# CENTRAL SIMPLE ALGEBRAS, BRAUER GROUPS, AND GALOIS COHOMOLOGY

ADAM MORGAN

Contents

## Part 1. Central simple algebras

Outside of these notes, much of the material for this part of the course (and plenty more besides) may be found in the book 'Central Simple Algebras and Galois Cohomology' by Philippe Gille and Tamás Szamuely [GS06], and their exposition of certain topics has strongly influenced these notes. Also recommended are Pete Clark's Noncommutative Algebra notes [Cla] and Curtis and Reiner's book 'Methods of Representation Theory' [CR90]. The former has greatly informed our treatment of splitting fields. If you have any questions or corrections regarding the notes (which will be updated regularly as the semester goes on) please don't hesitate to email adam.morgan@glasgow.ac.uk.

### 1. Preliminaries

1.1. **Rings.** Rings will be associative with unit, but **not necessarily commutative**. For a ring $R$ we denote by $Z(R)$ its *centre*,

$$Z(R) = \{r \in R \mid rx = xr \ \forall x \in R\}.$$

A *left ideal* of $R$ is an additive subgroup $I \subseteq R$ such that $rI \subseteq I$ for all $r \in R$. We define *right ideals* analagously. A subset $I$ of $R$ is a *2-sided ideal* if it's both a left ideal and a right ideal. For $r \in R$, we write $Rr, rR$ and $RrR$ for the left, right and 2-sided ideals generated by $r$ respectively.

*Remark* 1.1. If $\theta : R \to S$ is a ring homomorphism (which takes $1_R$ to $1_S$ by convention) then $\ker(\theta)$ is a 2-sided ideal of $R$, we can form the quotient ring $R/\ker(\theta)$, and, via $\theta$, $R/\ker(\theta) \xrightarrow{\sim} \mathrm{im}(S)$ (which is a subring of $S$).

We say that a ring $R \neq 0$ is *simple* if it has no non-trivial 2-sided ideals (i.e. other than 0 and $R$, which are always 2-sided ideals).

Given a ring $R$ we write $R^{\mathrm{opp}}$ for the new ring whose underlying additive group is that of $R$ but with multiplication reversed, i.e. $r \cdot r' = r'r$ with the left-hand side taking place in $R^{\mathrm{opp}}$ and the right-hand side taking place in $R$.

**Example 1.2.** Let $k$ be a field and, for $n \geq 1$, let $M_n(k)$ denote the ring of $n \times n$ matrices with coefficients in $k$ (and the usual matrix addition and multiplication). Then for $n > 1$ $M_n(k)$ is not commutative, yet $M_n(k) \cong M_n(k)^{\mathrm{opp}}$ via the map taking a matrix to its transpose.

*Remark* 1.3. For a group $G$ one could define the opposite group $G^{\mathrm{opp}}$ similarly. However for any group the map sending an element to its inverse gives an isomorphism between $G$ and $G^{\mathrm{opp}}$, so this doesn't ever give anything new. We'll see examples later in the course of rings which are not isomorphic to their opposite ring.

A non-zero ring in which every non-zero element is invertible is called a *division ring* (or skew field). Clearly $R$ is a division ring if and only if $R^{\mathrm{opp}}$ is. Similarly, $R$ is simple if and only if $R^{\mathrm{opp}}$ is, as $R$ and $R^{\mathrm{opp}}$ have the same 2-sided ideals. Note that commutative division rings are fields, and that all division rings are simple. If $R$ is commutative then conversely $R$ simple implies $R$ is division. We'll shortly see that this fails in the noncommutative case (see Proposition 2.4) but we do at least have.

**Lemma 1.4.** *Let $R$ be a simple ring. Then $Z(R)$ is a field.*

*Proof.* Let $0 \neq x \in Z(R)$. Then as $x$ is central the left ideal generated by $x$, $Rx$, is in fact a 2-sided ideal. Since $x \neq 0$ and $R$ is simple we have $Rx = R$, whence there is $r \in R$ with $rx = 1$. As $x$ is central $xr = 1$ also and $x$ is invertible. □

1.2. **Modules and Schur's lemma.** All $R$-modules will be left $R$-modules unless stated otherwise (i.e. by an *$R$-module* we mean an abelian group $M$ equipped with a ring homomorphism $R \to \mathrm{End}_{\mathbb{Z}}(M)$, by contrast a right $R$-module being the data of a ring homomorphism $R \to \mathrm{End}_{\mathbb{Z}}(M)^{\mathrm{opp}}$).[1] We say an $R$-module is *simple* if it has no non-trivial $R$-submodules (we caution that a simple ring $R$ need not be simple as a left-module over itself, due to the difference between left and 2-sided ideals; in this respect, maybe *irreducible* would be a better term for what we call simple modules). For a module $M$, we denote by $\mathrm{End}_R(M)$ the set of all $R$-module homomorphisms $M \to M$, which is a ring via addition and composition of homomorphisms. The same footnote as for $\mathrm{End}_{\mathbb{Z}}(M)$ continues to apply.

We will frequently use the following basic lemma which gives a source of division rings.

**Lemma 1.5** (Schur's lemma)**.** *Let $R$ be a ring and $L$ a simple $R$-module. Then $\mathrm{End}_R(L)$ is a division ring.*

*Proof.* Let $0 \neq f \in \mathrm{End}_R(L)$. Then $\ker(f)$ is a proper $R$-submodule of $L$. As $L$ is simple and $f \neq 0$, we must have $\ker(f) = 0$. In particular, $f$ is injective. Similarly, $\mathrm{im}(f) = L$ whence $f$ is invertible. □

**Example 1.6.** Let $G$ be a finite group and $V$ an irreducible representation of $G$ over a field $k$. Then (taking $R = k[G]$), $\mathrm{End}_G(V)$ is a division ring.

1.3. **Algebras over a field.** If $k$ is a field, by a *$k$-algebra* we mean a (possibly noncommutative) ring $R$ equipped with a (necessarily injective) homomorphism $k \to Z(R)$. Note that if $A$ is a $k$-algebra then this makes $A^{\mathrm{opp}}$ into a $k$-algebra also. We call this the *opposite algebra*. In this course we will primarily be interested in the collection of algebras over a fixed base field $k$. With this $k$ understood, we say that a $k$-algebra $R$ is *central* if $Z(R) = k$. If a $k$-algebra is a division ring we refer to it as a *division algebra*.

1.4. **Matrix rings.** For a ring $R$ and $n \geq 1$, denote by $M_n(R)$ the ring of $n \times n$ matrices with coefficients in $R$ (with the usual addition and matrix multiplication). Note that Example 1.2 generalises to give $M_n(R^{\mathrm{opp}}) \cong M_n(R)^{\mathrm{opp}}$.

*Caution* 1.7. For $n \geq 1$, $R^n$ is an $R$-module via the usual left 'scalar' multiplication. For $R = k$ a field we're used to identifying $\mathrm{End}_k(k^n)$ with $M_n(k)$. For general rings this isn't quite true, as the following lemma shows.

**Lemma 1.8.** *For any $n \geq 1$ we have*

$$\mathrm{End}_R(R^n) \cong M_n(R^{\mathrm{opp}}).$$

*(Explicitly, thinking of elements of $R^n$ as row vectors the action of a matrix $M$ on $R^n$ is right multiplication by the transpose of $M$.)*

*Proof.* It follows formally that for any $R$-module $L$, $\mathrm{End}_R(L^n) \cong M_n(\mathrm{End}_R(L))$. Thus it suffices to prove the case $n = 1$. Consider the map $R^{\mathrm{opp}} \to \mathrm{End}_R(R)$ given by

$$d \mapsto (\text{right multiplication by } d).$$

(We need to multiply by elements of $R$ on the right in order to commute with the module structure given by left multiplication.) This is a homomorphism and its inverse is the map $\mathrm{End}_R(R) \to R^{\mathrm{opp}}$ given by $\phi \mapsto \phi(1)$. □

[1] For us endomorphisms always act on the left, so that for $\phi, \psi \in \mathrm{End}_{\mathbb{Z}}(M)$, the product $\phi \cdot \psi$ sends $m \in M$ to $\phi(\psi(m))$. We caution that the literature is not universally in agreement on this.

**Proposition 1.9.** *Let $R$ be a ring. Then for any $n \geq 1$ we have:*

(1) *$Z(M_n(R)) = Z(R)$ (here the centre of $R$ is embedded in $M_n(R)$ as scalar matrices).*

(2) *The 2-sided ideals of $M_n(R)$ are precisely the ideals of the form $M_n(I)$ for $I$ a 2-sided ideal of $R$.*

In the course of the proof we'll use the *elementary matrices* $E^{(i,j)}$ which have all entries 0 except for a 1 in the $(i,j)$th slot. Note that these generate $M_n(R)$ as an $R$-module.

*Proof.* (1). Take $M \in M_n(R)$ and let $r \in R$. Then $rE^{(i,j)}M$ is the matrix whose $i$th row is the $j$th row of $M$, multiplied by $r$ on the left, and zeros elsewhere. On the other hand, $MrE^{(i,j)}$ is the matrix whose $j$th column is the $i$th column of $M$, multiplied by $r$ on the right, and zeros elsewhere. Now suppose that $M$ is in the centre of $M_n(R)$, so that the matrices $rE^{(i,j)}M$ and $MrE^{(i,j)}$ must agree for all $i, j$ and $r$. Taking $i = j$ and $r = 1$ we see that $M$ must be diagonal, and then taking $i = 1$, $r = 1$ and varying $j$ we see that $M$ is scalar. Finally, taking $i = j = 1$ and varying $r$ we see that this scalar must be in the centre of $R$. Thus $Z(M_n(D)) = Z(R)$ as desired.

(2). One sees easily from the definition of matrix (addition and) multiplication that if $I$ is a 2-sided ideal of $R$ then $M_n(I)$ (i.e. those matrices in $M_n(R)$ each of whose coefficients is in $I$) is a 2-sided ideal of $M_n(R)$. Conversely, let $J$ be a 2-sided ideal of $M_n(R)$ and define the subset $I$ of $R$ as

$$I = \{(m_{1,1}) \mid M = (m_{i,j})_{1 \leq i,j \leq n} \in J\}.$$

That is, $I$ is the subset of $R$ consisting of the $(1,1)$-entries of the elements of $J$. It's clear (e.g. since $J$ is closed under addition, and multiplication by scalar matrices both on the right and the left) that $I$ is a 2-sided ideal of $R$. We'll show that $J = M_n(I)$. Indeed, let $M = (m_{i,j}) \in J$ and fix $1 \leq i, j \leq n$. Then as $J$ is a 2-sided ideal of $M_n(R)$,

$$m_{i,j}E^{(1,1)} = E^{(1,i)}ME^{(j,1)} \in J$$

whence $m_{i,j} \in I$. Since $M$, $i$ and $j$ were arbitrary we deduce in particular that $J \subseteq M_n(I)$. For the reverse inclusion, since $J$ is closed under addition it suffices to show that if $r \in I$ and $1 \leq i, j \leq n$ then the matrix $rE_{i,j}$ consisting of $r$ in the $(i,j)$th-slot and 0s elsewhere is in $J$. Now since $r \in I$ we can find $M \in J$ whose $(1,1)$-entry is $r$. But then

$$rE^{(i,j)} = E^{(i,1)}ME^{(1,j)} \in J$$

as desired. □

## 2. Central simple algebras: Definition and examples

Fix a field $k$. The following definition is fundamental to the course.

**Definition 2.1.** A *central simple algebra* over $k$ (CSA/$k$) is a finite dimensional (as a $k$-vector space) $k$-algebra $A$ which is central, and simple as a ring. If in addition $A$ is a division algebra we call it a *central division algebra*.

Note that $k$ itself is a central division algebra over $k$.

*Remark* 2.2. If $A$ is any finite dimensional, simple $k$-algebra then $Z(A)$ is a field by Remark 2.2. In particular, this shows that any finite dimensional simple $k$-algebra is a central simple algebra over its centre. Thus the results of this course will apply to these objects also.

*Remark* 2.3. If $A$ is a central simple algebra over $k$, so is $A^{\mathrm{opp}}$ (and conversely).

2.1. **Matrix algebras.** The first examples of central simple algebras are the matrix algebras $M_n(k)$ for $n \geq 1$, as the following 'new from old' proposition shows.

**Proposition 2.4.** *Let $A$ be a central simple algebra over $k$. Then for any $n \geq 1$, the matrix ring $M_n(A)$ is a central simple algebra over $k$. (Here $M_n(A)$ is an algebra over $k$ by embedding $k$ diagonally.)*

*Proof.* Since $A$ is simple and central, the same is true of $M_n(A)$ by Proposition 1.9. Moreover, since $A$ is finite dimensional over $k$, and $M_n(A)$ is finitely generated over $A$ (by the elementary matrices) it follows that $M_n(A)$ is finite dimensional over $k$. □

2.2. **Quaternion algebras.** We will see in the next section that every central simple algebra is isomorphic to $M_n(D)$ for some central division algebra $D$. Thus we want to focus on finding examples of central division algebras. The first instances of these are *quaternion algebras*.

2.2.1. *Hamilton's quaternions.*

**Definition 2.5.** Let $\mathbb{H}$ be the 4-dimensional $\mathbb{R}$-vector space spanned by symbols $1, i, j, ij$, with multiplication determined by $i^2 = j^2 = -1$, $ij = -ji$.

**Lemma 2.6.** *$\mathbb{H}$ is a central division algebra over $\mathbb{R}$.*

*Proof.* To see that $\mathbb{H}$ is central, let $x \in Z(\mathbb{H})$ and write $x = a + bi + cj + dij$ for $a, b, c, d \in \mathbb{R}$. Then

$$xi = ai - b - ck + dj$$

whilst

$$ix = ai - b + ck - dj$$

whence $c = d = 0$. Similarly, comparing $xj$ with $jx$ we see that $b = 0$. Thus $x \in \mathbb{R}$ as desired.

To see that $\mathbb{H}$ is a division ring, for a quaternion $x = a + bi + cj + dij$ define its *conjugate* $\bar{x} = a - bi - cj - dij$. Then we define the *norm* of $x$ to be the real number

$$N(x) = x\bar{x} = \bar{x}x = a^2 + b^2 + c^2 + d^2$$

Now if $x \neq 0$ we see that $0 \neq N(x) \in \mathbb{R}$ and that $\bar{x}/N(x)$ is an inverse for $x$. □

2.2.2. *General quaternion algebras.* Now let $k$ be any field of characteristic not 2 (the following can be adapted to fields of characteristic 2 but we will not treat that here, see [GS06, Remark 1.18]).

