R + 1. Thus if K is a field then gl.dim $K[x_1,\dots,x_n] = n$.

PROOF THAT gl.dim R[x] ≤ gl.dim R + 1.

(1) If $\text{proj.dim}_R\ N \le n$ then $\text{proj dim}_{R[x]}\ R[x]\otimes_R N \le n$. There is projective resolution

$$0 \longrightarrow P_n \longrightarrow \ldots \longrightarrow P_0 \longrightarrow N \longrightarrow 0$$

and tensoring with R[x] get

$$0 \longrightarrow R[x]\otimes_R P_n \longrightarrow \ldots \longrightarrow R[x]\otimes_R P_0 \longrightarrow R[x]\otimes_R N \longrightarrow 0$$

Now $R[x]\otimes_R P_i$ is projective R[x]-module.

(2) If M is an R[x]-module then there is an exact sequence of R[x]-modules

$$0 \longrightarrow R[x]\otimes_R M \underset{h_1}{\overset{\alpha}{\rightleftarrows}} R[x]\otimes_R M \underset{h_0}{\overset{\beta}{\rightleftarrows}} M \longrightarrow 0$$

where $\alpha(p\otimes m) = px\otimes m - p\otimes xm$ and $\beta(p\otimes m) = pm$ for $p\in R[x]$ and $m\in M$.

Clearly $\beta\alpha = 0$. To prove it is exact, consider it as a chain complex of R-modules with M in degree 0. Define maps h_0, h_1 via

$$h_0(m) = 1\otimes m, \quad h_1(rx^i\otimes m) = \textstyle\sum_{j=0}^{i-1} rx^j\otimes x^{i-j-1}m.$$

A straightforward calculation shows that h is a contracting homotopy, so the chain complex is acyclic.

(3) Thus any R[x]-module M fits in an exact sequence $0\longrightarrow L\longrightarrow L\longrightarrow M\longrightarrow 0$ with L having $\text{proj.dim} \le n$. Thus if N is any R[x]-module the long exact sequence for Hom(-,N) gives

$$..\longrightarrow \text{Ext}^{n+1}(L,N)\longrightarrow \text{Ext}^{n+2}(M,N)\longrightarrow \text{Ext}^{n+2}(L,N)\longrightarrow$$

The outside terms vanish, so the middle term does, so $\text{proj.dim}\ M \le n+1$.

2.29. ASIDE. Analogous to Ext^n there are Tor groups $\text{Tor}_n^R(X,Y)$ defined for X a right R-module and Y a left R-module.

You can define it by taking a projective resolution $P_\bullet$ of X and taking the homology of the chain complex

$$\longrightarrow P_2 \otimes Y \longrightarrow P_1 \otimes Y \longrightarrow P_0 \otimes Y \longrightarrow 0$$

or by taking a projective resolution $Q_\bullet$ of Y and taking the homology of

$$\longrightarrow X \otimes Q_2 \longrightarrow X \otimes Q_1 \longrightarrow X \otimes Q_0 \longrightarrow 0$$

If $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence of right R-modules you get a long exact sequence

$$\longrightarrow \mathrm{Tor}_2(N,Y) \longrightarrow \mathrm{Tor}_1(L,Y) \longrightarrow \mathrm{Tor}_1(M,Y) \longrightarrow \mathrm{Tor}_1(N,Y) \longrightarrow L \otimes Y \longrightarrow M \otimes Y \longrightarrow N \otimes Y \longrightarrow 0$$

and similarly for the second variable.

2.30. ASIDE. If R is a ring, the <u>derived</u> <u>category</u> D(R) has objects the cochain complexes of R-modules and morphisms as in the homotopy category K(R), except that one adjoins an inverse to any quasi-isomorphism. (This is analogous to Ore localization of rings RS^{-1}). The effect is that

(1) A module M, identified with the complex M(in deg 0), is isomorphic to its projective resolutions.

(2) $\mathrm{Hom}_{D(R)}(M(\text{in deg } n), N(\text{in deg } 0)) \cong \mathrm{Ext}^n(M,N)$.

Thus elements of Ext^n become morphisms in D(R).

§3. Group cohomology

References

K. S. Brown, Cohomology of groups
Cassels and Frölich, Algebraic number theory
J.-P. Serre, Local fields

3.1. DEFINITION. Let G be a group. The group algebra $\mathbb{Z}G$ is the free $\mathbb{Z}$-module with basis the elements of G. Thus a typical element is

$$\sum_{g\in G} a_g\, g$$

with $a_g \in \mathbb{Z}$, all but finitely many zero. Then $\mathbb{Z}G$ is a ring with multiplication defined by

$$\left(\sum_{g\in G} a_g\, g\right)\left(\sum_{h\in G} b_h\, h\right) = \sum_{g,h\in G} a_g b_h\, gh.$$

The identity element is given by the identity element of G.

A $\mathbb{Z}G$-module is exactly the same thing as a $\mathbb{Z}$-module M and a group homomorphism $G \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(M)$ (group of invertible $\mathbb{Z}$-module maps $M \longrightarrow M$).

Any $\mathbb{Z}$-module M becomes <u>a</u> <u>trivial</u> $\mathbb{Z}G$-module by using the homomorphism sending any element of G to the identity map $M \longrightarrow M$. In particular $\mathbb{Z}$ becomes <u>the</u> <u>trivial</u> $\mathbb{Z}G$-module.

3.2. DEFINITION. If M is a $\mathbb{Z}G$-module then its <u>cohomology</u> is

$$H^n(G,M) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},M).$$

(Its homology is defined using Tor. No more complicated, but I won't discuss).

Thus if $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ you get a long exact sequence sequence
$0 \longrightarrow H^0(G,L) \longrightarrow H^0(G,M) \longrightarrow H^0(G,N) \longrightarrow H^1(G,L) \longrightarrow \ldots$

*** We shall compute this using a standard projective resolution of the trivial module.

3.3. DEFINITION. The bar resolution for G is the system

$$\longrightarrow P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

where

- P_n is the free $\mathbb{Z}$-module with basis the elements $[g_0|g_1|...|g_n]$, made into a $\mathbb{Z}G$-module by defining $g\,[g_0|...|g_n] = [gg_0|...|gg_n]$,
- ε is the map sending each basis element $[g_0]$ to 1
- $\partial_n : P_n \longrightarrow P_{n-1}$ is given by $\partial_n[g_0|...|g_n] = \sum_{i=0}^{n}(-1)^i\,[g_0|...|\hat{g}_i|...|g_n]$.

3.4. PROPOSITION. The bar resolution is a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module.

PROOF. P_n is a free $\mathbb{Z}G$-module with basis the elements $[1|g_1|...|g_n]$.

∂_n and ε are clearly $\mathbb{Z}G$-module maps.

Clearly $\varepsilon\partial_1 = 0$. To see that $\partial^2 = 0$ follow the proof for simplicial complexes.

To show that the sequence

$$\longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

is exact, we show that it is contractible as a chain complex of $\mathbb{Z}$-modules. Define maps

$h_{-1} : \mathbb{Z} \longrightarrow P_0$ the map sending 1 to [1]
$h_n : P_n \longrightarrow P_{n+1}$ the map sending $[g_0|...|g_n]$ to $[1|g_0|...|g_n]$.

Then $\partial_{n+1}h_n([g_0|...|g_n]) = \partial_{n+1}([1|g_0|...|g_n])$

$$= [g_0|...|g_n] - [1|\hat{g}_0|g_1|...|g_n] + \dots$$

$$= [g_0|\dots|g_n] - \sum_{i=0}^{n}(-1)^n[g_0|\dots|\hat{g}_i|\dots|g_n]$$

$$= [g_0|\dots|g_n] - h_{n-1}\partial_n([g_0|\dots|g_n]).$$

so $\partial_{n+1}h_n + h_{n-1}\partial_n$ is the identity on P_n. Also εh_{-1} is the identity on $\mathbb{Z}$. Thus h is a contracting homotopy.

3.5. PROPOSITION. If $P_\bullet$ is the bar resolution and M is a $\mathbb{Z}G$-module then you can identify the cochain complex Hom(P,M) with the non-negative cochain complex $C^n = \{\text{functions } G^n \longrightarrow M\}$ and $\partial{:}C^n \longrightarrow C^{n+1}$ defined by

$$(\partial f)(g_1,\dots,g_{n+1}) = g_1\ f(g_2,\dots,g_{n+1})$$
$$+ \sum_{i=1}^{n} (-1)^i\ f(g_1,\dots,g_ig_{i+1},\dots,g_{n+1})$$
$$+ (-1)^{n+1}\ f(g_1,\dots,g_n)$$

PROOF. This formula looks nothing like the one in the bar resolution. How can they be related?

First $\mathrm{Hom}(P,M)^n = \mathrm{Hom}_{\mathbb{Z}G}(P_n,M)$.

Now P_n is the free $\mathbb{Z}G$-module with basis the elements $[1|g_1|\dots|g_n]$.
Thus P_n is the free $\mathbb{Z}G$-module with basis $[1|h_1|h_1h_2|\dots|h_1\dots h_n]$ $(h_i\in G)$.
Thus we can identify $\mathrm{Hom}_{\mathbb{Z}G}(P_n,M)$ with the set of functions $G^n \longrightarrow M$, with a homomorphism $\theta{:}P_n \longrightarrow M$ corresponding to the function

$$f{:}G^n \longrightarrow M,\ f(h_1,\dots,h_n) = \theta([1|h_1|h_1h_2|\dots|h_1\dots h_n]).$$

Now the differential in the cochain complex Hom(P,M) sends $\theta\in\mathrm{Hom}(P_n,M)$ to the composite $\theta\partial_{n+1} \in \mathrm{Hom}(P_{n+1},N)$. After the identification, it sends a function $f{:}G^n \longrightarrow M$, corresponding to homomorphism θ to the function ∂f with

$$(\partial f)(h_1,\dots,h_{n+1}) = \theta\partial_{n+1}([1|h_1|h_1h_2|\dots|h_1\dots h_n|h_1\dots h_{n+1}])$$

$$= \theta(\ [h_1|h_1h_2|\dots|h_1\dots h_n|h_1\dots h_{n+1}]$$
$$+ \sum_{i=1}^{n} (-1)^i\ [1|h_1|\dots|\overline{h_1\dots h_i}|\dots|h_1\dots h_{n+1}]$$

$$+ (-1)^{n+1} [1|h_1|\ldots|h_1\ldots h_n] \,)$$

1st term is $\theta(h_1[1|h_2|\ldots|h_2\ldots h_{n+1}]) = h_1\, f(h_2,\ldots,h_{n+1})$

2nd term is $\sum_{i=1}^{n} (-1)^i\, f(h_1,\ldots,h_i h_{i+1},\ldots,h_{n+1})$

3rd term is $(-1)^{n+1}\, f(h_1,\ldots,h_n)$.

3.6. COROLLARY. You can identify

$$H^n(G,M) = \frac{\text{n-cocycles}}{\text{n-coboundaries}}$$

where an n-cocycle is a function $f:G^n \longrightarrow M$ satisfying $\partial f = 0$ with ∂ as in the last proposition, and an n-coboundary is a function of the form ∂f with $f:G^{n-1} \longrightarrow M$.

3.7. COROLLARY.

(1) $H^0(G,M) = M^G$ the set of fixed points of M, so $M^G = \{x\in M \mid gx = x \ \forall\ g\in G\}$

(2) $H^1(G,M) = \{\text{crossed homomorphisms } f:G\longrightarrow M\} / \{\text{principal ones}\}$ where a function $f:G\longrightarrow M$ is a crossed homomorphism if $f(g_1g_2) = g_1f(g_2) + f(g_1)$, and it is principal if there is $x\in M$ with $f(g) = gx - x$ for all g.

(3) $H^2(G,M) = \{\text{factor sets } f:G\times G\longrightarrow M\} / \{\text{2-coboundaries}\}$ where a function $f:G\times G\longrightarrow M$ is a factor set if

$$g_1\, f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2) = 0.$$

3.8. REMARK. Suppose that M and G are groups. Recall that a <u>group extension</u> $1\longrightarrow M\xrightarrow{\theta} E\xrightarrow{\phi} G\longrightarrow 1$ is given by an injective group homomorphism θ and a surjective one ϕ with $\mathrm{Im}(\theta) = \mathrm{Ker}(\phi)$.

Now if M is an additive group then it becomes a $\mathbb{Z}G$-module as follows. Identify M with a subgroup of E, then it is a normal subgroup. Now let $g\in G$ act on $m\in M$ via $g.m = eme^{-1}$ for any e with $\phi(e) = g$. This is well-defined since M is abelian.

Now if M is a $\mathbb{Z}G$-module then one can show that $H^2(G,M)$ classifies equivalence classes of extensions for which the induced action of G on M is the given module action. [Given an extension, for each $g \in G$ choose $e_g \in E$ with $\phi(e_g)=g$. Then the function $f(g_1,g_2) = e_{g_1} e_{g_2} e_{g_1 g_2}^{-1}$ is a factor set.]

If M is a trivial $\mathbb{Z}G$-module then $H^2(G,M)$ classifies equivalence classes of <u>central</u> <u>extensions</u>, those with $M \subseteq Z(E)$.

WARNING. $H^1(G,M)$ classifies extensions of $\mathbb{Z}G$-modules $0 \longrightarrow M \longrightarrow E \longrightarrow \mathbb{Z} \longrightarrow 0$. Don't confuse these.

3.9. EXAMPLE. If M is a trivial $\mathbb{Z}G$-module then $H^1(G,M) = \mathrm{Hom}_{\mathrm{group}}(G,M)$. Thus, for example if G is finite then $H^1(G,\mathbb{Z}) = 0$.

3.10. EXAMPLE. Say G is the cyclic group of order m with generator σ. Let $N = 1 + \sigma + \sigma^2 + \ldots + \sigma^{m-1}$. Thus $(\sigma-1)N = \sigma^m - 1 = 0$. Then the trivial $\mathbb{Z}G$-module has projective resolution

$$\ldots \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

where $\varepsilon(g)=1$ for all $g \in G$ and the other maps are multiplication by $\sigma-1$ or N. To check this is exact, say $\xi \in \mathbb{Z}G$, $\xi = \sum_{i=0}^{m-1} a_i \sigma^i$ with $a_i \in \mathbb{Z}$.

If $N\xi = 0$ then $\sum a_i N = 0$ since $N\sigma^i = N$.
Thus $\sum a_i = 0$, so $\xi = \sum_{i=1}^{m-1} a_i(\sigma^i - 1) \in (\sigma-1)\, \mathbb{Z}G$.

If $(\sigma-1)\xi = 0$ then $\sum a_i \sigma^{i+1} = \sum a_i \sigma^i$ so $a_0 = a_1 = \ldots = a_{m-1}$.
Thus $\xi = a_0(1+\sigma+\ldots+\sigma^{m-1}) \in N\, \mathbb{Z}G$.

Thus $H^n(G,M)$ is the cohomology of the cochain complex

$$0 \longrightarrow M \xrightarrow{\sigma-1} M \xrightarrow{N} M \xrightarrow{\sigma-1} M \xrightarrow{N} \ldots$$

$$\text{so } H^n(G,M) = \begin{cases} \{x \in M \mid \sigma x = x\} & (n=0) \\ \{x \in M \mid Nx = 0\} / (\sigma-1)M & (n \text{ odd}) \\ \{x \in M \mid \sigma x = x\} / N M & (n \geq 2 \text{ even}). \end{cases}$$

eg $H^n(G,\mathbb{Z}) = \begin{cases} \mathbb{Z} & (n=0) \\ 0 & (n \text{ odd}) \\ \mathbb{Z}/m\mathbb{Z} & (n\geq 2 \text{ even}). \end{cases}$

*** Next we do some nonabelian cohomology.

3.11. DEFINITION. A multiplicative G-module (my name) is a group M together with a homomorphism $\rho:G\longrightarrow \mathrm{Aut}(M)$. If $g\in G$ and $x\in M$ we write gx for $\rho(g)(x)$. Thus $g(xy) = (gx)(gy)$ and $g(x^{-1}) = (gx)^{-1}$.

Observe that an abelian multiplicative G-module is exactly the same as a $\mathbb{Z}G$-module, it just depends whether you write the operation as $\times$ or +.

Now suppose that M is a multiplicative G-module.

Define $M^G = \{x\in M \mid gx = x\}$. This is a subgroup of M.

A function $f:G\longrightarrow M$ is a crossed homomorphism if $f(g_1g_2) = f(g_1)\,(g_1f(g_2))$.

Two crossed homomorphisms f,f' are equivalent if there is $x\in M$ with $f'(g) = x^{-1}\,f(g)\,(gx)$ for all $g\in G$.

A crossed homomorphism is principal if there is $x\in M$ with $f(g) = x^{-1}\,(gx)$ for all $g\in G$. Thus the principal crossed homomorphisms form one equivalence class.

Let $H^1(G,M)$ be the set of equivalence classes of crossed homomomorphisms $G\longrightarrow M$. This generalizes the notion for $\mathbb{Z}G$-modules. It is a set with a distinguished element, the equivalence class of principal crossed homomorphisms.