**Definition 2.7.** For $a, b \in k^\times$, define the *generalised quaternion algebra* $(a, b)$ to be the 4-dimensional $k$-vector space with basis $1, i, j, ij$ and multiplication determined by $i^2 = a, j^2 = b, ij = -ji$ (so that $(ij)^2 = -ab$). The same argument as for Hamilton's quaternions shows that the centre of $(a, b)$ is $k$. Given $x = \alpha + \beta i + \gamma j + \delta ij$ we define its *conjugate*

$$\bar{x} = \alpha - \beta i - \gamma j - \delta ij$$

and *norm*

$$N(x) = x\bar{x} = \bar{x}x = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2.$$

One readily computes that $N : (a, b) \to k$ is multiplicative.

**Lemma 2.8.** *We have*

1. *Up to isomorphism the quaternion algebra $(a, b)$ depends only on the classes of $a$ and $b$ in $k^\times/k^{\times 2}$.*
2. *$(a, b) \cong (b, a)$.*

(3) $(1, b) \cong M_2(k)$.

*Proof.* (1). For $\alpha, \beta \in k^\times$, the change of variable $i \mapsto \alpha i$ and $j \mapsto \beta j$ gives an isomorphism $(a, b) \cong (a\alpha^2, b\beta^2)$. (2). The map $i \mapsto j$ and $j \mapsto i$ gives the desired isomorphism. (3). The matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ J = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \ IJ = \begin{pmatrix} 0 & b \\ -1 & 0 \end{pmatrix}$$

generate $M_2(k)$ as a $k$-vector space and satisfy $I^2 = 1, J^2 = b$ and $IJ = -JI$. □

**Corollary 2.9.** *There are pricisely two quaternion algebras over $\mathbb{R}$ up to isomorphism, $\mathbb{H}$ and $M_2(\mathbb{R})$.*

*Proof.* We have $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$. Now note that $\mathbb{H} = (-1, -1)$ and that by parts (2) and (3) above, $(1, 1)$ and $(1, -1) = (-1, 1)$ are isomorphic to $M_2(\mathbb{R})$. □

**Definition 2.10.** We say a quaternion algebra over $k$ is *split* if it is isomorphic to $M_2(k)$.

The following is a generalisation of the argument used to show that Hamilton's quaternions form a division algebra.

**Proposition 2.11.** *Let $A = (a, b)$ be a quaterion algebra over $k$. Then the following are equivalent.*

(1) *$A$ is a split quaternion algebra,*
(2) *$A$ is not a division algebra,*
(3) *The norm map $N : (a, b) \to k$ has a non-trivial zero,*
(4) *The element $b \in k^\times$ is a norm from $k(\sqrt{a})/k$.*

*Proof.* (1) $\Rightarrow$ (2) is clear: there are plenty of $2 \times 2$ matrices which are non-zero but not invertible. (2) $\Rightarrow$ (3): If $N$ has no non-trivial zero then for each $x \in A$ with $x \neq 0$ we have $x^{-1} = \bar{x}/N(x)$, so that $A$ is a division algebra, contradiction. (3) $\Rightarrow$ (4): It suffices to assume that $a$ is not a square in $k$, for otherwise $k(\sqrt{a}) = k$ and all elements of $k$ are norms. Pick $x \in A$ with $x \neq 0$ yet $N(x) = 0$, say

$$x = \alpha + \beta i + \gamma j + \delta ij$$

for $\alpha, \beta, \gamma, \delta$ not all zero, so that (see above)

$$0 = N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2. \tag{2.12}$$

Rewriting (2.12) gives

$$\alpha^2 - a\beta^2 = b(\gamma^2 - a\delta^2)$$

and the right hand side cannot be zero else the assumption that $x$ is nonzero would force $a$ to be a square in $k$, which we have assumed to not be the case. But we now have

$$b = N_{k(\sqrt{a})/k}\left(\frac{\alpha + \beta\sqrt{a}}{\gamma + \delta\sqrt{a}}\right)$$

as desired. (4) $\Rightarrow$ (1): Again we may assume that $a$ is not a square in $k$ else we are done by Lemma 2.8. Now if $b$ is a norm so is $b^{-1}$ so pick $\gamma$ and $\delta$ in $k$ so that $b^{-1} = \gamma^2 - a\delta^2$. Define $u = \gamma j + \delta ij$ so that

$$u^2 = -N(u) = b(\gamma^2 - a\delta^2) = 1.$$

Now one computes $ui = -iu$. Now the elements $1, u, i, ui$ are linearly independent. Indeed, $ui = -\delta aj - \gamma ij$ and we have

$$\det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \gamma & 0 & -\delta a \\ 0 & \delta & 0 & -\gamma \end{pmatrix} = \gamma^2 - \delta^2 a = b^{-1} \neq 0.$$

Thus $A$ is the 4-dimensional $k$-vector space spanned by $1, u, i, ui$ subject to $u^2 = 1, i^2 = a$ and $ui = -iu$. That is, $A$ is isomorphic to the quaternion algebra $(1, a)$ which we have already seen is split (Lemma 2.8 (3)). □

*Remark* 2.13. Let $D$ be a quaternion division algebra. The map $x \mapsto \bar{x}$ on $D$ is $k$-linear and satisfies $\bar{xy} = \bar{y}\bar{x}$ and $\bar{\bar{x}} = x$ (this is known as an *involution* in ring theory; note that this gives an isomorphism of $k$-algebras between $D$ and $D^{\mathrm{opp}}$). In particular, its restriction to any subfield of $D$ is a $k$-algebra automorphism (if $x = \alpha + \beta i + \gamma j + \delta ij$ then $\bar{x} = 2\alpha - x$ so that the involution necessarily preserves the subfield). In particular, we see that its restriction to each quadratic subfield $K/k$ is the unique non-trivial element of the Galois group of this field extension. It follows that the involution, and hence the quaternion norm, is intrinsic to $D$ and does not depend on its presentation as $(a, b)$ for some $a, b \in k$.

We end this subsection by showing that quaternion algebras exhaust all four dimensional central division algebras. We begin with the following basic lemma which will be used frequently throught.

**Lemma 2.14.** *Let $D$ be a central division algebra over $k$ and $x \in D$. Then the $k$-subalgebra of $D$ generated by $x$, denoted $k(x)$, is a finite field extension of $k$.*

*Proof.* The ring $k(x)$ is commutative, and as a subring of a division ring it's an integral domain. Moreover, since $D$ is finite dimensional over $k$, so is $k(x)$. But any integral domain finite over a field is itself a field. □

**Theorem 2.15.** *Let $D$ be a 4-dimensional central division algebra over $k$. Then $D$ is a quaternion algebra. Moreover, if $D$ contains a subfield $k(\sqrt{a})/k$ for some $a \in k^\times \setminus k^{\times 2}$ then there is $b \in k^\times$ such that $D \cong (a, b)$.*

*Proof.* Let $x \in D \setminus k$. Then $K = k(x)$ is a subfield of $D$, $D$ is a $K$-vector space, and by the tower law we have $4 = [D : k] = [D : K][K : k]$. Since $D$ is not commutative we cannot have $K = D$, whence $[K : k] = 2$. Since $\mathrm{char}(k) \neq 2$ we may write $K = k(\sqrt{a})$ for some $a \in k^\times \setminus k^{\times 2}$. To prove the lemma it thus suffices to argue that $D = (a, b)$ for some $b \in k^\times$. Now by assumption $D$ contains an element $i$ with $i^2 = a$. Consider the $k$-linear endomorphism of $D$ given by $x \mapsto ixi^{-1}$. This has exact order 2 (since $i$ is not in $k = Z(D)$). In particular it has an eigenvector with eigenvalue $-1$. That is, there is an element $j$ of $D$ with $ij = -ji$. Moreover, the $k$-subalgebra of $D$ generated by $i$ and $j$ is a $k(\sqrt{a})$-vector space of dimension at least 2 and as such is equal to $D$. Now $ij^2i^{-1} = (iji^{-1})^2 = j^2$ so that $j^2$ commutes with $i$, and also trivially commutes with $j$. Thus $j^2 \in Z(D) = k$, say $j^2 = b$. It now follows that $1, i, j$ and $ij$ are $k$-linearly independent (else the subalgebra generated by $i$ and $j$ would not have large enough $k$-dimension) whence $D \cong (a, b)$. □

## 3. Modules over central simple algebras and Wedderburn's theorem

The aim of this section is to prove the following.

**Theorem 3.1** (Wedderburn's theorem)**.** *Let $A$ be a CSA/$k$. Then there is an integer $n \geq 1$ and a central division algebra $D$ such that $A \cong M_n(D)$. Moreover, $n$ is unique and $D$ is unique up to isomorphism (of $k$-algebras).*

To motivate the proof of this theorem, which is somewhat technical, we are going to first understand how to recover $n$ and $D$ from $M_n(D)$ 'ring theoretically'. Along the way, we'll study finitely generated modules over $M_n(D)$, which by Wedderburn's theorem will amount to studying finitely generated modules over central simple algebras in general.

Note that there is one obvious $M_n(D)$-module, namely $V = D^n$ thought of as column vectors of length $n$, along with the usual matrix multiplication. Similarly, $M_n(D)$ has some obvious left ideals, namely the ideals $I_i$ consisting of matrices which are 0 outside the $i$-th column. Each such is isomorphic to $V$.

**Lemma 3.2.** *The $M_n(D)$-module $V$ is simple. In particular, each $I_i$ is a minimal left ideal of $M_n(D)$.*

*Proof.* Pick $0 \neq x \in V$. It suffices to prove that $M_n(D)x = V$. Pick $i$ such that the $i$th-coordinate of $x$ is non-zero, say $x_i = d$. Then $d^{-1}E^{(1,i)}x = (1, 0, ..., 0)$ is in $M_n(D)x$. Thus for any $d_1, ..., d_n \in D$, we have

$$\begin{pmatrix} d_1 & 0 & & 0 \\ d_2 & 0 & & 0 \\ \vdots & \vdots & \cdots & 0 \\ d_n & 0 & & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}$$

is in $M_n(D)x$ and we are done. □

*Remark* 3.3. One can show more generally (with essentially the same argument) that for any ring $R$ and $n \geq 1$, the $M_n(R)$-submodules of $R^n$ are precisely those of the form $I^n$ for $I$ a left ideal of $R$. Thus it's the simplicity of $D$ as a left module over itself which drives the result. In particular, one sees that $R^n$ is a simple $M_n(R)$-module if and only if every non-zero element of $R$ is left-invertible.

**Proposition 3.4.** *Let $D$ be a central division algebra and $n \geq 1$. Then*

1. *the ring $M_n(D)$ decomposes as a (finite) direct sum of simple $M_n(D)$-submodules, each of which is isomorphic to $V$,*
2. *every simple $M_n(D)$-module is isomorphic to $V$,*
3. *any finitely generated $M_n(D)$-module is isomorphic to $V^r$ for some $r \geq 1$.*

*Proof.* (1). This follows from Lemma 3.2 since

$$M_n(D) = \bigoplus_{i=1}^{n} I_i.$$

(2). Let $L$ be any simple $M_n(D)$-module and pick $0 \neq x \in L$. Consider the map $\phi : M_n(D) \to L$ given by $M \mapsto Mx$ and for each $i$, let $\phi_i$ be the restriction of $\phi$ to $I_i$. Each $\phi_i$ is a homomorphism between two simple $M_n(D)$-modules and is hence either the zero map or an isomorphism. Since $M_n(D)$ is a direct sum of the $I_i$, and $\phi$ is not the zero map since its image contains $x$, at least one of the $\phi_i$ must be an isomorphism and the result follows.

(3). Let $L$ be one such. Since $L$ is finitely generated we can find a surjection $\phi : M_n(D)^r \to L$ for some $r$. But then as $M_n(D)$ is a direct sum of finitely many modules isomorphic to $V$ we

may view this as a surjection

$$\bigoplus_{i=1}^{r'} V \to L$$

for some $r'$. Now each summand is simple, so the restriction of $\phi$ to each summand is either the zero map, or injective. Removing the summands for which $\phi$ restricts to 0, we may assume that $\phi$ is injective when restricted to each summand. In particular, $L$ is generated by its simple submodules. Let $N$ be a submodule of $L$ which is maximal with respect to being a direct sum of simple modules. Such an $N$ exists since $L$ is finite dimensional as a $k$-vector space (as $M_n(D)$ is finite dimensional over $k$ and $L$ is finitely generated over $M_n(D)$). Suppose for contradiction that $N \neq L$. Then as $L$ is generated by simple submodules there is some simple submodule $N'$ not contained entirely within $N$. But then $N'$ is simple so $N \cap N' = 0$ whence $N \oplus N'$ is a larger submodule which is isomorphic to a direct sum of simple submodules, contradiction. Thus $N = L$ and we are done. □

*Remark* 3.5. Note that the number of copies of $V$ appearing in (3) is uniquely determined by counting dimenisons as a $k$-vector space. Taking $n = 1$ in the above shows that any finitely generated module over a central division algebra $D$ is isomorphic to $D^r$ for some $r$, and moreover this $r$ is uniquely determined. This is a generalisation of the fact that each finite dimensional $k$-vector space is isomorphic to $k^n$, and is classified by its dimension.

We now move towards Wedderburn's theorem. Given any central simple algebra $A$ over $k$, and $L$ a simple $A$-module, Schur's lemma says that $\mathrm{End}_A(L)$ is a division ring. In fact, it's clear that it's a finite dimensional division algebra over $k$. For $A = M_n(D)$ we can determine exactly what it is.