*** The long exact sequence in cohomology extends to G-groups:

3.12. THEOREM. Let $1\longrightarrow L\xrightarrow{\theta} M\xrightarrow{\phi} N\longrightarrow 1$ be a central extension of multiplicative G-modules (so L is abelian, and can be considered as a

$\mathbb{Z}G$-module). Then there is a natural sequence of maps of sets

$$1 \longrightarrow L^G \longrightarrow M^G \longrightarrow N^G \longrightarrow H^1(G,L) \longrightarrow H^1(G,M) \longrightarrow H^1(G,N) \longrightarrow H^2(G,L)$$

which is exact in the sense that at each stage $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ one has $\mathrm{Im}(\alpha) = \beta^{-1}(e)$ where e is the identity element of Z if it is a group, or is the equivalence class of principal crossed homomorphisms in H^1.

PROOF. I'll define the maps. The exactness is straightforward.

The maps $L^G \longrightarrow M^G \longrightarrow N^G$ are group homomorphisms obtained by restricting θ, ϕ.

The maps $H^1(G,L) \longrightarrow H^1(G,M) \longrightarrow H^1(G,N)$ are given by composing a crossed homomorphism with θ or ϕ.

The connecting map $N^G \longrightarrow H^1(G,L)$ is given as follows. Identify L with a subgroup of M. If $x \in N^G$, choose $m_x \in \phi^{-1}(x)$ and send x to the equivalence class of the crossed homomorphism

$$f_x : G \longrightarrow L,\ g \longmapsto m_x^{-1}.(gm_x)$$

Note that the element $m_x^{-1}.(gm_x)$ belongs to L since its image in N is $x^{-1}.(gx) = x^{-1}x = 1$.

[f_x is well-defined up to equivalence since an alternative choice of m_x would be of the form $m_x\ell$ and the crossed homomorphism this defines is

$$f'(g) = (m_x\ell)^{-1}(g(m_x\ell)) = \ell^{-1}m_x^{-1}(gm_x)(g\ell) = \ell^{-1}\ f(g)\ (g\ell)$$

so it is equivalent to f.]

The connecting map $H^1(G,N) \longrightarrow H^2(G,L)$ is given as follows.
Suppose $f : G \longrightarrow N$ is a crossed homomorphism.
For each $g \in G$ choose $m_g \in \phi^{-1}(f(g))$.
For $g_1, g_2 \in G$ define $\alpha(g_1,g_2) = m_{g_1}\ (g_1\ m_{g_2})\ m_{g_1g_2}^{-1}$.

Now check:

1. Identifying L as a subgroup of M you have $\alpha(g_1,g_2) \in L$.
2. The function $\alpha:G\times G \longrightarrow L$ is a factor set.
3. Up to a 2-coboundary, α doesn't depend on the choice of the m_g.
4. A crossed homomorphism equivalent to f gives a factor set which differs by a 2-coboundary.

Now the connecting map sends the equivalence class of f to the class of α in $H^2(G,L)$.

3.13. EXAMPLE. Representations and projective representations.
Let K be a field (usually $\mathbb{C}$).

A <u>representation</u> (or <u>ordinary</u> <u>representation</u>) of G over K is a homomorphism $\rho:G \longrightarrow GL_n(K)$.

Two representations $\rho,\rho':G \longrightarrow GL_n(K)$ are <u>equivalent</u> if there is a matrix $A \in GL_n(K)$ with $\rho'(g) = A^{-1}\rho(g)A$ for all $g \in G$.

(One can show that equivalence classes of representations correspond 1-1 to isomorphism classes of KG-modules which are finite dimensional vector spaces / K.)

Consider $GL_n(K)$ as a trivial multiplicative G-module.

Then $H^1(G,GL_n(K))$ = representations / equivalence.

Recall that $Z(GL_n(K)) = \{diag(a,a,...,a) \mid a \in K,\ a \neq 0\} \cong K^\times$.
Define $PGL_n(K) = GL_n(K) / Z(GL_n(K))$. The <u>projective</u> <u>general</u> <u>linear</u> <u>group</u>.

(To those who know about projective varieties:

- If K is alg. closed then $PGL_n(K)$ is affine variety, NOT projective.
- $PGL_n(K) \cong Aut_{variety}(\mathbb{P}^{n-1})$)

A <u>projective</u> <u>representation</u> of G is a homomorphism $\sigma:G \longrightarrow PGL_n(K)$.

DO NOT CONFUSE. Projective module with projective representation.

Two projective representations $\sigma, \sigma' : G \longrightarrow PGL_n(K)$ are <u>equivalent</u> if there is $A \in PGL_n(K)$ with $\sigma'(g) = A^{-1}\sigma(g)A$ for all $g \in G$.

Thus $H^1(G, PGL_n(K))$ = projective representations / equivalence.

Have a central extension $1 \longrightarrow K^\times \longrightarrow GL_n(K) \longrightarrow PGL_n(K) \longrightarrow 1$.
Consider all as trivial multiplicative G-modules.
Get sequence $\ldots \longrightarrow H^1(G, GL_n(K)) \xrightarrow{b} H^1(G, PGL_n(K)) \xrightarrow{c} H^2(G, K^\times)$.

The map b sends a representation $G \xrightarrow{\rho} GL_n(K)$ to the projective representation $G \longrightarrow GL_n(K) \xrightarrow{nat} PGL_n(K)$.

Thus a projective resolution σ lifts to an ordinary representation ρ if and only if $c(\sigma) = 0$ in $H^2(G, K^\times)$. One says that $c(\sigma)$ is the <u>obstruction</u> to lifting σ to an ordinary representation.

In particular one can always lift if $H^2(G, K^\times) = 0$.
The <u>Schur</u> <u>multiplier</u> of G is $H^2(G, \mathbb{C}^\times)$.

§4. Hochschild cohomology

References

Jacobson, Basic algebra II

Cohn, Algebra 2nd ed, vol 3

Pierce, Associative algebras.

4.1. DEFINITION. Let R be a commutative ring.

An R-algebra A is a ring which is at the same time an R-module in a compatible way, that is, if $a,b \in A$ and $r \in R$ then $r(ab) = (ra)b = a(rb)$.

To give an R-algebra is the same as giving a ring A and a ring homomorphism $R \longrightarrow A$ with image contained in the centre of A.

- If A is an R-algebra, you get a homomorphism $R \longrightarrow A$, $r \longmapsto r.1_A$
- Given a homomorphism θ, make A into an R-module by defining $ra = \theta(r)a$.

Observe that a $\mathbb{Z}$-algebra is just a ring.

4.2. CONSTRUCTIONS.

(1) $M_n(R)$ is an R-algebra. More generally if A is an R-algebra then so is $M_n(A)$.

(2) If A is an R-algebra then so is A^{op}. This has the same R-module structure, but multiplication $a * b = b \times a$ (* the multiplication in A^{op}, $\times$ the multiplication in A).

(3) If A and B are R-algebras, then so is $A \otimes_R B$ with the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$.

EXERCISES. $M_n(R) \otimes A \cong M_n(A)$.

$M_n(R) \otimes M_m(R) \cong M_{nm}(R)$.

$Z(M_n(A)) = \{aI \mid a \in Z(A)\} \cong Z(A)$.

$M_n(A)^{op} \cong M_n(A^{op})$ under the map sending a matrix to its transpose.

4.3. DEFINITION. If A is an R-algebra then any left or right A-module M becomes an R-module by defining $rm = (r1_A)m$ for $r\in R$ and $m\in M$ for a left module, and $rm = m(r1_A)$ for a right module.

Recall that an A-B-<u>bimodule</u> consists of an additive group M together with module actions $A\times M \longrightarrow M$ and $M\times B \longrightarrow M$ which are compatible in the sense that $a(mb) = (am)b$ for all $a\in A$, $m\in M$, $b\in B$. It will also be understood that the two R-module structures on M agree, ie that $(r1_A)m = m(r1_B)$ for all $r\in R$, $m\in M$.

If A and B are R-algebras you can naturally identify A-B-bimodules with $A \otimes_R B^{op}$-modules by the identification

$$(a\otimes b)\, m \quad = \quad amb.$$

Under this identification, bimodule maps correspond to $A\otimes B^{op}$-module maps, etc.

Note that $A\otimes B^{op}$ coincides as a set with $A\otimes B$, and it is only when we want to consider it as an algebra that we need to write the "op".

In particular the free $A\otimes B^{op}$-module of rank one is $A\otimes B$. Considered as an A-B-bimodule the actions of A and B are given by $a(a'\otimes b')b'' = aa' \otimes b'b''$.