**Lemma 3.6.** *Let $D$ be a central division algebra and $n \geq 1$. Then (as $k$-algebras) we have*

$$\mathrm{End}_{M_n(D)}(V) \cong D^{\mathrm{opp}}.$$

*(The explicit map from right to left is given by multiplication on the right.)*

*Proof.* Let $x \in V$ be arbitrary and write $M_x$ for the matrix whose first column is $x$ and whose other entries are 0. Further write $e_1 = (1, 0, ..., 0) \in D^n$. Note that $x = M_x e_1$. Thus for any $\phi \in \mathrm{End}_{M_n(D)}(V)$ we have

$$\phi(x) = \phi(M_x e_1) = M_x \phi(e_1) = xd$$

where $d \in D$ is the first coordinate of $\phi(e_1)$. Thus $\phi$ is multiplication on the right by $d$. In particular, the map sending $\phi \in \mathrm{End}_{M_n(D)}(V)$ to the first coordinate of $\phi(e_1)$ is an inverse to the natural map $D^{\mathrm{opp}} \to \mathrm{End}_{M_n(D)}(V)$ in the statement of the lemma. □

*Remark* 3.7. As promised this allows us to reconstruct $D$ and $n$ from $M_n(D)$ intrinsically. Indeed, we've seen that each $I_i$ is a simple $M_n(D)$-module, and hence a minimal (non-zero) left ideal. Moreover, any minimal left ideal is necessarily a simple $M_n(D)$-module and as such isomorphic to $V$. Thus we may pick any minimal (non-zero) left ideal $L$ of $M_n(D)$, and recover $D^{\mathrm{opp}}$ (and hence $D$) as $\mathrm{End}_{M_n(D)}(L)$ by Lemma 3.6. Once $D$ has been determined, $n$ may be recovered e.g. from the $k$-dimension of $M_n(D)$. Note also that by Lemma 1.8 we have (as $k$-algebras)

$$M_n(D) \cong \mathrm{End}_D^{\mathrm{opp}}(V).$$

*Proof of Wedderburn's theorem.* We first show uniqueness (c.f. Remark 3.7). Let $A$ be a CSA/$k$. If $A \cong M_n(D)$ for some $n$ and a central divison algebra $D$, then we may recover $D$ as $\mathrm{End}_A(L)^{\mathrm{opp}}$ where $L$ is any minimal left ideal of $A$. This gives uniqueness of $D$, and counting dimensions as a $k$-vector space then shows uniqueness of $n$.

Now motivated by the discussion above, let $A$ be arbitrary and $0 \neq L$ be a minimal left ideal of $A$ (these exist since each left ideal is a $k$-vector subspace of the finite dimensional $k$-vector space $A$). By Schur's lemma $D = \mathrm{End}_A(L)$ is a finite dimensional division algebra over $k$. We'll show that $A \cong M_n(D^{\mathrm{opp}})$ for some $n$.

We claim that the map $\lambda : A \to \mathrm{End}_D(L)$ given by $a \mapsto (l \mapsto al)$ is an isomorphism of $k$-algebras. (Secretly, $A = M_n(D^{\mathrm{opp}})$ and then $A \cong \mathrm{End}_D(L)$ as in Remark 3.7.) Note that left multiplication by elements of $A$ does indeed commute with the action of $D = \mathrm{End}_A(L)$ on $L$.

To prove the claim, note that the kernel of $\lambda$ is a 2-sided ideal of $A$. Thus $\lambda$ is injective. Morever, $\lambda(L)$ is a left ideal of $\mathrm{End}_D(L)$. To see this, take $\phi \in \mathrm{End}_D(L)$ and $l \in L$. Then $\phi\lambda(l)$ is the map $x \mapsto \phi(lx)$. Now for each $x \in L$, right multiplication by $x$ is a $A$-endomorphism of $L$, or in other words an element of $D$. Since $\phi$ commutes with all elements of $D$, $(\phi\lambda(l))(x) = \phi(l)x$ for all $x \in L$. Thus $\phi\lambda(l) = \lambda(\phi(l)) \in \lambda(L)$. Next, since $L$ is a left ideal of $A$, the right ideal $LA$ generated by $L$ is a 2-sided ideal and hence equal to $A$. In particular we may write

$$1 = \sum_i l_i a_i$$

for some $l_i \in L$ and $a_i \in A$. Then for any $\phi \in \mathrm{End}_D(L)$,

$$\phi = \phi \circ \lambda(1) = \sum_i \phi \circ \lambda(l_i) \circ \lambda(a_i).$$

Since $\lambda(L)$ is a left ideal of $\mathrm{End}_D(L)$, $\phi \circ \lambda(l_i)$ is in $\lambda(L)$ for each $i$, whence the whole sum is in the image of $\lambda$. Thus $\phi \in \mathrm{im}(\lambda)$ and $\lambda$ is an isomorphism as claimed.

Now since $D$ is a division algebra, as a $D$-module, $L \cong D^n$ for some $n$. But then $A \cong \mathrm{End}_D(D^n) \cong M_n(D^{\mathrm{opp}})$ by Remark 3.7. Finally, since $A$ is a central simple algebra, so must $M_n(D^{\mathrm{opp}})$ be, from which it's clear that $D^{\mathrm{opp}}$ is central and has finite $k$ dimension. □

**Corollary 3.8.** *Let $A$ be a finite dimensional simple $k$-algebra. Then $A$ is a direct sum of simple submodules, all of which are isomorphic (to $L$ say). Moreover, any finitely generated $A$-module is isomorphic to $L^r$ for some $r$. As such, finitely generated $A$-modules are classified up to isomorphism by their dimension as a $k$-vector space.*

*Proof.* This follows immediately upon noting that $A$ is a central simple algebra over its centre, cf. Remark 2.2. □

## 3.1. **Central simple algebras over an algebraically closed field.**

**Theorem 3.9.** *Let $k$ be an algebraically closed field and $A/k$ a central simple algebra. Then $A \cong M_n(k)$ for some $n \geq 1$.*

*Proof.* By Wedderburn's theorem, $A \cong M_n(D)$ for some $n \geq 1$ and central division algebra $D$. Thus it suffices to prove that the only central division algebra over $k$ is $k$ itself. Let $D$ be one such and $0 \neq x \in D$. Then the subalgebra $k(x) \subseteq D$ generated by $x$ is a finite field extension of $k$. Since $k$ is algebraically closed this is just $k$ itself, whence $x \in k$ and we are done. □

## 4. Splitting fields for central simple algebras

4.1. **Tensor products of central simple algebras.** For $A$ and $B$ (possibly infinite dimensional) $k$-algebras, the tensor product $A \otimes_k B$ is a ring, with multiplication induced by

$$(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'$$

and it's $k$-vector space structure makes it into a $k$-algebra via $\lambda \mapsto \lambda(1 \otimes 1)$. Note that it contains both $A$ and $B$ as $k$-subalgebras, via $a \mapsto a \otimes 1$ and $b \mapsto 1 \otimes b$ respectively.

**Lemma 4.1.** *Let $A$ and $B$ be (possibly infinite dimensional) $k$-algebras. Then*

1. *the centre of $A \otimes_k B$ is $Z(A) \otimes_k Z(B)$ (in particular, if $A$ is central then $Z(A \otimes_k B) = Z(B)$).*
2. *if $A$ is a CSA/$k$ then the 2-sided ideals of the $k$-algebra $A \otimes_k B$ are precisely those of the form $A \otimes_k J$ for $J$ a 2-sided ideal of $B$.*

*Proof.* (1). Clearly $Z(A) \otimes_k Z(B) \subseteq Z(A \otimes_k B)$. For the converse pick a basis $\{x_i\}_{i \in I}$ for $B$ as a $k$-vector space, so that any $w \in A \otimes_k B$ is uniquely of the form

$$w = \sum_{i \in I} a_i \otimes x_i$$

for some $a_i \in A$. Suppose that such a $w$ is in the centre of $A \otimes_k B$. Then for all $a \in A$ we have

$$0 = (a \otimes 1)w - w(a \otimes 1) = \sum_{i \in I} (aa_i - a_i a) \otimes x_i.$$

Thus $a_i \in Z(A)$ for all $i$. That is, $w \in Z(A) \otimes_k B$. Now pick a basis $\{y_j\}_{j \in J}$ for $Z(A)$ as a $k$-vector space, so that we may write $w$ uniquely as

$$w = \sum_{j \in J} y_j \otimes b_j$$

for some $b_j \in B$. Since $w$ commutes with $1 \otimes b$ for each $b \in B$, the same argument as above shows that each $b_j$ is in $Z(B)$. But then $w \in Z(A) \otimes_k Z(B)$ as desired.

(2). First note that for each 2-sided idea of $B$, $A \otimes_k J$ is a 2-sided ideal of $B$.

For the converse, let $\mathcal{J}$ be a 2-sided ideal of $A \otimes_k B$. Then $J = \mathcal{J} \cap B$ is easily seen to be a 2-sided ideal of $B$, and we clearly have $A \otimes_k J \subseteq \mathcal{J}$. To conclude, we will show that in fact $A \otimes_k J = \mathcal{J}$. To do this, fix a $k$-basis $\{x_i\}_{i \in I'}$ for $J$ and extend to a $k$-basis $\{x_i\}_{i \in I}$ for $B$. Set $I'' = I \setminus I'$. Then

$$A \otimes_k J = \bigoplus_{i \in I'} A \otimes x_i \qquad \text{and} \qquad A \otimes_k B = \bigoplus_{i \in I} A \otimes x_i.$$

Suppose for contradiction that $\mathcal{J} \neq A \otimes_k J$ and pick $w \in \mathcal{J} \setminus A \otimes_k J$. Subtracting elements of $A \otimes_k J$ if necessary we may assume that

$$w = \sum_{i \in I''} a_i \otimes x_i$$

for some $a_i \in A$. Now define $\emptyset \neq I_w$ to be the (finite) set of indices $i$ such that $a_i \neq 0$. We may suppose that $|I_w|$ is minimal amongst all such $w$. Fix $i_0 \in I_w$, so that $a_{i_0} \neq 0$, and let

$$S = \{a'_{i_0} \mid \exists\ w' \in \mathcal{J} \text{ with } w' = a'_{i_0} \otimes x_{i_0} + \sum_{i \in I_w \setminus \{i_0\}} a'_i \otimes x_i \text{ for some } a'_i\}.$$

Then $S$ is a 2-sided ideal of $A$ and $S \neq 0$ since $a_{i_0} \in S$. Thus $S = A$ since $A$ is simple. In particular, $1 \in S$ whence we can find $w' \in \mathcal{J}$ of the form

$$w' = 1 \otimes x_{i_0} + \sum_{i \in I_w \setminus \{i_0\}} a'_i \otimes x_i.$$

Now for any $a \in A$,

$$z = aw' - w'a = \sum_{i \in I_w \setminus \{i_0\}} (aa'_i - a'_i a) \otimes x_i \in \mathcal{J}.$$

By minimality of $|I_w|$ we must have $z = 0$, whence $a'_i \in Z(A) = k$ for all $i \in I_w \setminus \{i_0\}$. Hence

$$w' \in \mathcal{J} \cap (k \otimes_k B) = \mathcal{J} \cap B = J.$$

But this is a contradiction since $w' \neq 0$ and $I_w \subseteq I''$. Hence $\mathcal{J} = A \otimes_k J$ as desired. □

*Remark* 4.2. It's tempting to try to prove part (2) by showing the more general statement that for any $k$-algebras $A$ and $B$, the 2-sided ideals of $A \otimes_k B$ are all of the form $I \otimes_k J$ for $I$ and $J$ 2-sided ideals of $A$ and $B$ respectively. Whilst everything of this form *is* a 2-sided ideal of $A \otimes_k B$, the converse in fact fails. For a counterexample one can consider the ideals of the 2-variable polynomial ring $k[x, y] \cong k[x] \otimes_k k[y]$.

This result has several fundamental corollaries.

**Corollary 4.3.** *Let $A_1, A_2$ be CSAs/$k$. Then $A_1 \otimes_k A_2$ is a central simple algebra over $k$ also.*

*Proof.* Immediate from Lemma 4.1. □

Note that if $A$ is a $k$-algebra and $K/k$ is a field extension then $A \otimes_k K$ is a $K$-algebra via $\lambda \mapsto 1 \otimes \lambda$.

**Theorem 4.4.** *Let $A$ be a $k$-algebra and $K/k$ a (possibly infinite) field extension. Then $A$ is a CSA/$k$ if and only if $A \otimes_k K$ is a CSA/$K$.*

*Proof.* First suppose $A$ is a CSA/$k$. Then by Lemma 4.1 (1), $A \otimes_k K$ is simple, since $K$ is. Moreover, by Lemma 4.1 (2), since $K$ is commutative, the centre of $A \otimes_k K$ is equal to $K$. Finally, $A$ is finite dimensional as a $k$-vector space, hence $A \otimes_k K$ is finite dimensional as a $K$-vector space. Thus $A \otimes_k K$ is a central simple algebra over $K$.

Conversely, suppose that $A \otimes_k K$ is a central simple algebra over $K$. Note that $A$ is necessarily finite dimensional over $k$ else any infinite $k$-linearly independent subset of $A$ would give an infinite $K$-linearly independent subset of $A \otimes_k K$. Next, if $J$ is a non-trivial 2-sided ideal of $A$ then $J \otimes_k K$ is a 2-sided ideal of $A \otimes_k K$ and is non-trivial by counting dimensions over $K$. Similarly, if $Z(A)$ has $k$-dimension greater than 1, then $Z(A) \otimes_k K \subseteq Z(A \otimes_k K)$ has $K$-dimension greater than 1, a contradiction. □

**Corollary 4.5.** *Let $A$ be a $k$-algebra and write $\bar{k}$ for the algebraic closure of $k$. Then $A$ is a CSA/$k$ if and only if $A \otimes_k \bar{k} \cong M_n(\bar{k})$ for some $n \geq 1$ (which may be determined by counting dimensions over $k$).*

*Proof.* Follows from Theorem 4.4 and Theorem 4.4. □

The above corollary shows the non-obvious fact that the $k$-dimension of any CSA/$k$ is a square. Indeed, for any such $A$, its $k$ dimension is the same as the $\bar{k}$-dimension of $A \otimes_k \bar{k} \cong M_n(\bar{k})$ for some $n$. But then the dimension of $A \otimes_k \bar{k}$ is $n^2$.

**Definition 4.6.** Let $A$ be a CSA/$k$. We define the *degree* of $A$ as

$$\deg A = \sqrt{\dim_k A}.$$

4.2. **Automorphisms of central simple algebras: the Skolem–Noether theorem.**

**Definition 4.7.** Let $R$ be a ring and $\alpha$ an automorphism of $R$. We call $\alpha$ *inner* if there is an invertible element $r \in R$ such that $\alpha$ is given by $x \mapsto rxr^{-1}$.

**Theorem 4.8** (Skolem–Noether theorem)**.** *Let $A/k$ be a CSA and $B$ a simple $k$-subalgebra. Then any $k$-algebra homomorphism $f : B \to A$ extends to an inner automorphism of $A$. In particular, any $k$-algebra automorphism of $A$ is inner.*

*Proof.* View $A$ as a $B \otimes_k A^{\mathrm{opp}}$-module in two different ways, the first via $(b \otimes a)x = bxa$ and the second via $(b \otimes a)x = f(b)xa$. To avoid confusion, write $A_1$ and $A_2$ for $A$ equipped with these two different module structure. Now $B \otimes_k A^{\mathrm{opp}}$ is a finite dimensional simple $k$-algebra by Lemma 4.1. In particular, since finitely generated $B \otimes_k A^{\mathrm{opp}}$-modules are classified by their dimension as a $k$-vector space (Corollary 3.8) we can fix an isomorphism $\phi : A_1 \to A_2$ of $B \otimes_k A^{\mathrm{opp}}$-modules. In particular, for all $x, a \in A$ and $b \in B$ we have

$$\phi(bxa) = f(b)\phi(x)a. \tag{4.9}$$

Setting $b = x = 1$ and noting that $f(1) = 1$ we see that $\phi$ is multiplication on the left by $d = \phi(1)$ and since $\phi$ is an isomorphism it follows that $d$ is invertible (any element of a finite dimensional $k$-algebra with a right inverse also has a left inverse). Finally, setting $a = x = 1$ in (4.9) we see that for all $b \in B$ we have

$$db = \phi(b) = f(b)d$$

so that $f(b) = dbd^{-1}$ for all $b \in B$, and we may extend $f$ to an inner automorphism of $A$ by this same formula. □

**Corollary 4.10.** *For any field $k$ we have* $\mathrm{Aut}_k(M_n(k)) \cong PGL_n(k)$.

*Proof.* Define a map $GL_n(k) \to \mathrm{Aut}_k(M_n(k))$ by sending $x \in GL_n(k)$ the the automorphism $M \mapsto xMx^{-1}$. This is surjective by the Skolem–Noether theorem and the kernel consists of the elements of $GL_n(k)$ which lie in the centre of $M_n(k)$. But this is just $K^\times$ embedded in $GL_n(k)$ as scalar matrices. Thus

$$\mathrm{Aut}_k(M_n(k)) \cong GL_n(K)/K^\times = PGL_n(k)$$

as desired. □

*Remark* 4.11. For a general central simple algebra $A/k$ the same argument gives $\mathrm{Aut}_k(A) \cong A^\times/k^\times$.

4.3. **Derivations of central simple algebras.**

**Definition 4.12.** Let $A$ be a $k$-algebra. A *$k$-derivation* of $A$ is a $k$-linear map $D : A \to A$ such that

$$D(aa') = D(a)a' + aD(a')$$

for all $a, a' \in A$. Note that this forces $D(1) = D(1 \cdot 1) = 2D(1)$, so that $D(1) = 0$. By $k$-linearity, this in turn gives

$$D(\lambda) = 0$$

for all $\lambda \in k$. A $k$-derivation $D$ is called *inner* if there is $d \in A$ with

$$D(a) = da - ad$$

for all $a \in A$. Note that this formula does indeed define a $k$-derivation of $A$ for all $d \in A$, and that this derivation is zero if and only if $d \in Z(A)$.

We can also define derivations in a slightly more general setting.

**Definition 4.13.** Let $A$ and $B$ be $k$-algebras. An $A$-$B$-bimodule is an abelian group $M$ which is both a left $A$-module and a right $B$-module, in such a way that

$$(am)b = a(mb)$$

for all $a \in A, b \in B$, and $m \in M$, and such that, for all $\lambda \in k$, we have

$$\lambda m = m\lambda$$

for all $m \in M$. This is the same data as being a left $A \otimes_k B^{\mathrm{opp}}$-module (if $M$ is a $A$-$B$-bimodule then setting $(a \otimes b) \cdot m = amb$ makes $M$ into a $A \otimes_k B^{\mathrm{opp}}$-module, and conversely).

Note in particular that if $B$ is a subalgebra of a $k$-algebra $A$, then left and right multiplication by elements of $B$ makes $A$ into a $B$-$B$-bimodule.

**Definition 4.14.** Let $A$ be a $k$-algebra and $M$ an $A$-$A$-bimodule. Then a *$k$-derivation* $D : A \to M$ is a $k$-linear map such that

$$D(aa') = D(a)a' + aD(a') \quad \text{for all } a, a' \in A.$$

**Proposition 4.15** (Skolem–Noether for derivations)**.** *Let $A$ be a CSA/$k$, $B$ a simple subalgebra of $A$, and $D : B \to A$ a $k$-derivation. Then $D$ extends to an inner derivation of $A$. In particular, all $k$-derivations of $A$ are inner.*

*Proof.* By Proposition 2.4, the matrix algebra $M_2(A)$ is a central simple algebra over $k$ also, and $B$ (embedded diagonally) is a simple subalgebra of $M_2(A)$. Define the map $f : B \to M_2(A)$ by, for $b \in B$, setting

$$f(b) = \begin{pmatrix} b & D(b) \\ 0 & b \end{pmatrix}.$$

Clearly $f$ is a $k$-linear map, and it's actually a ring homomorphisms since (it visibly sends 1 to 1 and) for all $b, b' \in B$ we have

$$f(b)f(b') = \begin{pmatrix} b & D(b) \\ 0 & b \end{pmatrix}\begin{pmatrix} b' & D(b') \\ 0 & b' \end{pmatrix} = \begin{pmatrix} bb' & bD(b') + D(b)b' \\ 0 & bb' \end{pmatrix} = \begin{pmatrix} bb' & D(bb') \\ 0 & bb' \end{pmatrix}.$$

Thus $f$ is a $k$-algebra homomorphism $B \to M_2(A)$ and by the Skolem–Noether theorem $f$ extends to an inner automorphism of $M_2(A)$. That is, there is an inveritble matrix

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

in $M_2(A)$ with $f(b)M = Mb$ for all $b \in B$. Writing this out as a matrix equation we find, for all $b \in B$,

$$\begin{cases} \alpha b = b\alpha + D(b)\gamma \\ \beta b = b\beta + D(b)\delta \\ \gamma b = b\gamma \\ \delta b = b\delta. \end{cases}$$

Now as $M$ is invertible, at least one of $\gamma$ and $\delta$ is non-zero. Suppose first $\gamma \neq 0$. The third equation says that $\gamma$ is in $Z(B)$. In particular, since $B$ is simple, $Z(B)$ is a field whence $\gamma$

is invertible in $B$ (and hence $A$). The first equation now gives (remembering that $\gamma \in Z(B)$ hence $\gamma^{-1} \in Z(B)$ also)

$$D(b) = (\alpha\gamma^{-1})b - b(\alpha\gamma^{-1})$$

for all $b \in B$, whence $D$ extends to an inner derivation of $A$ as desired. The argument when $\delta$ is non-zero instead of $\gamma$ is identical. □

4.4. **Splitting fields for central simple algebras.** We saw in Theorem 4.4 that if $A$ is a CSA/$k$, then $A \otimes_k \bar{k} \cong M_n(\bar{k})$ for some $n \geq 1$. This motivates the following definition.

**Definition 4.16.** Let $A$ be a CSA/$k$ and let $K/k$ be a field extension. We say that $K$ is a *splitting field* for $A$ if

$$A \otimes_k K \cong M_n(K)$$

for some $n \geq 1$ (necessarily equal to the degree of $A$).

*Remark* 4.17. We've seen that any CSA/$k$ is split by $\bar{k}$. Note moreover, that for any field extension $L/K$, $M_n(K) \otimes_K L \cong M_n(L)$, thus if $K$ splits a central simple algebra $A/k$, and $L/K$ is *any* field extension, then $L$ splits $A$ also.

*Remark* 4.18. Let $A/k$ be a CSA and $K/k$ a field. Then $A$ is split by $K$ if and only if $A^{\text{opp}}$ is. To see this, note that for any $n$, $M_n(K) \cong M_n(K)^{\text{opp}}$ be the map sending a matrix to its transpose. Now conclude by noting that $A^{\text{opp}} \otimes_k K \cong (A \otimes_k K)^{\text{opp}}$.

4.4.1. *Splitting fields for quaternion algebras.* Let $A = (a, b)$ be a quaternion algebra over a field $k$ ($\text{char}(k) \neq 2$ as usual for quaternion algebras) and let $K/k$ be a field extension. Then $A \otimes_k K$ is simply the quaternion algebra $(a, b)$ viewed over $K$ rather than $k$. In particular, since we've seen that $(a, b)$ is split as soon as either $a$ or $b$ is a square in $k$ we see that both $K = k(\sqrt{a})$ and $K = k(\sqrt{b})$ split $A$.

In fact, we have the following result:

**Theorem 4.19.** *Let $A$ be a quaternion algebra over $k$ and let $a \in k^\times \setminus k^{\times 2}$. Then the following are equivalent.*

1. *There exists $b \in k^\times$ such that $A$ is isomorphic to the quaternion algebra $(a, b)$,*
2. *$A$ is split by the quadratic extension $k(\sqrt{a})/k$.*
3. *$A$ contains a subfield isomorphic to $k(\sqrt{a})$.*

*Proof.* (1)⇒(2) was already noted in the discussion above. (2)⇒ (3). We may assume that $A$ is a division algebra. Indeed, if not then $A$ is isomorphic to $(1, a)$ and we are done taking the second basis vector (w.r.t. this presentation) as the generator of the field extension. Now elements of $A \otimes_k k(\sqrt{a})$ are uniquely of the form $x + \sqrt{a}y$ for $x, y \in A$. Write $N$ for the quaternion norm on $A \otimes_k k(\sqrt{a})$ (say extended from $A$ in the obvious way). Since $A$ is split by $k(\sqrt{a})$ this has a non-trivial zero of the form $x + y\sqrt{a}$. That is,

$$0 = (x + y\sqrt{a})\overline{(x + y\sqrt{a})} = N(x) + aN(y) + \sqrt{a}(x\bar{y} + y\bar{x})$$

from which we deduce that $N(x) = -aN(y)$ and $x\bar{y} = -y\bar{x}$. Let $u = x\bar{y}$. Then

$$u^2 = x\bar{y}x\bar{y} = -y\bar{x}x\bar{y} = -N(x)N(y) = aN(y)^2.$$

Since $A$ is a division algebra $N(y) \neq 0$ whence $u/N(y)$ squares to $a$ and we have found the desired square root of $a$ inside $A$. (3)⇒ (1). If $A$ is split the $A$ is isomorphic to $(a, 1)$ an we are done. So we may assume that $A$ is a division algebra so that in particular $a$ is not a square in $k$. Now Theorem 2.15 shows that $A \cong (a, b)$ for some $b \in k^\times$. □

Moreover we have:

**Proposition 4.20.** *Let $A$ be a quaternion division algebra over $k$ and $K/k$ a finite extension which splits $A$. Then $[K:k]$ is even.*

*Proof.* Say $A \cong (a,b)$ for $a,b \in K^\times$. Since $A$ is division $a \notin k^\times$ and we may assume $a \notin K^{\times 2}$ either, else $k(\sqrt{a})/k$ is a degree 2 subextension of $K/k$, whence $K/k$ is even by the tower law. Since $K$ splits $A$, $b$ is a norm from the quadratic extension $K(\sqrt{a})/K$ (Proposition 2.11), say $b = N_{K(\sqrt{a})/K}(\beta)$. We now compute $N_{K(\sqrt{a})/k}(\beta)$ in two different ways. Firstly we have

$$N_{K(\sqrt{a})/k}(\beta) = N_{K/k}\left(N_{K(\sqrt{a})/K}(\beta)\right) = N_{K/k}(b) = b^{[K:k]}.$$

On the other hand,

$$N_{K(\sqrt{a})/k}(\beta) = N_{k(\sqrt{a})/k}\left(N_{K(\sqrt{a})/k(\sqrt{a})}(\beta))\right).$$

Thus we have

$$b^{[K:k]} = N_{k(\sqrt{a})/k}(\gamma)$$

for $\gamma = N_{K(\sqrt{a})/k(\sqrt{a})}(\beta) \in k(\sqrt{a})$. If $[K:k]$ were odd, say $[K:k] = 2r+1$ for some integer $r$, then we'd have

$$b = N_{k(\sqrt{a})/k}(\gamma/b^r)$$

whence $A$ would be split by Proposition 2.11, a contradiction. Thus $[K:k]$ is even as desired. □

4.4.2. *The double centraliser theorem.* Our analysis of quaternion algebras suggests that to investigate splitting fields of central simple algebras we study subfields of division algebras. In fact, we have the following:

**Proposition 4.21.** *Let $D$ be a central division algebra over $k$, and suppose we have a field $K$ with $k \subseteq K \subseteq D$ and such that $[K:k] = \deg D$. Then $K$ splits $D$.*

*Proof.* View $D$ as a vector space over $K$ by right multiplication (this is ok since $K$ is commutative). Let $n = [D:K]$, so that as a $K$-vector space we have $D \cong K^n$. Consider the $K$-algebra homomorphism $\phi : D \otimes_k K \to \mathrm{End}_K(D) \cong M_n(K)$ given by $d \otimes x \mapsto (d' \mapsto dd'x)$. This is well defined since $K$ is commutative. Now $\ker(\phi)$ is a 2-sided ideal of the simple algebra $D \otimes_k K$. Thus $\phi$ is injective. We can now count dimensions. We have $[D:k] = [D:K][K:k]$ whilst the assumption gives $[K:k] = \deg D = \sqrt{[D:k]}$. We conclude that $[D:K] = \deg D$ also. Then

$$[D \otimes_k K : K] = [D:k] = [D:K]^2$$

whilst

$$[M_n(K) : K] = n^2 = [D:K]^2$$

and we are done. □

Suppose we have found a subfield $K$ of a division algebra (e.g. by adjoining any element of $D \setminus k$ to $k$). It's then natural to ask if we can extend it to a larger subfield, which can be done if and only if there is an element of $D \setminus K$ which commutes with every element of $K$. This motivates the study of the centraliser of a given subalgebra.