If A is an R-algebra then its <u>enveloping</u> <u>algebra</u> is $A^e = A \otimes_R A^{op}$. Thus A^e-modules correspond to A-A-bimodules.

The algebra A can naturally be considered as an A-A-bimodule.

4.4. DEFINITION. If A is an R-algebra then the <u>bar</u> <u>resolution</u> of the A-A-bimodule A is the exact sequence

$$\dots \longrightarrow S_2 \xrightarrow{\partial_2} S_1 \xrightarrow{\partial_1} S_0 \xrightarrow{\varepsilon} A \longrightarrow 0$$

where S_n the the tensor product of $n+2$ copies of A, considered as an A-A-bimodule via

$$a(a_0\otimes\ldots\otimes a_{n+1})a' = aa_0\otimes a_1\otimes\ldots\otimes a_n\otimes a_{n+1}a',$$

ε is the multiplication map, and ∂_n is given by

$$\partial_n(a_0\otimes\ldots\otimes a_{n+1}) = \sum_{i=0}^{n} (-1)^i\ a_0\otimes\ldots\otimes a_i a_{i+1}\otimes\ldots\otimes a_{n+1}.$$

It is easily checked that ∂_n,ε are bimodule maps, $\partial^2 = 0$ and $\varepsilon\partial_1 = 0$.

EXERCISE. Show that the bar resolution is exact by showing that it is contractible when considered as a chain complex of R-modules with A in degree -1.

4.5. DEFINITION. The <u>Hochschild</u> <u>cohomology</u> $H^n(A,M)$ of A with coefficients in an A-A-bimodule M is the cohomology in degree n of the cochain complex $\mathrm{Hom}(S_\bullet,M)$

$$0 \longrightarrow \mathrm{Hom}(S_0,M) \longrightarrow \mathrm{Hom}(S_1,M) \longrightarrow \mathrm{Hom}(S_2,M) \longrightarrow \ldots$$

where Hom refers to A-A-bimodule maps, or equivalently A^e-module maps.

4.6. PROPOSITION. If A is projective as an R-module, for example if R is a field, then the bar resolution is a projective resolution of A as an A^e-module, so $H^n(A,M) \cong \mathrm{Ext}^n_{A^e}(A,M)$.

PROOF. First note that $S_0 = A\otimes A$ is the free A^e-module of rank 1. For the others, if as an R-module, A is a summand of a free R-module F, then $S_n = A\otimes\ldots\otimes A$ is a summand of $A\otimes F\otimes F\otimes\ldots\otimes F\otimes A$. Now if F has basis f_i as an R-module then $A\otimes F\otimes F\otimes\ldots\otimes F\otimes A$ has basis $1\otimes f_{i1}\otimes\ldots\otimes f_{in}\otimes 1$ as an A^e-module.

4.7. PROPOSITION. If $S_\bullet$ is the bar resolution of A and M is an A-A-bimodule then you can identify the cochain complex Hom(S,M) with the non-negative cochain complex

$$C^n = \{\text{functions } A^n \longrightarrow M \text{ which are R-linear in each variable}\},$$

($C^0 = M$ since $A^0 = pt$, and no variables in which to be R-linear), and with $\partial:C^n\longrightarrow C^{n+1}$ defined by

$$(\partial f)(a_1,\ldots,a_{n+1}) = a_1 f(a_2,\ldots,a_{n+1})$$

$$+ \sum_{i=1}^{n} (-1)^i f(a_1,\ldots,a_i a_{i+1},\ldots,a_{n+1})$$

$$+ (-1)^{n+1} f(a_1,\ldots,a_n)a_{n+1}$$

Here it differs.

PROOF. For any R-module N we have a 1-1 correspondence between A-A-bimodule maps $\theta:A\otimes N\otimes A \longrightarrow M$ and R-module maps $\phi:N\longrightarrow M$ given by $\theta(a\otimes n\otimes b) = a\phi(n)b$. Thus

$$\mathrm{Hom}_{A\text{-}A\text{-bimod}}(S_n,M) \cong \mathrm{Hom}_R(\underbrace{A\otimes\ldots\otimes A}_{n},M) \cong \{\text{multilinear functions } A^n\longrightarrow M\}.$$

No need to mess about with differentials this time.

4.8. COROLLARY. If M is a $\mathbb{Z}G$-module then $H^n(G,M) \cong H^n(\mathbb{Z}G,M)$, Hochschild cohomology of the $\mathbb{Z}$-algebra $\mathbb{Z}G$ with coefficients in M, considered as a bimodule M with the given action of G on the left and the trivial action of G on the right.

4.9. COROLLARY.
(0) $H^0(A,M) = M^{(A)} = \{x\in M \mid ax = xa \text{ for all } a\in A\}$. The centre of M.

(1) $H^1(A,M) = \{\text{R-linear derivations } \delta:A\longrightarrow M\} / \{\text{inner ones}\}$ where a function $\delta:A\longrightarrow M$ is a derivation if $\delta(ab) = a\delta(b) + \delta(a)b$, and it is inner if there is $x\in M$ with $\delta(a) = ax - xa$ for all $a\in A$.

(2) $H^2(A,M) = \{\text{2-cocycles}\} / \{\text{2-coboundaries}\}$ where an R-bilinear function $f:A\times A\longrightarrow M$ is a 2-cocycle if

$$af(b,c) - f(ab,c) + f(a,bc) - f(a,b)c = 0.$$

4.10. DEFINITION. An algebra extension is an exact sequence of R-modules

$$0\longrightarrow M\xrightarrow{\theta}E\xrightarrow{\phi}A\longrightarrow 0$$

where E and A are R-algebras

ϕ is a ring homomorphism

M is an A-A-bimodule with $e\theta(x) = \theta(\phi(e)x)$, $\theta(x)e = \theta(x\phi(e))$ for $e \in E$, $x \in M$.

Then $\theta(M)$ is an ideal in E of square zero.

Two algebra extensions are <u>equivalent</u> if they have the same end terms and there is an algebra homomorphism $E \longrightarrow E'$ giving a commutative diagram.

An algebra extension is <u>split</u> if there is a subalgebra $S \subseteq E$ with $E = S \oplus \theta(M)$. The split extensions form one equivalence class.

4.11. THEOREM. If A is projective over R and M is an A-A-bimodule then $H^2(A,M)$ classifies the equivalence classes of algebra extensions.

(For comparison, $H^1(A,M)$ classifies the extensions $0 \longrightarrow M \longrightarrow E \longrightarrow A \longrightarrow 0$ of A-A-bimodules.)

CONSTRUCTION. Given such a sequence, identify M with its image in E. The sequence splits as R-modules, so there is an R-module map s which is a section for ϕ.

Now s need not be an algebra map. Its failure is given by the map.

$$f(a,b) = s(ab) - s(a)s(b)$$

Then $f: A \times A \longrightarrow M$ is a 2-cocycle since

$$\begin{aligned} s(a.bc) &= f(a,bc) + s(a)s(bc) \\ &= f(a,bc) + s(a)(f(b,c) + s(b)s(c)) \\ &= f(a,bc) + af(b,c) + s(a)s(b)s(c) \\ s(ab.c) &= f(ab,c) + f(a,b)c + s(a)s(b)s(c) \end{aligned}$$

Conversely given a 2-cocycle you can turn $A \oplus M$ into an algebra with the multiplication $(a,x)(b,y) = (ab, ay + xb + f(a,b))$, and if f was constructed as above then this algebra is isomorphic to E.

4.12. DEFINITION. The <u>Hochschild</u> <u>dimension</u> of A is

$$\mathrm{H.dim}\ A = \sup \{ n \mid H^n(A,M) \neq 0 \text{ for some A-A-bimodule } M \}.$$

If A is projective over R this is the same as proj.dim $_{A^e}$ A.

4.13. THEOREM (Wedderburn’s principal theorem). Suppose B is an algebra over a field K and $J \subseteq B$ is a nilpotent ideal. If H.dim $B/J \leq 1$ then B has a subalgebra A with $B = A \oplus J$.

PROOF. Say $J^n=0$, $n\geq 1$. Proof by induction on n. Trivial for n=1.
Write $\bar{B}$ for B/J^{n-1}. By induction $\bar{B}$ has a subalgebra $\bar{C}$ with $\bar{B} = \bar{C}\oplus\bar{J}$.
Lifting to B we have $B=C+J$ and $C\cap J = J^{n-1}$.
Then $C/C\cap J \cong B/J$ and $(C\cap J)^2 = 0$ so the algebra extension

$$0 \longrightarrow C\cap J \longrightarrow C \longrightarrow C/C\cap J \longrightarrow 0$$

splits. Thus C has a subalgebra A with $C=A\oplus(C\cap J)$.
Then $B=A\oplus J$.