**Definition 4.22.** Let $A$ be a CSA/$k$ and $B$ a $k$-subalgebra of $A$. Define the *centraliser* of $B$ in $A$ as

$$C_A(B) = \{a \in A \mid ab = ba \text{ for all } b \in B\}.$$

For $c \in C_A(B)$ we can consider the endomorphism of $A$ given by left multiplication by $c$. Since $c$ centralises $B$, this commutes with multiplication on the left by any element of $B$, and also (trivially) commutes with multiplication on the right by elements of $A$. In fact, we have the following.

**Lemma 4.23.** *Write $E = B \otimes_k A^{\mathrm{opp}}$ and view $A$ as an $E$-module via $(b \otimes a)x = bxa$. Then the map $C_A(B) \to \mathrm{End}_E(A)$ given by $c \mapsto (x \mapsto cx)$ is an isomorphism of $k$-algebras.*

*Proof.* Taking $x = 1$ we see that the map is injective, and it's clearly a homomorphism of $k$-algebras. To show surjectivity, let $\phi \in \mathrm{End}_E(A)$. Then for all $x \in A$ we have

$$\phi(x) = \phi((1 \otimes x) \cdot 1) = \phi(1)x$$

so that $\phi$ is multiplication on the left by $c = \phi(1)$. To see that $c \in C_A(B)$, note that for all $b \in B$ we have

$$cb = \phi(b) = \phi((b \otimes 1) \cdot 1) = b\phi(1) = bc$$

as desired. □

**Theorem 4.24** (Double centraliser theorem)**.** *Let $A$ be a CSA/$k$ and $B$ a simple $k$-subalgebra of $A$. Then*

1. *the $k$-algebra $C_A(B)$ is simple,*
2. *$[A : k] = [B : k][C_A(B) : k]$,*
3. *(hence the name of the theorem) $C_A(C_A(B)) = B$.*

*Proof.* (1). Write $E = B \otimes_k A^{\mathrm{opp}}$. By Lemma 4.1 (1), $E$ is simple and hence a central simple algebra over its centre, $K$ say, cf. Remark 2.2. Now by Corollary 3.8, as an $E$-module $A \cong L^r$ for some $r$, where $L$ is any minimal left ideal of $E$. Then by Lemma 4.23 we have

$$C_A(B) \cong \mathrm{End}_E(A) \cong M_r(\mathrm{End}_E(L)).$$

By Schur's lemma, $D = \mathrm{End}_E(L)$ is a division algebra whence $C_A(B) \cong M_r(D)$ is simple.

(2). Maintaing the notation of (1), by the proof of Wedderburn's theorem $E \cong M_n(D^{\mathrm{opp}})$ for some $n$, and $L \cong (D^{\mathrm{opp}})^n$. It is now just a matter of comparing various dimensions. We have $A \cong L^r$ (as $E$-modules) so that

$$[A : k] = r[L : k] = rn[D : k]. \tag{4.25}$$

Since $E = B \otimes_k A^{\mathrm{opp}}$ we have

$$[B : k][A : k] = [E : k] = n^2[D : k]. \tag{4.26}$$

Finally, $C_A(B) \cong M_r(D)$ so that

$$[C_A(B) : k] = r^2[D : k]. \tag{4.27}$$

Multiplying (4.26) by (4.27) and comparing the result with (4.25) gives the desired equality.

(3). Clearly we have $B \subseteq C_A(C_A(B))$. Now replacing $B$ with $C_A(B)$ (which is simple by (1)) in (2) gives

$$[A : k] = [C_A(B) : k][C_A(C_A(B)) : k].$$

Comparing this with the original statement of (2) we deduce that $[B : k] = [C_A(C_A(B)) : k]$ and we are done. □

We now have the necessary tools to understand splitting fields of central division algebras.

**Theorem 4.28.** *Let $D/k$ be a central division algebra and $k \subseteq K \subseteq D$ a field. Then the following are equivalent:*

(1) *$K$ is a maximal field in $D$,*
(2) *$C_D(K) = K$,*
(3) *$[K : k] = \deg D$,*
(4) *$K$ splits $D$.*

*Remark* 4.29. Note that any central division algebra $D/k$ does have at least one maximal subfield $K$ with $k \subseteq K$, since the subfields of $D$ containing $k$ are all $k$-vector subspaces of the finite dimensional $k$-vector space $D$.

*Proof of Theorem 4.28.* (1) $\Leftrightarrow$ (2). Clear. (2) $\Leftrightarrow$ (3). Since we always have $K \subseteq C_D(K)$ we see that $K = C_D(K)$ if and only if $[K : k] = [C_D(K) : k]$. By the double centraliser theorem we have $[D : k] = [K : k][C_D(K) : k]$ so that $K = C_D(K)$ if and only if

$$[K : k] = \sqrt{[D : k]} = \deg D.$$

(3) $\Rightarrow$ (4). This is Proposition 4.21. (4) $\Rightarrow$ (3). Suppose that $K$ splits $D$ and write $n = \deg D$. Certainly $K$ is contained in some maximal subfield which by (1) $\Rightarrow$ (3) has degree $n$ over $k$. By the tower law $[K : k]$ divides $n$ and it remains to show the reverse divisibility. Fix an isomorphism

$$\phi : D \otimes_k K \to M_n(K).$$

Now consider the (simple) $M_n(K)$-module $V = K^n$. This becomes a $D$-module via $\phi$ and as such is isomoprhic to $D^r$ for some $r$. Now on the one hand we have

$$[V : k] = r[D : k] = rn^2$$

whilst on the other

$$[V : k] = n[K : k].$$

Combining the two gives $[K : k] = nr$ and we are done. □

In fact, we can adapt the argument for (3) $\Rightarrow$ (4) above to say something about splitting fields for division algebras that are not necessarily subfields.

**Theorem 4.30.** *Let $D/k$ be a central division algebra and $K/k$ a finite extension that splits $D$. Then $\deg D$ divides $[K : k]$. Moreover, if $[K : k] = \deg D$ then $K$ is $k$-isomorphic to a maximal subfield of $D$.*

*Proof.* For reasons that will become clear later, it's more convenient to run to argument of (3) $\Rightarrow$ (4) for $D^{\mathrm{opp}}$ instead of $D$. Note that by Remark 4.18 $K$ splits $D^{\mathrm{opp}}$since it splits $D$, and we have $\deg D = \deg D^{\mathrm{opp}} = n$, say. As above write $V = K^n$ and fix an isomorphism

$$\phi : D^{\mathrm{opp}} \otimes_k K \xrightarrow{\sim} M_n(K).$$

Then the identical argument to the proof of (3) $\Rightarrow$ (4) in Theorem 4.28 shows that $n$ divides $[K : k]$ and in fact $[K : k] = nr$ where $V \cong (D^{\mathrm{opp}})^r$ as $D^{\mathrm{opp}}$-modules (the LHS viewed as a $D^{\mathrm{opp}}$-module via $\phi$).

Now suppose we have $[K : k] = n$ so that $r = 1$ in the above and $V \cong D^{\mathrm{opp}}$ as $D^{\mathrm{opp}}$-modules. The isomorphism $\phi$ gives an action of all of $D^{\mathrm{opp}} \otimes_k K$ on $V$, rather than just $D^{\mathrm{opp}}$, and since $K$ (embedded in the second factor) is central in $D^{\mathrm{opp}} \otimes_k K$ the induced $K$ action on $V$ commutes with the $D^{\mathrm{opp}}$ action. This gives a homomorphism of $k$-algebras $K \to \mathrm{End}_{D^{\mathrm{opp}}}(D^{\mathrm{opp}}) \cong D$ which is an embedding since $K$ is a field. The image of $K$ in $D$ is then a maximal subfield by (1) $\Rightarrow$ (3) of Theorem 4.28. □

*Remark* 4.31. In the last paragraph of the proof of Theorem 4.30, if we don't assume $[K:k] = n$ then the same argument gives an embedding of $K$ into $\mathrm{End}_{D^{\mathrm{opp}}}((D^{\mathrm{opp}})^r) \cong M_r(D)$. Then $A = M_r(D)$ has degree $rn = [K:k]$ and contains $K$ as a subfield. The same double centraliser theorem argument as for division algebras then shows that $C_A(K) = K$, so that in particular $K$ is a maximal subfield in $A$. When we later define Brauer equivalence (Definition 5.1), we can neatly phrase the above as saying that any central simple algebra over $k$ split by a finite extension $K/k$ is Brauer equivalent to a central simple algebra in which $K$ embeds as a maximal subfield.

4.4.3. *Central simple algebras over* $\mathbb{R}$.

**Theorem 4.32.** *Let $D/\mathbb{R}$ be a central division algebra. Then $D$ is isomorphic to $\mathbb{R}$ or $\mathbb{H}$.*

*Proof.* Let $K$ be a maximal subfield of $D$. Then either $K = \mathbb{R}$ or $K = \mathbb{C}$. Since the degree of $D$ is equal to $[K:\mathbb{R}]$, $\deg D = 1$ or 2 respectively. In the first instance $D$ has $\mathbb{R}$-dimension 1, and as such is isomorphic to $\mathbb{R}$. In the second instance $D$ has dimension 4 over $\mathbb{R}$ and $K$ is isomorphic to $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. Now Theorem 2.15 shows that $D \cong (-1, b)$ for some $b \in \mathbb{R}^\times$. Since we may shift $b$ by squares in $\mathbb{R}$ without changing the isomorphism class of the associated quaternion algebra we see that $D$ is either isomorphic to $\mathbb{H}$ or the quaternion algebra $(-1, 1)$. However the later is not a division algebra and we are done. □

Wedderburn's theorem now gives the following corollary.

**Corollary 4.33.** *Every central simple algebra over $\mathbb{R}$ is isomorphic to $M_n(\mathbb{R})$ on $M_n(\mathbb{H})$ for some $n \geq 1$.*

4.4.4. *Central simple algebras over finite fields.* Let $k$ be a finite field, say with $q$ elements. We'll show that any central simple algebra over $k$ is isomorphic to $M_n(k)$ for some $n$. By Wedderburn's theorem, this amounts to showing that there are no nontrivial central division algebras over $k$. Note that if $D$ is a central division algebra over $k$ then the multiplicative group $D^\times = D \setminus \{0\}$ is a finite group. In fact, $D^\times$ has order $q^{n^2} - 1$ where $n = \sqrt{\dim_k D}$ is the degree of $D$. We'll need the following group theoretic lemma. For a finite group $G$ and $H \leq G$ we write $N_G(H)$ for the *normaliser* of $H$ in $G$:

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Note that for any subgroup $H \leq G$ we always have $H \subseteq N_G(H)$.

**Lemma 4.34.** *Let $G$ be a finite group and $H \leq G$ a subgroup. Then $G$ is a union of conjugates of $H$ (i.e. $G = \cup_{g \in G} gHg^{-1}$) if and only if $H = G$.*

*Proof.* Let $S$ be the set of all conjugates of $H$, i.e.

$$S = \{gHg^{-1} \mid g \in G\}.$$

Then $G$ acts transitively on the elements of $S$ by conjugation and the stabiliser of $H \in S$ is precisely its normaliser $N_G(H)$. Thus the orbit-stabiliser theorem gives

$$|G| = |S||N_G(H)| \geq |S||H|. \tag{4.35}$$

On the other hand, $\cup_{g \in G} gHg^{-1}$ is simply the union over all elements of $S$. Since all elements of $S$ contain the identity, this union is disjoint if and only if $|S| = 1$, i.e. if and only if $S = \{H\}$. In particular, we have

$$|\cup_{g \in G} gHg^{-1}| \leq |S||H|$$

with equality if and only if this union is equal to $H$. Comparing with (4.35) gives the result. □

**Theorem 4.36** (Wedderburn's little theorem)**.** *Let $D$ be a central division algebra over a finite field $k$. Then $D = k$.*

*Proof.* Let $n$ be the degree of $D$ and fix a maximal subfield $L$ of $D$. By Theorem 4.28 $L$ has degree $n$ over $k$, and as such is isomorphic to the unique finite field with $q^n$ elements. Now let $\alpha \in D^\times$ be arbitrary. Since $k(\alpha)$ is a subfield of $D$, it's necessary contained in some maximal subfield of $D$, say $L'$. Again by Theorem 4.28 this has degree $n$ over $k$, so $L'$ is also isomorphic to the unique finite field of $q^n$ elements. That is, we may fix a $k$-algebra isomorphism $\phi : L \xrightarrow{\sim} L' \subseteq D$, which by the Skolem–Noether theorem (Theorem 4.8) is given by conjugation by an element of $D^\times$. That is, inside $D$ we have $L' = dLd^{-1}$ for some $d \in D^\times$. Since $\alpha \in D^\times$ was arbitrary, this shows that every element of $D^\times$ lies in some conjugate of $L^\times$. In other words, we have

$$D^\times = \bigcup_{d \in D^\times} dL^\times d^{-1}.$$

But $L^\times$ is a subgroup of the finite group $D^\times$ and so Lemma 4.34 gives $L^\times = D^\times$. Thus $D$ is commutative whence $D = k$. □

Wedderburn's theorem now gives the following corollary.

**Corollary 4.37.** *Let $k$ be a finite field. Then every central simple algebra over $k$ is isomorphic to $M_n(k)$ for some $n \geq 1$.*

4.5. **Galois splitting fields for central simple algebras.** We close this section by showing that not only is every central simple algebra over $k$ split by a finite extension, but that this extension may be taken to be Galois over $k$. This will be crucial later when we use Galois cohomology to describe the Brauer group of a field. In what follows we will use various facts about separable and purely inseparable extensions. See Keith Conrad's notes [Con] for an introduction to these topics.

**Proposition 4.38.** *Let $D/k$ be a central division algebra. Then $D$ has a maximal subfield which is separable over $k$. In particular, $D$ is split by a finite separable extension of $k$.*

The key step in the proof of Proposition 4.38 is the following lemma.

**Lemma 4.39.** *Let $D/k$ be a central division algebra not equal to $k$. Then there is a non-trivial separable extension $K/k$ with $k \subseteq K \subseteq D$.*

*Proof.* Recall that a purely inseparable extension has trivial $k$-automorphism group. Thus we wish to exhibit a non-trivial extension of $k$ which has non-trivial $k$-automorphisms. By the Skolem–Noether theorem such automorphisms will extend to inner automorphisms of $D$. So we want to find a non-trivial extension of $k$ such that some inner automorphism of $D$ acts non trivially on this extension.

Fix $x \in D \setminus k$ so that $k(x)$ is a non-trivial extension of $k$. If $k(x)/k$ is not purely inseparable we are done, so we assume that $k(x)/k$ is purely inseparable. In particular $\mathrm{char}(k) = p > 0$ and the minimal polynomial of $x$ over $k$ has the form $X^{p^e} - \alpha$ for some $0 \neq \alpha \in k$ and $e \geq 1$. Replacing $x$ by $x^{p^{e-1}}$ if necessary we may assume that $e = 1$ so that $x^p \in k$ but $x \notin k$.

Now consider the $k$-automorphism $\sigma$ of $D$ given by $d \mapsto xdx^{-1}$. Since $x^p \in k = Z(D)$ we have $\sigma^p = \mathrm{id}$, yet $\sigma \neq \mathrm{id}$ since $x \notin k$. Since $\mathrm{char}(k) = p$ this says that $(\sigma - 1)^p = 0$ yet $\sigma - 1 \neq 0$ inside $\mathrm{End}_k(D)$. Let $1 \leq r < p$ be maximal so that $(\sigma - 1)^r \neq 0$. Then there is $y \in D$ with $(\sigma - 1)^r y \neq 0$. Define

$$a = (\sigma - 1)^{r-1} y \neq 0$$

and

$$b = (\sigma - 1)a = (\sigma - 1)^r y \neq 0.$$

By construction $\sigma(b) = b$ (since $(\sigma - 1)^{r+1} = 0$). Finally, set $c := b^{-1}a$ so that

$$\sigma(c) = \sigma(b)^{-1}\sigma(a) = b^{-1}(b + a) = 1 + c.$$

Thus $k(c)$ is stable under the action of $\sigma$ yet $\sigma$ restricts to a non-trivial $k$-automorphism of $k(c)$. Thus $k(c)/k$ is a non-trivial field extension which cannot be purely inseparable. The maximal separable subextension of $k(c)$ then provides the desired field extension of $k$. □

*Proof of Proposition 4.38.* Amongst all subfields $k \subseteq K \subseteq D$ with $K/k$ separable, pick one which maximises $[K : k]$. If $K = C_D(K)$ then $K$ is a maximal subfield of $D$ and we ae done. So suppose $K \subsetneq C_D(K)$. By the double centraliser theorem $C_D(K_1)$ is a central simple algebra over $K_1$. In fact, it's also division being a finite dimensional subalgebra of a division algebra. Then by Lemma 4.39 we can find a non-trivial separable extension $K'$ with $K \subsetneq K' \subseteq C_D(K)$. Since $K'/K$ and $K/k$ are separable, so is $K'/k$, contradicting the maximality of $[K : k]$. □

**Corollary 4.40.** *Let $A/k$ be a central simple algebra. Then $A$ is split by a finite Galois extension of $k$.*

*Proof.* By Wedderburn's theorem it suffices to prove this for $A/k$ a central division algebra. We now find the desired extension as the Galois closure of a maximal subfield of $A$ seperable over $k$. □

*Remark* 4.41. It is natural to ask if, in fact, every central division algebra has a maximal *Galois* subfield, not just a separable one. It was shown by Amitsur in 1972 [Ami72] that this is not the case. Central division algebras which do have a maximal Galois subfield are called *crossed products*.

## 5. The Brauer group of a field

**Definition 5.1.** Let $A$ and $A'$ be central simple algebras over $k$. We say that $A$ and $A'$ are *Brauer equivalent* if there are positive integers $m, n$ such that $M_n(A) \cong M_m(A')$ as $k$-algebras. We write $A \sim A'$. It's easy to see that this is an equivalence relation on isomorphism classes of central simple algebras. Here for transitivity we note that if $M_m(A) \cong M_n(A')$ and $M_r(A') \cong M_s(A'')$ then

$$M_{mr}(A) \cong M_{nr}(A') \cong M_{ns}(A'').$$

We denote by $\mathrm{Br}(k)$ the set

$$\mathrm{Br}(k) = \{k\text{-alg iso classes of central simple algebras over } k\}/\sim$$

and for $A$ a central simple algebra over $k$ we denote by $[A]$ its class in $\mathrm{Br}(k)$.

*Remark* 5.2. It follows from Wedderburn's theorem that $A$ and $A'$ are Brauer equivalent if and only if they have the same underlying division algebra. In other words, every $\mathrm{CSA}/k$ is Brauer equivalent to a unique division algebra.

Recall that if $A$ and $A'$ are central simple algebras over $k$ then $A \otimes_k A'$ is also a central simple algebra over $k$. Our aim is to show that $\mathrm{Br}(k)$ is an abelian group under tensor product. Note that if $A$ and $A'$ a Brauer equivalent, say $M_n(A) \cong M_r(A')$ and $B$ is another central simple algebra, then

$$M_n(A \otimes_k B) \cong M_n(A) \otimes_k B \cong M_r(A') \otimes_k B \cong M_r(A' \otimes_k B)$$

so that tensor product descends to a binary operation on Brauer equivalence classes.

**Lemma 5.3.** *Let $A/k$ be a central simple algebra of degree $n$. Then*

$$A \otimes_k A^{\mathrm{opp}} \cong M_{n^2}(k).$$

*Proof.* Define the $k$-algebra homomorphism

$$\psi : A \otimes_k A^{\mathrm{opp}} \to \mathrm{End}_k(A) \cong M_{n^2}(A)$$

(here $\mathrm{End}_k(A)$ denotes $k$-vector space endomorphisms of $A$) by setting $a \otimes b \to (x \mapsto axb)$. Now $A \otimes_k A^{\mathrm{opp}}$ is a central simple algebra over $k$ and the kernel of $\psi$ is a 2-sided ideal not equal to $A \otimes_k A^{\mathrm{opp}}$ (note that $1 \otimes 1$ is not in the kernel). Thus $\psi$ is injective, and by counting dimensions over $k$ we see that $\psi$ is surjective. □

**Theorem 5.4.** *The set* $\mathrm{Br}(k)$ *becomes an abelian group under* $\otimes_k$*, which we call the* Brauer group *of* $k$*.*

*Proof.* This follows from Lemma 5.3 and the discussion above. The identity element is the class of $k$ and the inverse of (the class of) a central simple algebra $A$ is the opposite algebra $A^{\mathrm{opp}}$. Moreover, we have $A \otimes_k A' \cong A' \otimes_k A$ via the map $a \otimes a' \mapsto a' \otimes a$. □

**Proposition 5.5.** *If $k$ is either algebraically closed or finite, then* $\mathrm{Br}(k) = 0$*. Moreover, we have*

$$\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$$

*with the unique non-trivial element being given by (the class of) Hamilton's quaternions* $\mathbb{H}$*.*

*Proof.* By Theorem 3.9 every central simple algebra over an algebraically closed field $k$ has the form $M_n(k)$ for some $n$, and is hence trivial in the Brauer group. The same is true for $k$ a finite field by Corollary 4.37. For $k = \mathbb{R}$ we have seen in Theorem 4.32 that there are precisely two central division algebras over $k$, $\mathbb{H}$ and $k$ itself. Since each Brauer class is represented by a unique central division algebra, with the identity element corresponding to $k$, the result follows. □

*Remark* 5.6. By Proposition 4.38 we can in fact replace 'algebraically closed' with the weaker 'separably closed' in the statement of Proposition 5.5.

The following refinement of the Brauer group will be useful. Note that if $A$ and $A'$ are Brauer equivalent and $A$ is split by $K$ then so is $A'$. Indeed, a central simple algebra over $K$ is split by if and only if the underlying divison algebra is.

**Definition 5.7.** Let $K$ be a (possibly infinite) extension of $k$. Denote by $\mathrm{Br}(K/k)$ the subset of $\mathrm{Br}(k)$ consisting of classes split by $K/k$.

Recall from Theorem 4.4 that if $A$ is a CSA$/k$ and $K/k$ is any field extension, then $A \otimes_k K$ is a CSA$/K$.

**Lemma 5.8.** *For any field exension $K/k$, the map $[A] \mapsto [A \otimes_k K]$ gives a homomorphism from* $\mathrm{Br}(k)$ *to* $\mathrm{Br}(K)$ *with kernel* $\mathrm{Br}(K/k)$*. In particular,* $\mathrm{Br}(K/k)$ *is a subgroup of* $\mathrm{Br}(k)$*.*

*Proof.* If $A$ and $A'$ are central simple algebras over $k$ with $A \ A'$, say $M_n(A) \cong M_m(A')$, then $A \otimes_k K \ A \otimes_k K'$ since

$$M_n(A \otimes_k K) \cong M_n(A) \otimes_k K \cong M_m(A') \otimes_k K \cong M_n(A' \otimes_k K).$$

Thus the map is well defined. It's a homomorphism since given $[A]$ and $[A']$ in $\mathrm{Br}(k)$ we have

$$(A \otimes_k A') \otimes_k K \cong A \otimes_k A' \otimes_k K \otimes_K K \cong (A \otimes_k K) \otimes_K (A \otimes_k K).$$

Finally, note that $[A] \in \mathrm{Br}(k)$ is in the kernel of this map if and only if $A \otimes_k K$ has underlying division algebra $K$, i.e. if and only if $A \otimes_k K \cong M_n(K)$ for some $n$. That is, if and only if $A$ is split by $K$. □

*Remark* 5.9. Since every central simple algebra over $k$ is split by a finite Galois extension we have

$$\mathrm{Br}(k) = \bigcup_{K/k \text{ fin. Gal.}} \mathrm{Br}(K/k).$$

We end this section by giving a slightly different construction of the Brauer group which will be useful later. For $K/k$ a field extension, denote by $CSA_n(K/k)$ the set of isomorphism classes of central simple algebras over $k$ which are split by $K/k$, and have degree $n$.

**Proposition 5.10.** *As $n, m$ range over all positive integers, the maps $CSA_n(K/k) \to CSA_{mn}(K/k)$ given by $A \mapsto M_m(A)$ make $\{CSA_n(K/k)\}_n$ into a direct system, and we have*

$$\varinjlim CSA_n(K/k) = \mathrm{Br}(K/k)$$

*via the natural map sending the class of a central simple algebra on the left hand side to its Brauer class on the right hand side.*

*Remark* 5.11. We caution that the $CSA_n(K/k)$ do not have a natural group structure, so that the direct limit in the proposition takes place in the category of sets. In particular, the equality with $\mathrm{Br}(K/k)$ is as sets rather than groups. Thus the proposition is maybe best thought of as another way of constructing Brauer equivalence, rather than the Brauer group itself.

*Proof of Proposition 5.10.* It's clear that the maps for a direct system. By definition, the direct limit in question is

$$\bigsqcup_{n \geq 1} CSA_n(K/k)$$

modulo the equivalence relation that $A \in CSA_n(K/k)$ is equivalent to $A' \in CSA_m(K/k)$ if and only if there is $s \geq 1$ with $s = nr = mr'$ for some $r, r' \geq 1$ and such that $M_r(A) \cong M_{r'}(A')$. Now note that the disjoint union is just the collection of isomorphism classes of CSAs$/k$, and that the equivalence relation just described is precisely Brauer equivalence. □

## 6. Non-abelian $H^1$ and Galois descent

In this section we leverage the existence of Galois splitting fields for central simple algebras to reduce the study of central simple algebras over a field $k$ to the study of various 'twisted' Galois actions on matrix algebras over larger fields. In this way, we obtain a cohomological description of the Brauer group.

### 6.1. Semilinear actions.

Let $K/k$ be a finite Galois extension and denote by $G$ the Galois group $G = \mathrm{Gal}(K/k)$.

**Definition 6.1.** We say that $G$ acts *semilinearly* on a $K$-vector space $V$ if $G$ acts on $V$ and for all $\sigma \in G$ we have

$$\sigma(v_1 + v_2) = \sigma(v_1) + \sigma(v_2) \text{ for all } v_1, v_2 \in V$$

and

$$\sigma(\lambda v) = \sigma(\lambda)\sigma(v) \text{ for all } \lambda \in K,\ v \in V.$$

If $G$ acts semilinearly on $V$ then we define

$$V^G = \{v \in V \mid gv = v \ \forall g \in G\}.$$

Note that $V^G$ is naturally a $k$-vector space.

*Remark* 6.2. For any $n \geq 1$, both the 'coordinatewise' action of $G$ on $K^n$ and the 'coefficientwise' action of $G$ on $M_n(K)$ are semilinear actions. More generally, if $V_0$ is a $k$-vector space then $G$ acts semilinearly on the $K$-vector space $V_0 \otimes_k K$ via $\sigma(v \otimes \lambda) = v \otimes \sigma(\lambda)$. As usual we view $V_0$ inside $V_0 \otimes_k K$ via $v \mapsto v \otimes 1$.

**Lemma 6.3.** *For any (possibly infinite dimensional) $k$-vector space $V_0$ we have*

$$(V_0 \otimes_k K)^G = V_0.$$

*Proof.* Let $\mathcal{B} = \{x_i\}_{i \in I}$ be a $k$-basis for $V_0$, so that $\mathcal{B}$ is also a $K$-basis for $V_0 \otimes_k K$. Then for any $x \in V_0 \otimes_k K$ and $\sigma \in G$, writing

$$x = \sum_{i \in I} x_i \otimes \lambda_i$$

for some $\lambda_i \in K$ we find

$$\sigma(x) = \sum_{i \in I} x_i \otimes \sigma(\lambda_i).$$

Since the $x_i$ are linearly independent over $K$, $x$ is fixed by $\sigma$ if and only if each of the $\lambda_i$ are. In particular, $x$ is in $(V_0 \otimes_k K)^G$ if and only if each $\lambda_i$ is in $K^G = k$. Thus

$$(V_0 \otimes_k K)^G = V_0 \otimes_k k = V_0$$

as desired. □

Lemma 6.3 says that we can recover a $k$-vector space $V_0$ from $V_0 \otimes_k K$ along with its semilinear action. In the next subsection we prove a sort of converse to this. Between the two, we will show that for $K/k$ finite Galois, the data of a $k$-vector space is equivalent to the data of a $K$-vector space equipped with a semilinear action. The importance of this result for us is that this correspondence will be compatible with algebra structures on the vector spaces, reducing studying central simple algebras over $k$ to studying central simple algebras over $K$ equipped with an appropriate Galois action.