4.14. PROPOSITION. If A is projective over R, and M is an A-module then proj.dim $_A$ M $\leq$ proj.dim $_R$ M + H.dim A. In particular gl.dim A $\leq$ gl.dim R + H.dim A.

PROOF. First suppose that M is projective as an R-module. Let n = H.dim A and take a projective resolution of A as an A^e-module

$$0 \longrightarrow P_n \longrightarrow \dots \longrightarrow P_0 \longrightarrow A \longrightarrow 0.$$

Since A is projective as an R-module, $A\otimes_R A$ is projective as a left A-module, and hence so is any projective A^e-module. Now by induction all the syzygy sequences $0\longrightarrow\Omega^{n+1}A\longrightarrow P_n\longrightarrow\Omega^n A\longrightarrow 0$ are split and all $\Omega^n A$ are projective left A-modules. Thus these sequences stay exact on tensoring with M. Reassembling you get an exact sequence

$$0 \longrightarrow P_n\otimes_A M \longrightarrow \dots \longrightarrow P_0\otimes_A M \longrightarrow M \longrightarrow 0.$$

Now $(A\otimes_R A)\otimes_A M \cong A\otimes_R M$ is projective as an A-module, so all $P_i\otimes_A M$ are projective A-modules, so proj.dim $M \leq n$.

Now suppose that $m = \mathrm{proj.dim}_R\, M$ is general. Take a projective resolution $\longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ of M. It is also a projective resolution as an R-module, so $\Omega^m M$ is projective as an R-module, as in the proof of 2.26. By the above there is an A-module projective resolution

$$0 \longrightarrow Q_n \longrightarrow \dots \longrightarrow Q_0 \longrightarrow \Omega^m M \longrightarrow 0$$

so you get a projective resolution

$$0 \longrightarrow Q_n \longrightarrow \dots \longrightarrow Q_0 \longrightarrow P_{m-1} \longrightarrow \dots \longrightarrow P_0 \longrightarrow M \longrightarrow 0.$$

4.15. DEFINITION. An R-algebra A is <u>separable</u> if A is projective as an A^e-module.

Thus if A is projective over R, separable is the same as H.dim 0.

4.16. THEOREM. Let A be an R-algebra. Tfae

(1) A is separable.

(2) The sequence of A-A-bimodules $0 \longrightarrow J \longrightarrow A\otimes A \xrightarrow{\varepsilon} A \longrightarrow 0$ splits where ε is multiplication.

(3) There is $e \in A\otimes A$ with $\varepsilon(e)=1$ and $ae=ea$ for all $a \in A$.

PROOF. (1)$\Leftrightarrow$(2) clear.

(2)$\Rightarrow$(3) If $s: A \longrightarrow A\otimes A$ is an A-A-bimodule section for ε let $e=s(1_A)$.

(3)$\Rightarrow$(2) Define a section s by $s(a) = ae$.

REMARK. The element e in (3) is called a <u>separability</u> <u>idempotent</u> for A.

4.17. EXAMPLE. $M_n(R)$ is a separable R-algebra.

PROOF. Let u_{ij} be the matrix units and let $e = \sum_{i=1}^n u_{i1}\otimes u_{1i} \in M_n(R)\otimes M_n(R)$. Clearly $\varepsilon(e) = 1$. Also $u_{rs}e = u_{r1}\otimes u_{1s} = eu_{rs}$.

4.18. EXAMPLE. If A and B are R-algebras then $A\oplus B$ is separable if and only if A and B are separable.

PROOF. The enveloping algebra of $A \oplus B$ is $A^e \oplus B^e \oplus A \otimes B^{op} \oplus B \otimes A^{op}$. Separability idempotents of A and B combine to give one for $A \oplus B$. One for $A \oplus B$ projects down to one for A or B.

4.19. PROPOSITION. If A is a separable K-algebra, K a field, then A is semisimple.

PROOF. gl.dim $A = 0$.

§5. Descent Theory.

I wanted to do faithfully flat descent, cf Waterhouse, Introduction to affine group schemes, §17. Through lack of time I'll only do it for field extensions.

Let $K \subseteq L$ be a field extension.

5.1. DEFINITION. A K-vector space X <u>with additional structure</u> is one of the following

a K-vector space,
a K-algebra,
an A-module, for some fixed K-algebra A,
an A-B-bimodule,
etc.

If X is a K-vector space with additional structure, then $X^L = X\otimes_K L$ is an L-vector space, and the structure extends.

- If A is a K-algebra then A^L is an L-algebra. The multiplication is given by $(a\otimes\ell)(a'\otimes\ell') = aa' \otimes \ell\ell'$, and the L-algebra structure is given by the homomorphism $L \longrightarrow A^L$, $\ell \longmapsto 1\otimes\ell$.

- If M is an A-module then M^L is an A^L-module.

- If M is an A-B-bimodule then M^L is an A^L-B^L-bimodule, etc.
  Observe that $(A^L)^e = (A\otimes_K L)\otimes_L(A^{op}\otimes_K L) \cong A\otimes_K A^{op}\otimes_K L \cong (A^e)^L$.

Properties of X often carry over to X^L. This is <u>ascent</u>.
Sometimes properties of X^L carry to X. This is <u>descent</u>.

5.2. PROPOSITION. A K-algebra A is separable if and only if A^L is a separable L-algebra

PROOF. Identify $(A^L)\otimes_L(A^L)$ with $(A\otimes_K A)\otimes_K L$.

If A is separable and $e\in A\otimes A$ is a separability idempotent for A then $e\otimes 1$ is a separability idempotent for A^L.

Now suppose that A^L is separable. Choose a basis $\{\ell_i\}$ for L over K, such that $\ell_0 = 1$, and write the separability idempotent for A^L in the form $\sum_i z_i \otimes \ell_i$ with $z_i \in A \otimes_K A$.

Then $\varepsilon(e)=1$, so $\sum_i \varepsilon(z_i)\otimes\ell_i = 1$ in $A\otimes L$, so $\varepsilon(z_0) = 1$.
Also if $a\in A$ then $(a\otimes 1)e = (a\otimes 1)e$ so $\sum_i az_i\otimes\ell_i = \sum z_i a\otimes\ell_i$, and hence $az_0=z_0e$.

Thus z_0 is a separability idempotent for A.

5.3. PROPOSITION. If L/K is a finite field extension then L is a separable K-algebra if and only if the field extension is separable.

PROOF. If the field extension is separable then by the theorem of the primitive element it can be generated by one element, so $L = K[x]/(f(x))$ for some irreducible polynomial in K[x] with distinct roots in a splitting field K′ over K.

Thus $L^{K'} = K'[x]/(f(x)) = K'[x]/((x-\lambda_1)...(x-\lambda_n))$ with the λ_i distinct elements of K′.

Then $L^{K'} \cong K'\oplus...\oplus K'$ by the Chinese remainder Theorem.
Thus $L^{K'}$ is separable over K′.
Thus L is separable as a K-algebra.

Conversely if L/K is not separable there is $x\in L$ whose minimal polynomial f(x) has a repeated root in some extension K′/K.

It follows that $L^{K'}$ has nonzero nilpotent elements.
Since it is commutative, it is not semisimple artinian.
Thus it is not separable over K′.
Thus L is not separable over K.

5.4. LEMMA. If $\overline{K}$ is an algebraically closed field then, apart from $\overline{K}$ itself, there are no division algebras which are finite dimensional over $\overline{K}$.

PROOF. If $d\in D$ then the map $D \longrightarrow D$, $x \longmapsto dx$ has an eigenvalue $\lambda\in\overline{K}$, so $dx = \lambda x$ for all $x\in D$, so $(d-\lambda)x = 0$ for all x, so $d=\lambda\in K$.

5.5. THEOREM. f.d. K-algebra A is separable if and only if A^L is semisimple for any field extension L/K.

PROOF. If A is separable then so is A^L, so it is semisimple.

If all A^L are semisimple then so is $A^{\overline{K}}$ where $\overline{K}$ is the algebraic closure of K. Thus by the Lemma

$$A^{\overline{K}} \cong M_{n_1}(\overline{K}) \oplus M_{n_2}(\overline{K}) \oplus \dots$$

This is separable over $\overline{K}$, so A is separable over K.

5.6. DEFINITION. If Z is an L-vector space with additional structure then a K-<u>form</u> of Z is a K-vector space X with the same type of additional structure such that $X^L \cong Z$.

5.7. THEOREM. Suppose L/K is a finite Galois field extension with group G and Z is an L-vector space. Then there is a 1-1 correspondence between

(1) K-subspaces X of Z such that the natural map $m:X\otimes L \longrightarrow Z$ is an isomorphism
(so that X is a K-form of Z).

(2) Families of K-linear maps $\alpha_g:Z \longrightarrow Z$ satisfying

$\alpha_g(\ell z) = g(\ell)z$ for $z\in Z$, $\ell\in L$
$\alpha_{gg'} = \alpha_g\alpha_{g'}$
$\alpha_1 = \mathrm{Id}_Z$.

PROOF. Given $X \subseteq Z$ and $g\in G$ define α_g by $\alpha_g = m(1\otimes g)m^{-1}$.
These maps clearly have the right property.

Given maps α_g, define $X = \{z\in Z \mid \alpha_g(z) = z \text{ for all } g\in G\}$.

This is a K-subspace of Z.

Consider the multiplication map $m:X\otimes L \longrightarrow Z$.

Let $v_1, \dots, v_n$ be a basis of L over K.

Then G has n elements $g_1=1,\dots,g_n$.

The g_i are contained in $\mathrm{Hom}_K(L,L)$.

By Dedekind's Lemma they are linearly independent over L.

Thus the matrix $(g_i(v_j))$ is invertible.

A typical element of $X\otimes L$ is of the form $\sum x_i \otimes v_i$.

If in the kernel of m then $\sum v_i x_i = 0$.

Thus also for any j,

$$0 = \alpha_{g_j} (\sum v_i x_i) = \sum g_j(v_i)\, x_i$$

since $\alpha_{gj}(x_i) = x_i$. Thus all $x_i = 0$, so m is injective.

If $z\in Z$ then it is easy to see that $\sum \alpha_{gi}(z) \in X$.

Applying this to $v_j z$ for all j, we obtain elements $x_j \in X$ with

$$x_j = \sum_i \alpha_{gi}(v_j z) = \sum_i g_i(v_j)\, \alpha_{gi}(z)$$

By invertibility there are $b_{ij} \in L$ with

$$\alpha_{gj}(z) = \sum_i b_{ij}\, x_j$$

Thus $z = \alpha_{g1}(z) = \sum_i b_{1j} x_j$ is in the image of m.

Now it is trivial that the constructions are inverse.

5.8. DEFINITION. If X,Y are a pair of K-vector spaces with the same additional structure we say that X and Y are _twisted forms_ of each other, _split_ by L, if $X^L \cong Y^L$.

5.9. THEOREM. If X is a K-vector space with additional structure and L/K is a finite Galois field extension with group G then $\mathrm{Aut}(X^L)$ is naturally a multiplicative G-module and there is a 1-1 correspondence

$$\text{Elements of } H^1(G,\mathrm{Aut}(X^L)) \longleftrightarrow \begin{array}{l}\text{Isomorphism classes of twisted}\\ \text{forms of } X \text{ split by } L.\end{array}$$

PROOF. $\mathrm{Aut}(X^L)$ becomes a multiplicative G-module as follows. If θ is an automorphism of X^L and $g\in G$, let $g\theta$ be the composite

$$X\otimes L \xrightarrow{1\otimes g^{-1}} X\otimes L \xrightarrow{\theta} X\otimes L \xrightarrow{1\otimes g} X\otimes L.$$

By definition it is a K-linear map, but in fact it is L-linear since

$$\ell(x\otimes\ell') \longmapsto g^{-1}(\ell)(x\otimes g^{-1}\ell') \longmapsto g^{-1}(\ell)\theta(x\otimes g^{-1}\ell') \longmapsto \ell\,(g\theta)(x\otimes\ell').$$

Moreover $g\theta$ preserves the additional structure so $g\theta \in \mathrm{Aut}(X^L)$.

A twisted form Y of X gives a crossed homomorphism as follows. Choose an isomorphism $\psi{:}Y\otimes L\longrightarrow X\otimes L$ of L-vector spaces with additional structure. Now if $g\in G$ let $\rho_\psi(g)$ be the composite map

$$X\otimes L \xrightarrow{1\otimes g^{-1}} X\otimes L \xrightarrow{\psi^{-1}} Y\otimes L \xrightarrow{1\otimes g} Y\otimes L \xrightarrow{\psi} X\otimes L.$$

Again $\rho_\psi(g)$ is L-linear and belongs to $\mathrm{Aut}(X^L)$. Also

$$\begin{aligned}\rho_\psi(gg') &= \psi\,(1\otimes gg')\,\psi^{-1}\,(1\otimes g'^{-1}g^{-1})\\ &= \psi\,(1\otimes g)\,(1\otimes g')\,\psi^{-1}\,(1\otimes g'^{-1})\,(1\otimes g^{-1})\\ &= \psi\,(1\otimes g)\,\psi^{-1}\,(1\otimes g^{-1})\,(1\otimes g)\,\psi\,(1\otimes g')\,\psi^{-1}\,(1\otimes g'^{-1})\,(1\otimes g^{-1})\\ &= \rho_\psi(g)\,(1\otimes g)\,\rho_Y(g')\,(1\otimes g^{-1})\\ &= \rho_\psi(g)\,(g\,\rho_\psi(g')),\end{aligned}$$

so ρ_ψ is a crossed homomorphism $G\longrightarrow\mathrm{Aut}(X^L)$. Now if $\psi'{:}Y\otimes L\longrightarrow X\otimes L$ is a different isomorphism then $\theta=\psi(\psi')^{-1} \in \mathrm{Aut}(X^L)$, and

$$\rho_{\psi'}(g) = \theta^{-1}\,\rho_\psi(g)\,(g\theta)$$

so ρ_ψ and $\rho_{\psi'}$ are equivalent, so determine one element of $H^1(G,\mathrm{Aut}(X^L))$.

Conversely a crossed homomorphism $\rho: G \longrightarrow \mathrm{Aut}(X^L)$ gives a twisted form X_ρ as follows. The maps $\alpha_g = \rho(g)(1\otimes g) : X^L \longrightarrow X^L$ satisfy the conditions of the previous theorem. Thus

$$X_\rho = \{z\in X^L \mid \rho(g)((1\otimes g)z) = z \text{ for all } g\in G\}$$

is a K-form of X^L as a vector space. Moreover the additional structure on X^L restricts to an additional structure on X_ρ. For example if X is a K-algebra and $u,v \in X\otimes L$ then the multiplication in X extends to a multiplication for $X\otimes L$, and

$$\begin{aligned} \rho(g)((1\otimes g)(u.v)) &= \rho(g)((1\otimes g)u \,.\, (1\otimes g)v) \\ &= \rho(g)((1\otimes g)u)\ \rho(g)((1\otimes g)v) \end{aligned}$$

since $\rho(g) \in \mathrm{Aut}(X^L)$ preserves the algebra structure. Thus if $u,v\in X_\rho$ then $u.v \in X_\rho$.

Now it is easy to check that if ρ,ρ' are equivalent crossed homomorphisms then $X_\rho \cong X_{\rho'}$, and that the constructions X_ρ and ρ_ψ are inverse.

5.10. COROLLARY. If L/K is a finite Galois extension with group G then $GL_n(L)$ is naturally a multiplicative G-module and $H^1(G,GL_n(L))$ is trivial (has only one element). In particular taking n=1 we have $H^1(G,L^\times) = 1$.

(Don't confuse this with the setup of the Schur multiplier $H^2(G,\mathbb{C}^\times)$. There G is any group and the action is trivial).

PROOF. Clearly the action of $g\in G$ on a matrix (a_{ij}) is $(g(a_{ij}))$. $H^1(G,GL_n(L))$ classifies twisted forms of the K-vector space K^n split by L, but all are isomorphic to K^n.

5.11. COROLLARY. (Hilbert's Theorem 90). Suppose L/K is a Galois field extension whose group G is cyclic of order n, say generated by σ. Let N be the norm, so

$$N(x) = x.\sigma(x).\sigma^2(x)\ldots.\sigma^{n-1}(x)$$

for $x\in L$. Then $x\in L^\times$ is of the form $y^{-1}\sigma(y)$ for some $y\in L$ if and only if $N(x)=1$.

PROOF. Observe that $N(xx') = N(x)N(x')$ and $N(\sigma(x)) = N(x)$. It follows that if x has the indicated form that $N(x)=1$.

Now suppose that $N(x)=1$. Define a map $\rho:G\longrightarrow L^\times$, $\rho(\sigma^i) = x.\sigma x. \ldots \sigma^{i-1}(x)$. This is well-defined. It is a crossed homomorphism since

$$\rho(\sigma^{i+j}) = x.\sigma x. \ldots \sigma^{i+j-1}(x) = \rho(\sigma^i).\sigma^i\rho(\sigma^j).$$

Thus it is principal, so of the form

$$\rho(\sigma^i) = y^{-1}\sigma^i(y)$$

for some $y\in L^\times$. Taking $i=1$ gives $x = y^{-1}\sigma(y)$.