6.2. **Galois descent for vector spaces.** We begin with a general result.

**Lemma 6.4** (Linear independence of characters)**.** *Let $F$ be a field and $V$ an $F$-vector space. Further, let $\Sigma$ be a group and $\chi_1, ..., \chi_n$ distinct homomorphisms*

$$\chi_i : \Sigma \to F^\times$$

*(i.e. 1-dimensional characters defined over $F$). If $v_1, ..., v_n \in V$ are such that*

$$\chi_1(g)v_1 + ... + \chi_n(g)v_n = 0$$

*for all $g \in \Sigma$, then $v_1 = ... = v_n = 0$.*

*Proof.* The proof is by induction on $n$. If $n = 1$ then the result is clear. Now suppose $n > 1$, so that $\chi_n \neq \chi_1$, and fix $h \in \Sigma$ with $\chi_1(h) \neq \chi_n(h)$. Then for all $g \in \Sigma$ we have

$$0 = \sum_{i=1}^{n} \chi_i(gh)v_i - \chi_n(h) \sum_{i=1}^{n} \chi_i(g)v_i = \sum_{i=1}^{n-1} \chi_i(g) \left(\chi_i(h) - \chi_n(h)\right) v_i.$$

Defining $v_i' = (\chi_i(h) - \chi_n(h))\, v_i$ the inductive hypothesis gives $v_i' = 0$ for $i = 1, ..., n-1$. Since we've chosen $h$ such that $\chi_1(h) \neq \chi_n(h)$, we in particular have $v_1 = 0$. But then applying the inducitve hypothesis once again gives $v_2 = ... = v_n = 0$. □

We now return to the situation where $K/k$ is a finite Galois extension with Galois group $G$.

**Definition 6.5.** Let $V$ be a $K$-vector space on which $G$ acts semilinearly. We define the *trace map* to be the additive map $\mathrm{Tr} : V \to V$ given by

$$v \mapsto \sum_{\sigma \in G} \sigma(v).$$

Note that this takes values in $V^G$.

**Lemma 6.6** (Non-vanishing of trace)**.** *Let $V$ be a $K$-vector space on which $G$ acts semilinearly. Then for any non-zero element $0 \neq v \in V$ there is $\lambda \in K$ with $\mathrm{Tr}(\lambda v) \neq 0$. In particular, if $V \neq 0$, then $V^G \neq 0$ and* Tr *does not vanish identically.*

*Proof.* Suppose no such $\lambda$ exists, so that for all $\lambda \in K^\times$ we have

$$0 = \mathrm{Tr}(\lambda v) = \sum_{\sigma \in G} \sigma(\lambda)\sigma(v).$$

Now each $\sigma \in G$ restricts to a homomorphism $K^\times \to K^\times$ and as $\sigma$ ranges over all elements of $G$, these homomorphisms are all distinct. By Lemma 6.4 we find $\sigma(v) = 0$ for all $\sigma \in G$. In particular, taking $\sigma = \mathrm{id}$ we find $v = 0$, a contradiction. □

**Theorem 6.7.** *Let $V$ be a $K$-vector space on which $G$ acts semilinearly. Then the map $\phi : V^G \otimes_k K \to V$ given by $v \otimes \lambda \mapsto \lambda v$ is an isomorphism of $K$-vector spaces.*

*Proof.* Let $\{v_i\}_{i \in I}$ be a basis for $V^G$ as a $k$-vector space. Then this same set is a $K$-basis for $V^G \otimes_k K$. Thus any element of $V^G \otimes_k K$ is uniquely a finite sum $\sum_{i \in I} v_i \otimes \lambda_i$ for some $\lambda_i \in K$, and under $\phi$ this maps to $\sum_{i \in I} \lambda_i v_i$. In particular, to show that $\phi$ is injective it suffices to show that the set $\{v_i\}_{i \in I}$ is $K$-linearly independent inside $V$. Suppose otherwise and fix a non-trivial relation of minimal length, say

$$\sum_{j=1}^{r} \lambda_{i_j} v_{i_j} = 0 \tag{6.8}$$

for $i_1, ..., i_r \in I$ and $\lambda_{i_j} \in K^\times$. Multiplying this relation by $\lambda_{i_1}^{-1}$ we assume $\lambda_{i_1} = 1$. Now for any $\sigma \in G$, applying $\sigma$ to this relation and remembering that each $v_{i_j}$ is in $V^G$, we find

$$\sum_{j=1}^{r} \sigma(\lambda_{i_j}) v_{i_j} = 0.$$

Subtracting this from (6.8), noting that $\lambda_{i_1} = 1 = \sigma(\lambda_{i_1})$, we obtain

$$0 = \sum_{j=2}^{r} \left(\sigma(\lambda_{i_j}) - \lambda_{i_j}\right) v_{i_j}.$$

By minimality of the relation (6.8) we must have $\sigma(\lambda_{i_j}) = \lambda_{i_j}$ for each $j = 2, ..., r$, and this trivially holds for $\lambda_{i_1}$ also. Since $\sigma \in G$ was arbitrary all the $\lambda_{i_j}$ are in $K^G = k$. Thus (6.8) is in fact a $k$-relation, contradicting the $k$-linear independence of the $\{v_i\}_{i \in I}$.

It remains to show surjectivity of $\phi$. Now $\mathrm{im}(\phi)$ is visibly stable under the action of $G$, and we get an induced semilinear action on the quotient $\overline{V} = V/\mathrm{im}(\phi)$. For $v \in V$, write $\bar{v}$ for its class in $\overline{V}$. Since the trace map on $V$ takes values in $V^G \subseteq \mathrm{im}(\phi)$, for each $\bar{v} \in \overline{V}$ we have

$$\mathrm{Tr}(\bar{v}) = \overline{\mathrm{Tr}(v)} = 0.$$

Thus the trace map vanishes identically on $\overline{V}$ which, by Lemma 6.6, forces $\overline{V} = 0$. That is, $\mathrm{im}(\phi) = V$ as desired. □

**Corollary 6.9.** *Let $V$ be a $K$-vector space on which $G$ acts semilinearly. Then $V$ has a $K$-basis consisting of vectors invariant under the $G$-action.*

*Proof.* Let $\mathcal{B} = \{v_i\}_{i \in I}$ be any $k$-basis for $V^G$, so that $\mathcal{B}$ is also a $K$-basis for $V^G \otimes_k K$. Now Theorem 6.7 gives $V^G \otimes_k K \cong V$, and the explicit map from left to right sends each element of $\mathcal{B}$ viewed inside $V^G \otimes_k K$ to the same element viewed inside $V$ instead. Since this map is an isomorphism $\mathcal{B}$ is a basis for $V$ as a $K$-vector space and we are done. □

*Remark* 6.10. Note that as well as being an isomorphism of $K$-vector spaces, the map $\phi : V^G \otimes_k K \to V$ of Theorem 6.7 is *$G$-equivariant* in the sense that

$$\phi(\sigma x) = \sigma(\phi(x))$$

for all $x \in V^G \otimes_k K$ and $\sigma \in G$.

*Remark* 6.11. If $V_0$ and $V_0'$ are $k$-vector spaces and $f : V_0 \to V_0'$ is a $k$-linear homomorphism, then $f \otimes 1 : V_0 \otimes_k K \to V_0' \otimes_k K$ given by $a \otimes \lambda \mapsto f(a) \otimes \lambda$ is a $K$-linear homomorphism, equivariant for the action of $G$. Similarly, if $V$ and $V'$ are $K$-vector spaces on which $G$ acts semilinearly, and $f : V \to V'$ is a $G$-equivariant $K$-linear homomorphism, then $f$ restricts to a $k$-linear homomorphism

$$f|_{V^G} \colon V^G \to (V')^G.$$

In this way, $(-) \otimes_k K$ and $(-)^G$ are naturally functors.

The material in this section can be summarised in the following.

**Theorem 6.12** (Galois descent for vector spaces)**.** *Let $k$ be a field and $K/k$ a finite Galois extension. Then we have an equivalence of categories*

$$\left\{ \begin{array}{c} k\text{-vector spaces} \\ \text{and} \\ k\text{-linear homs} \end{array} \right\} \underset{(-)^G}{\overset{(-)\otimes_k K}{\rightleftarrows}} \left\{ \begin{array}{c} K\text{-vector spaces with semilinear } G\text{-action} \\ \text{and} \\ G\text{-equivariant } K\text{-linear homs} \end{array} \right\}.$$

*Proof.* This combines Lemma 6.3 and Theorem 6.7, the remaining details being an easy check. □

The category of $k$-vector spaces is not particularly interesting, since $k$-vector spaces are classified by their dimension. However, the main importance of Theorem 6.12 for us is that, suitably formulated, it preserves algebra structure on each side and takes central simple algebras to central simple algebras.

6.3. **Galois descent for central simple algebras.**

**Notation 6.13.** By a slight abuse of notation, when we say $G$ acts *semilinearly* on a $K$-algebra $A$, we mean that $A$ acts semilinearly on $A$ viewed as a $K$-vectors space, and that additionally the action is compatible with the ring structure in the sense that

$$\sigma(ab) = \sigma(a)\sigma(b)$$

for all $a, b \in A$ and $\sigma \in G$. Note that in this case, multiplication in $A$ makes $A^G$ into a $k$-algebra.

**Lemma 6.14.** *Let $A$ be a CSA/$K$ on which $G$ acts semilinearly. Then $A^G$ is a CSA/$k$.*

*Proof.* Note that the $K$-vector space isomorphism $A^G \otimes_k K \xrightarrow{\sim} A$ of Theorem 6.7 (sending $a \otimes \lambda$ to $\lambda a$) is in fact an isomorphism of $K$-algebras. Thus $A^G \otimes_k K$ is a central simple algebra over $K$, whence $A^G$ is a central simple algebra over $k$ by Theorem 4.4. □

*Remark* 6.15. If $A_0$ and $B_0$ are $k$-algebras and $f : A_0 \to B_0$ is a $k$-algebra homomorphism, then $f \otimes 1 : A_0 \otimes_k K \to B_0 \otimes_k K$ is a $K$-algebra homomorphism, equivariant for the action of $G$. Similarly, if $A$ and $B$ are $K$-algebras on which $G$ acts semilinearly, and $f : A \to B$ is a $G$-equivariant $K$-algebra homomorphism, then $f$ restricts to a $k$-algebra homomorphism

$$f|_{A^G} \colon A^G \to B^G.$$

Thus, like in the vector space case, $(-) \otimes_k K$ and $(-)^G$ are naturally functors.

**Theorem 6.16** (Galois descent for central simple algebras)**.** *Let $k$ be a field and $K/k$ a finite Galois extension. Then we have an equivalence of categories*

$$\left\{\begin{array}{c} k\text{-algebras} \\ \text{and} \\ k\text{-algebra homs} \end{array}\right\} \underset{(-)^G}{\overset{(-)\otimes_k K}{\rightleftarrows}} \left\{\begin{array}{c} K\text{-algebras with semilinear } G\text{-action} \\ \text{and} \\ G\text{-equivariant } K\text{-algebra homs} \end{array}\right\}$$

*which restricts to an equivalence of categories*

$$\left\{\begin{array}{c} \text{CSAs } /k \\ \text{and} \\ k\text{-algebra homs} \end{array}\right\} \underset{(-)^G}{\overset{(-)\otimes_k K}{\rightleftarrows}} \left\{\begin{array}{c} \text{CSAs } /K \text{ with semilinear } G\text{-action} \\ \text{and} \\ G\text{-equivariant } K\text{-algebra homs} \end{array}\right\}.$$

*Proof.* As in the vector space case, this combines Lemma 6.3 and Theorem 6.7 with the remaining details being easily checked. To see that it restricts to an equivalence of categories in the central simple algebra case we use Lemma 6.14. □

6.4. **Non-abelian $H^1$.** Let $G$ be a group. Recall that if $X$ is a set on which $G$ acts, a *$G$-set*, then we have an associated homomorphism

$$G \to \mathrm{Bij}(X) = \{\text{bijections } X \to X\}$$

via $g \mapsto (x \mapsto g \cdot x)$, where here $\mathrm{Bij}(X)$ is a group under composition.

**Definition 6.17.** Let $G$ be a group. A *$G$-group* is a group $X$ on which $G$ acts in a manner compatible with the group structure. Explicitly, an action of $G$ on the underlying set of $X$ makes $X$ into a $G$-group if

$$g \cdot (xy) = (g \cdot x)(g \cdot y) \quad \text{for all } g \in G,\ x, y \in X.$$

Note that, for all $g \in G$, this forces $g \cdot 1_X = 1_X$ and, for all $x \in X$, $g \cdot (x^{-1}) = (g \cdot x)^{-1}$. If $X$ is abelian we call $X$ a *$G$-module*. Put another way, the associated homomorphism $G \to \mathrm{Bij}(X)$ takes values in

$$\mathrm{Aut}(X) = \{\text{grp automorphisms of } X\} \leq \mathrm{Bij}(X).$$

Thus a $G$ group is precisely the data of a group $X$ and a homomorphism $G \to \mathrm{Aut}(X)$.

We similarly define a *$G$-ring* (resp. a *$G$-algebra* relative to a field $k$) to be a ring (resp. $k$-algebra) $X$ equipped with a homomorphism from $G$ into the group of ring (resp. $k$-algebra) automorphisms of $X$.

**Definition 6.18.** Let $G$ be a group and $X$ a $G$-group. A map $\rho : G \to X$ is called a 1-*cocycle* if

$$\rho(gh) = \rho(g)\ g \cdot \rho(h) \tag{6.19}$$

for all $g, h \in G$.

*Remark* 6.20. Note that:

- The map $G \to X$ sending every element of $G$ to $1_X$ is a 1-cocycle. We call this the *trivial cocycle*.
- If $G$ acts trivially on $X$ then a 1-cocycle is simply a homomorphism from $G$ into $X$.
- For any $x \in X$, the map $G \to X$ given by $g \mapsto x^{-1}(g \cdot x)$ is a 1-cocycle.
- For any 1-cocycle $\rho : G \to X$, we necessarily have $\rho(1_G) = 1_X$ (put $g = 1_G$ in (6.19)) and $\rho(g^{-1}) = g^{-1} \cdot \rho(g)^{-1}$ for all $g \in G$ (put $h = g^{-1}$ in (6.19)). In particular, the set

  $$\{g \in G \ \mid \ \rho(g) = 1_X\}$$

  is a (not necessarily normal) subgroup of $G$.