5.12. PROPOSITION. If K is a field then all algebra automorphisms of $M_n(K)$ are inner, so of the form $a \longmapsto s^{-1}as$ for some $s \in GL_n(K)$.
Thus $\mathrm{Aut}(M_n(K)) \cong GL_n(K) / K^\times = PGL_n(K)$.

PROOF. K^n is naturally an $M_n(K)$-module by matrix multiplication.
Now every $M_n(K)$-module is isomorphic to a direct sum of copies of this.

If $\theta:M_n(K)\longrightarrow M_n(K)$ is an algebra homomorphism you can make K^n into a different module by making $a\in M_n(K)$ act on $v\in K^n$ as $\theta(a)(v)$.

This must be isomorphic to the first module, so there is an isomorphism $s:K^n\longrightarrow K^n$ such that $s(\theta(a)v) = a(sv)$ for all $v\in K^n$, $a\in M_n(K)$.

Thus $\theta(a) = s^{-1}as$.

5.13. COROLLARY. If L/K is a finite Galois field extension with group G then The twisted forms of $M_n(K)$ split by L are classified by $H^1(G,PGL_n(K))$.

§6. Central simple algebras

6.1. DEFINITION. K be a field. A <u>central</u> <u>simple</u> K-algebra is a f.d. K-algebra which is simple and has centre $Z(A) = K$.

For example, $M_n(K)$.
$\mathbb{H}$ is a central simple $\mathbb{R}$-algebra.

6.2. LEMMA. An algebra is central simple if and only if it is of the form $M_n(D)$ where D is a division ring which has centre K and is f.d. over K.

PROOF. A f.d. simple algebra is simple artinian, so by Artin-Wedderburn it is of the form $A \cong M_n(D)$. Now $Z(M_n(D)) \cong Z(D)$.

6.3. EXAMPLE. Suppose char $K \neq 2$ and $\alpha,\beta \in K$ are nonzero. The <u>generalized</u> <u>quaternion</u> <u>algebra</u> $(\alpha,\beta/K)$ is the K-algebra with basis $1,\mathbf{i},\mathbf{j},\mathbf{k}$ and multiplication $\mathbf{i}^2 = \alpha$, $\mathbf{j}^2 = \beta$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$. Then $\mathbf{k}^2 = -\alpha\beta$, $\mathbf{ik} = -\mathbf{ki} = \alpha\mathbf{j}$, $\mathbf{jk} = -\mathbf{kj} = -\beta\mathbf{i}$. Thus $\mathbb{H} = (-1,-1/\mathbb{R})$.

It is central simple. Say $x = \lambda+a\mathbf{i}+b\mathbf{j}+c\mathbf{k}$. Now

$$\begin{aligned}
[\mathbf{i},x] &= \mathbf{i}x - x\mathbf{i} = 2\alpha c\mathbf{j} + 2b\mathbf{k} \\
[\mathbf{j},x] &= -2\beta c\mathbf{i} - 2a\mathbf{k} \\
[\mathbf{k},x] &= 2\beta b\mathbf{i} - 2\alpha a\mathbf{j}
\end{aligned}$$

so if x is central then a=b=c=0, so $x \in K$.

Suppose I is an ideal containing $x \neq 0$. Then I also contains

$$\begin{aligned}
\mathbf{i}[\mathbf{j},[\mathbf{i},x]] &= -4\beta\alpha b \\
\mathbf{j}[\mathbf{k},[\mathbf{j},x]] &= 4\alpha\beta^2 c \\
\mathbf{k}[\mathbf{i},[\mathbf{k},x]] &= 4\alpha^2\beta a
\end{aligned}$$

If b,c or $a \neq 0$ then $I = (\alpha,\beta/K)$.
If a=b=c=0 then I contains $\lambda \neq 0$, so again $I = (\alpha,\beta/K)$.

One can show that it is a division algebra if and only if the equation $\alpha u^2+\beta v^2 = w^2$ has no non-trivial solutions (u,v,w) in K. If it is not a division algebra, then by dimensions it is $M_2(K)$.

(If $x = \lambda+a\mathbf{i}+b\mathbf{j}+c\mathbf{k}$ is an element of $(\alpha,\beta/K)$, define $x^* = \lambda-a\mathbf{i}-b\mathbf{j}-c\mathbf{k}$. One can check that $(xy)^* = y^*x^*$ and $xx^* = x^*x = \lambda^2-\alpha a^2-\beta b^2+\alpha\beta c^2 \in K$. If there is non-trivial solution of the equation, then $xx^* = 0$ where $x = w+u\mathbf{i}+v\mathbf{j}$, so not a division algebra. Conversely, suppose no non-trivial solution, but not a division algebra. Then $xy = 0$ with $x,y\neq 0$. Then $0 = (xy)^*xy = y^*x^*xy = (x^*x)(y^*y)$ since $x^*x \in K$. Thus there is an element $x \neq 0$ with $x^*x = 0$. Write $x = \lambda+a\mathbf{i}+b\mathbf{j}+c\mathbf{k}$. Then $\lambda^2-\alpha a^2-\beta b^2+\alpha\beta c^2 = 0$. Hence $\alpha(a^2-\beta c^2)^2 + \beta(\lambda c+ab)^2 = (\lambda a+\beta bc)^2$. This is a trivial solution, so $a^2-\beta c^2 = 0$. This has only the trivial solution, so $a=c=0$, so $\lambda^2-\beta b^2=0$. This has only the trivial solution, so $\lambda=b=0$. Thus $x=0$. Contradiction.)

6.4. EXAMPLE. Suppose L/K is a finite Galois field extension with group G and let $f:G\times G\longrightarrow L^*$ be a factor set, so

$$g_1 f(g_2,g_3)\ f(g_1g_2,g_3)^{-1}\ f(g_1,g_2g_3)\ f(g_1,g_2)^{-1} = 1.$$

The <u>crossed</u> <u>product</u> $L*_fG$ is the following K-algebra. As a set it is the group algebra LG, but it has new multiplication

$$(\textstyle\sum_{g\in G} x_g\ g)\ (\sum_{h\in G} y_h\ h) = \sum_{g,h\in G} f(g,h)\ x_g\ g(y_h)\ gh.$$

($x_g,y_h \in L$). The factor set condition ensures this is associative.
I omit the proof that it is central simple.

If $\alpha \in K$ is not a square then $(\alpha,\beta/K)$ is a crossed product: let $L = K(\sqrt{\alpha})$, so $G = \{e,\sigma\}$ where e is the identity and $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$. Let $f:G\times G\longrightarrow L^*$ be the factor set

$$f(e,e)=1,\ f(e,\sigma)=1,\ f(\sigma,e)=1,\ f(\sigma,\sigma)=\beta.$$

Then $(\alpha,\beta/K) \cong L*_fG$ with $1,i,j,k$ corresponding to e, $\sqrt{\alpha}\ e$, σ, $\sqrt{\alpha}\ \sigma$.

6.5. THEOREM. If A is a central simple K-algebra of dimension d then
$A^e \cong M_d(K)$.

PROOF. A special case of Jacobson’s Density Theorem says that if B is a K-algebra and S is a finite dimensional simple B-module with endomorphism algebra K, then the algebra homomorphism

$$B \longrightarrow \mathrm{End}_K(S),\ b \longmapsto (s \longmapsto bs)$$

is surjective.

Apply this to $B = A^e$. To say that A has no non-trivial ideals means it is a simple A^e-module. Also $\mathrm{End}_{A^e}(A) \cong Z(A) = K$, under the map identifying $\theta\in\mathrm{End}_{A^e}(K)$ with $\theta(1)\in A$. Thus the map $A^e \twoheadrightarrow \mathrm{End}_K(A)$ is surjective. Now it is an isomorphism by dimensions. Now $\mathrm{End}_K(A) \cong M_d(K)$ where $d = \dim A$.

6.6. LEMMA. If A is a central simple K-algebra and B is a simple K-algebra then $A\otimes B$ is simple.

PROOF. If I is a non-trivial ideal in $A\otimes B$ then $A^{op}\otimes I$ is a non-trivial ideal in $A^{op}\otimes A\otimes B \cong M_n(K)\otimes B \cong M_n(B)$, but this is simple.

6.7. LEMMA. If A and B are K-algebras and $Z(A)=K$ then $Z(A\otimes B) = Z(B)$.

PROOF. Say $Z(A)=K$. Let b_i be a basis of B. Say $z = \sum a_i\otimes b_i \in Z(A\otimes B)$. Then if $a\in A$, $\sum(aa_i-a_ia)\otimes b_i = 0$ so each $aa_i-a_ia = 0$, so $a_i\in Z(A)$, so $a_i=\lambda_i 1$ with $\lambda_i\in K$. Then $z = \sum\lambda_i 1\otimes b_i = 1\otimes(\sum\lambda_i b_i) \in B$.

6.8. PROPOSITION. If A and B are central simple K-algebras then $A\otimes B$ is central simple.

6.9. DEFINITION. Two central simple algebras are similar, written $A \sim B$, if their division algebras are isomorphic. Thus $M_n(D) \sim M_m(D)$. Write [A] for the similarity class of A.

The Brauer group Br(K) consists of central simple K-algebras modulo similarity. The multiplication is defined by $[A][B] = [A\otimes B]$.

This is well-defined. By the proposition $A\otimes B$ is central simple.
Also if $A \cong M_n(D)$, $B \cong M_r(E)$, and $D\otimes E \cong M_s(F)$ then

$$\begin{aligned} A\otimes B &\cong M_n(D) \otimes M_r(E) \\ &\cong M_n(K) \otimes D \otimes M_r(K) \otimes E \end{aligned}$$

$$\begin{aligned} &\cong M_{nr}(K) \otimes D\otimes E \\ &\cong M_{nrs}(K) \otimes F \\ &\cong M_{nrs}(F) \end{aligned}$$

so $A\otimes B \sim D\otimes E$.

Clearly the multiplication is associative.

Identity element $[K]$.

Inverse of $[A]$ is $[A^{op}]$ since $A\otimes A^{op} \cong M_n(K) \sim K$.

EXAMPLES.

(1) If K is algebraically closed, $Br(K) = 1$.

(2) $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, with the two elements $[\mathbb{R}]$, $[\mathbb{H}]$.

6.10. THEOREM. If $K \subseteq L$ is a field extension then a K-algebra A is central simple if and only if A^L is central simple.

PROOF. If A is central simple, we're done by putting $B=L$ in the lemmas above.

If A^L is central simple then A must be simple, for if I is a non-trivial ideal then $I\otimes L$ is a non-trivial ideal in A^L. Also A must have centre K, for if $a\in A$ is central then $a\otimes 1$ is central in A^L.

6.11. COROLLARY. A is a central simple K-algebra $\Leftrightarrow A^{\overline{K}} \cong M_n(\overline{K})$, some n.

PROOF. No division algebras over $\overline{K}$.

6.12. COROLLARY. The dimension of any central simple algebra is a square.

6.13. COROLLARY. Any central simple algebra is separable.

One can show that the separable K-algebras are the semisimple ones $M_{n_1}(D_1)\oplus M_{n_1}(D_2)\oplus\ldots$ where all $Z(D_i)/K$ are separable field extensions.

6.14. DEFINITION. The <u>separable</u> <u>closure</u> of K is

$$K_s = \{x\in\overline{K} \mid x \text{ is separable over } K\}.$$

It is a subfield of $\overline{K}$. (Recall that x is <u>separable</u> over K if its minimal polynomial $f(x) \in K[x]$ has distinct roots in a splitting field. Equivalently if $(f(x), f'(x)) = 1$.)

If char K = 0 then $K_s = \overline{K}$.

If char K = p > 0 and $x \in \overline{K}$ one can show that $x^{p^r} \in K_s$ (some r).

6.15. THEOREM. Apart from K_s itself, there are no f.d. division algebras with centre K_s.

PROOF. Know this for algebraically closed fields, so ok for char 0.
Suppose K has characteristic p>0.
Let D be a f.d. division algebra with centre K_s.

If $x \in D$ then the subalgebra of D generated by x is commutative, finite dimensional, and a field, so it is a finite field extension of K_s. Thus it can be identified with a subfield of $\overline{K}$, so $x^{p^r} \in K_s$, some r.

If $x \in D$ let $\delta_x : K_s \longrightarrow D$ be the corresponding inner derivation, $\delta_x(a) = ax - xa$.
By induction $\delta_x^n(a) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} x^i a x^{n-i}$.
Thus $\delta_x^p(a) = ax^p - x^p a = \delta_{x^p}(a)$, so $\delta_x^{p^r}(a) = \delta_{x^{p^r}}(a)$.

Suppose $D \neq K_s$. Fix $x \in D \backslash K_s$. Then $x \notin Z(D)$, so $\delta_x \neq 0$.
Now $\delta_x^{p^r} = 0$ for some r, so there is $b \in D$ with $\delta_x(b) \neq 0$, $\delta_x^2(b) = 0$.
Thus x and $\delta_x(b)$ commute.

Let $y = bx\, \delta_x(b)^{-1}$.
Then $yx - xy = bx\, \delta_x(b)^{-1} x - xbx\, \delta_x(b)^{-1} = (bx-xb)\, \delta_x(b)^{-1} x = x$.
Thus $\delta_y(x) = -x$. Thus $\delta_y^{p^r}(x) = (-1)^{p^r} x$. But $\delta_y^{p^r}(x) = \delta_{y^{p^r}}(x) = 0$ for r large enough. Contradiction.

6.16. COROLLARY. A is central simple if and only if $A^{K_s} \cong M_n(K_s)$, some n.

6.17. COROLLARY. If A is a central simple K-algebra then there is a finite Galois field extension L/K such that $A^L \cong M_n(L)$.

PROOF. Fix a basis a_i of A and a basis b_i of $M_n(K)$, eg the matrix units. Choose isomorphisms

$$M_n(K_s) \underset{\phi}{\overset{\theta}{\rightleftarrows}} A^{K_s}.$$

Write each $\theta(b_i)$ in terms of the a_j and each $\phi(a_j)$ in terms of the b_i.
Finitely many elements of K_s occur.
Thus there is a finite extension L of K inside K_s such that all
$\theta(b_i) \in A^L$, $\phi(a_j) \in M_n(L)$.
Then L/K is separable, so can enlarge to be Galois.
Now θ and ϕ give inverse isomorphisms $M_n(L) \longrightarrow A^L$.

6.18. DEFINITION. If L/K is a field extension then there is a homomorphism $Br(K) \longrightarrow Br(L)$, $[A] \longmapsto [A \otimes L]$. The kernel is denoted by Br(L/K). It consists of the similarity classes [A] in Br(K) with $A \otimes L$ a matrix algebra over L.

6.19. COROLLARY. $Br(K) = \bigcup_{L/K \text{ Galois}} Br(L/K)$.

6.20. THEOREM. If L/K is Galois with group G then $Br(L/K) \cong H^2(G,L^*)$.

PROOF. Let S(n) be the set of isomorphism classes of central simple K-algebras of dimension n^2 split by L. These algebras are twisted forms of $M_n(K)$ split by L, so S(n) is in 1-1 correspondence with $H^1(G,PGL_n(L))$.

There is a central extension of multiplicative G-groups

$$1 \longrightarrow L^* \longrightarrow GL_n(L) \longrightarrow PGL_n(L) \longrightarrow 1.$$

This gives an exact sequence

$$\ldots \longrightarrow H^1(G,GL_n(L)) \longrightarrow H^1(G,PGL_n(L)) \longrightarrow H^2(G,L^*).$$

This gives a map $\delta_n : S(n) \longrightarrow H^2(G,L^*)$.

Also $H^1(G,GL_n(L))$ is trivial, so $\delta_n(A) = 0 \Leftrightarrow A \cong M_n(K)$.

One can show that if $A \in S(n)$ and $A' \in S(n')$ then

$$\delta_{nn'}(A\otimes A') = \delta_n(A) + \delta_{n'}(A')$$

(proof omitted).

If $A = M_r(D)$ with $\dim D = m^2$ then $A \cong M_r(K) \otimes D$, so

$$\delta_{rm}(A) = \delta_r(M_r(K)) + \delta_m(D) = \delta_m(D).$$

It follows that if $A \in S(n)$ and $B \in S(m)$ are similar then $\delta_n(A) = \delta_m(B)$.
Thus the δ_n induce a map $\delta{:}Br(L/K) \longrightarrow H^2(G,L^*)$.
Moreover this is a group homomorphism, and the kernel is trivial.

One can show that if $f{:}G\times G \longrightarrow L^*$ is a factor set then the crossed product $L*_fG$ is a twisted form of $M_n(K)$ split by L, and that its image under δ is the class $[f]$ in $H^2(G,L^*)$ (proof omitted).

It follows that δ is surjective.

REMARK. Class field theory shows that $Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ and that there is an exact sequence $0 \longrightarrow Br(\mathbb{Q}) \longrightarrow Br(\mathbb{R}) \oplus \oplus_p Br(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$.

An old problem was: is every central division algebra a crossed product?
The answer is no.