**Definition 6.21.** We say that 1-cocycles $\rho, \rho' : G \to X$ are *cohomologous* if there is $x \in X$ such that

$$\rho(g) = x^{-1}\rho'(g)(g \cdot x) \ \text{ for all } g \in G.$$

This is easily seen to give an equivalence relation on the set of 1-cocycles valued in $X$. We define the *first cohomology set of $G$ with values in $X$* as

$$H^1(G, X) = \{\text{equivalence classes of 1-cocycles } \rho : G \to X\}.$$

It is a pointed set with the distinguished element being the class of the trivial cocycle.

*Remark* 6.22. In the above, if $X$ is abelian (i.e. a $G$-module) then one checks that pointwise addition of cocycles makes the set of 1-cocycles valued in $X$ into an abelian group, denoted $Z^1(G, X)$. The collection of 1-cocycles cohomologous to the trivial cocycle, denoted $B^1(G, X)$, is then a subgroup of $Z^1(G, X)$ and we have $H^1(G, X) = Z^1(G, X)/B^1(G, X)$. In particular, $H^1(G, X)$ is itself an abelian group.

*Remark* 6.23. Say that homomorphisms $f, f' : G \to X$ are *conjugate* if there is $x \in X$ such that $f(g) = xf'(g)x^{-1}$ for all $g \in G$. If $G$ acts trivially on $X$ then one has

$$H^1(G, X) = \mathrm{Hom}(G, X)/\text{conjugacy}.$$

In particular, if $X$ is additionally abelian then

$$H^1(G, X) = \mathrm{Hom}(G, X).$$

6.5. **1-cocycles and semilinear actions.** We now use the formalism of 1-cocycles to classify semilinear actions on vector spaces and algebras. As usual, let $k$ be a field, $K/k$ a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$, and $V$ a $K$-vector space equipped with a fixed semilinear action (we will primarily be interested in $V = K^n$ or $V = M_n(K)$, equipped with their usual coordinatewise and coefficientwise actions). For $\sigma \in G$, write this action as $v \mapsto \sigma(v)$ and denote by $\sigma$ also the associated map $V \to V$ given by $v \mapsto \sigma(v)$. Finally, denote by $GL(V)$ the group of $K$-linear automorphisms of $V$ and equip this with the left $G$-action given by $\phi \mapsto {}^{\sigma}\phi := \sigma\phi\sigma^{-1}$. That is, for $v \in V$ we have

$$ {}^{\sigma}\phi(v) = \sigma(\phi(\sigma^{-1}(v))).$$

Note that, since $\sigma$ appears along with its inverse in this formula, this action does indeed take $K$-linear automorphisms to $K$-linear automorphisms, even though $\sigma$ itself is only semilinear. In this way, we view $GL(V)$ as a $G$-group. Note that when $V = K^n$, this action on $GL(V) = GL_n(K)$ agrees with the usual coefficientwise action on matrices.

By comparing an arbitrary semilinear action on $V$ to the fixed one we will show that all possible semilinear actions on $V$ are classified by the cohomology group $H^1(G, GL(V))$. First a definition.

**Definition 6.24.** Suppose we have two semilinear actions on $V$, corresponding to homomorphims $\eta, \eta' : G \to \mathrm{Bij}(V)$. Write ${}_{\eta}V$ (resp. ${}_{\eta'}V$) for $V$ considered along with the action $\eta$ (resp. $\eta'$). We say that the actions $\eta$ and $\eta'$ are *isomorphic* if there is a $G$-equivariant $K$-linear isomorphism ${}_{\eta}V \cong {}_{\eta'}V$. Explicitly, $\eta$ and $\eta'$ are isomorphic if there is $\phi \in GL(V)$ such that

$$\eta(\sigma) = \phi^{-1}\eta'(\sigma)\phi$$

for all $\sigma \in G$.

Note that if $\eta : G \to \mathrm{Bij}(V)$ is any semilinear action of $G$ on $V$, then the difference between this and our fixed action, i.e. the map

$$\sigma \mapsto \eta(\sigma)\sigma^{-1} \in \mathrm{Bij}(V),$$

takes values in $GL(V)$ since the precence of both $\sigma$ and its inverse in the above formula 'cancels out' the semilinearity. This observation leads to the the following proposition.

**Proposition 6.25.** *Let $V$ be a $K$-vector space equipped with a fixed semilinear action via which we view $GL(V)$ as a $G$-group. Then*

1. *If $\eta : G \to \mathrm{Bij}(V)$ is a homomorphism associated to another semilinear action of $G$ on $V$, then the map $G \to GL(V)$ given by $\sigma \mapsto \eta(\sigma)\sigma^{-1}$ is a 1-cocycle.*
2. *Conversely, if $\rho : G \to GL(V)$ is a 1-cocycle then the map $G \to \mathrm{Bij}(V)$ given by $\sigma \mapsto \rho(\sigma)\sigma$ defines a semilinear action of $G$ on $V$.*
3. *The maps of (1) and (2) induce a bijection of pointed sets*

$$\{\text{semiliear actions on } V\} \longleftrightarrow \{\text{1-cocycles } G \to GL(V)\}$$

*where the distinguished element on the left is the initial semilinear action. This descends to a bijection of pointed sets*

$$\{\text{semiliear actions on } V\}/\text{iso} \longleftrightarrow H^1(G, GL(V)).$$

*Proof.* (1). As noted previously, since both actions are semilinear and $\sigma$ appears along with its inverse, the map $\rho : \sigma \mapsto \eta(\sigma)\sigma^{-1}$ does indeed take values in $GL(V)$. Moreover, it's a 1-cocycle since for all $\sigma, \tau \in G$ we have

$$\rho(\sigma\tau) = \eta(\sigma\tau)(\sigma\tau)^{-1} = \eta(\sigma)\eta(\tau)\tau^{-1}\sigma^{-1} = (\eta(\sigma)\sigma^{-1})\sigma(\eta(\tau)\tau^{-1})\sigma^{-1} = \rho(\sigma)\ {}^{\sigma}\rho(\tau)$$

as desired.

(2). The map $\eta : \sigma \mapsto \rho(\sigma)\sigma$ is a homomorphism since for all $\sigma, \tau \in G$ we have

$$\eta(\sigma\tau) = \rho(\sigma\tau)\sigma\tau = \rho(\sigma)\ {}^{\sigma}\rho(\tau)\sigma\tau = \rho(\sigma)\sigma\rho(\tau)\sigma^{-1}\sigma\tau = \rho(\sigma)\sigma\rho(\tau)\tau = \eta(\sigma)\eta(\tau).$$

Thus $\eta$ defines an action of $G$ on $V$. Moreover, this action is semilinear since for $\sigma \in G$, $v \in V$, and $\lambda \in K$, noting that $\rho(\sigma)$ is $K$-linear we have

$$\eta(\sigma)(\lambda v) = \rho(\sigma)\sigma(\lambda v) = \rho(\sigma)(\sigma(\lambda)\sigma(v)) = \sigma(\lambda)\rho(\sigma)(\sigma(v)) = \sigma(\lambda)\eta(\sigma)(v).$$

(3). Since the maps of (1) and (2) are visibly inverse to each other, the first bijection follows upon noting that the maps of (1) and (2) take the distinguished elements to each other. Finally, suppose we have two semilinear actions associated to homomorphisms $\eta, \eta' : G \to \mathrm{Bij}(V)$, and let $\rho$ and $\rho'$ be the corresponding cocycles. Then the actions are isomorphic if and only if there is $\phi \in GL(V)$ with

$$\eta(\sigma) = \phi^{-1}\eta'(\sigma)\phi$$

for all $\sigma \in G$. That is, if and only if there is $\phi \in GL(V)$ such that, for all $\sigma \in G$, we have

$$\rho(\sigma) = \eta(\sigma)\sigma^{-1} = \phi^{-1}\eta'(\sigma)\sigma^{-1}\sigma\phi\sigma^{-1} = \phi^{-1}\rho'(\sigma)\ {}^{\sigma}\phi,$$

i.e. if and only if $\rho$ and $\rho'$ are cohomologous. Thus the first bijection takes the notion of actions being isomorphic to the notion of cocycles being cohomologous, whence the result. □

Now let $A$ be a $K$-algebra and recall that by a semilinear action of $G$ on $A$ we mean one that is semilinear when $A$ is viewed as a $K$-vector space, and additionally preserves the ring structure. Now, similarly to the vector space case, $\mathrm{Aut}_K(A)$ (the group of $K$-algebra automorphisms of $A$) becomes a $G$-group via $\phi \mapsto {}^{\sigma}\phi = \sigma\phi\sigma^{-1}$. Note that for $A = M_n(K)$, the identification of $\mathrm{Aut}_K(M_n(K))$ with $PGL_n(K)$ of Corollary 4.10 carries this action to the usual coefficientwise action on elements of $PGL_n(K)$. We say that two semilinear actions of $G$ on $A$ are *isomorphic* if Definition 6.24 is satisfied for some $\phi \in \mathrm{Aut}_K(A)$. One easily checks that the correspondence of Proposition 6.25 becomes the following.

**Corollary 6.26.** *Let $A$ be a $K$-algebra equipped with a fixed semilinear action. Then the same formulae as (1) and (2) of Proposition 6.25 yield a bijection of pointed sets*

$$\{\text{semiliear actions on } A\} \longleftrightarrow \{1\text{-cocycles } G \to \mathrm{Aut}_K(A)\}$$

*which descends to a bijection of pointed sets*

$$\{\text{semiliear actions on } A\}/\text{iso} \longleftrightarrow H^1\left(G, \mathrm{Aut}_K(A)\right).$$

6.6. **Hilbert's Theorem 90.** The following result is one of the foundational computations in Galois cohomology.

**Theorem 6.27** (Hilbert's theorem 90)**.** *Let $k$ be a field and $K/k$ a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. Then for any $n \geq 1$ we have*

$$H^1\left(G, GL_n(K)\right) = \{\bullet\}$$

*(i.e. it is the one element set consisting of the class of the trivial cocycle).*

*Proof.* We'll work slightly harder than necessary in order to give an conceptual way of thinking about this result. Let $\eta : G \to \mathrm{Bij}(K^n)$ be a semilinear action of $G$ on $K^n$, and denote by ${}_{\eta}K^n$ the $K$-vector space $K^n$ equipped with this action. Then $V = ({}_{\eta}K^n)^G$ is a $k$-vector space and Theorem 6.7 gives an isomorphism $V \otimes_k K \cong K^n$. Moreover, if $\eta$ and $\eta'$ are two isomorphic semilinear actions on $K^n$ then there is a $G$-equivariant $K$-isomorphism $\phi : {}_{\eta}K^n \xrightarrow{\sim} {}_{\eta'}K^n$.

Taking $G$-invariants we obtain an isomorphism of $k$-vector spaces $({}_\eta K^n)^G \cong ({}_{\eta'} K^n)^G$. Thus we have a well-defined map

$$\left\{ \begin{array}{c} \text{semilinear actions on } K^n \\ \text{up to isomorphism} \end{array} \right\} \stackrel{(-)^G}{\longrightarrow} \left\{ \begin{array}{c} \text{iso classes of } k\text{-vector spaces } V \\ \text{such that } V \otimes_k K \cong K^n \end{array} \right\}$$

which is a map of pointed sets if we define $k^n$ to be the distinguished element on the righthand side. It follows formally from the equivalence of categories of Theorem 6.12 that this is a bijection (see the proof of Theorem 6.28 below) however we can cheat slightly in this setting. Note that any $k$-vector space $V$ with $V \otimes_k K \cong K^n$ necessarily has dimension $n$. Since any two $k$-vector spaces of the same dimension are isomorphic, the righthand set consists of a single element: the class of $k^n$. In particular, the map is visibly surjective, since $K^n$ with its standard coordinatewise action maps to $k^n$. To prove injectivity, take semilinear actions $\eta, \eta' : G \to \mathrm{Bij}(K^n)$ and suppose that we have a $k$-isomorphism $\phi : ({}_\eta K^n)^G \stackrel{\sim}{\longrightarrow} ({}_{\eta'} K^n)^G$. Then $\phi \otimes 1$ gives a $G$-equivariant $K$-isomorphism

$$\phi \otimes 1 : ({}_\eta K^n)^G \otimes_k K \stackrel{\sim}{\longrightarrow} ({}_{\eta'} K^n)^G \otimes_k K.$$

However, by Theorem 6.7, $({}_\eta K^n)^G \otimes_k K$ is canonically isomorphic to ${}_\eta K^n$, and similarly for $\eta'$, so that we may view $\phi \otimes 1$ as a $K$-isomorphism from ${}_\eta K^n$ to ${}_{\eta'} K^n$ which is $G$-equivariant also (cf. Remark 6.10). Thus the two actions are isomorphic.

Putting everything together we have bijections of pointed sets

$$\left\{ \begin{array}{c} \text{iso classes of } k\text{-vector spaces } V \\ \text{such that } V \otimes_k K \cong K^n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{semilinear actions on } K^n \\ \text{up to isomorphism} \end{array} \right\} \stackrel{\text{Prop 6.25}}{\longleftrightarrow} H^1(G, GL_n(K))$$

and since we have already seen that the leftmost set consists of a single element, the result follows. □

6.7. **Central simple algebras split by a fixed Galois extension.** Recall that for a field extension $K/k$, $CSA_n(K/k)$ denotes the set of isomorphism classes of central simple algebras of degree $n$ over $k$ which are split by $K/k$. This is a pointed set with the class of $M_n(k)$ being the distinguished element.

**Theorem 6.28.** *Let $K/k$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. Then there is a bijection of pointed sets*

$$CSA_n(K/k) \leftrightarrow H^1(G, PGL_n(K)).$$

*Proof.* The proof follows the strategy of Theorem 6.27. Specifically, let $\eta : G \to \mathrm{Bij}(M_n(K))$ be a semilinear action of $G$ on $M_n(K)$, and denote by ${}_\eta M_n(K)$ the $K$-algebra $M_n(K)$ equipped with this action. Then $A = ({}_\eta M_n(K))^G$ is a central simple algebra over $k$ and Theorem 6.7 gives an isomorphism of $K$-algebras $({}_\eta M_n(K))^G \otimes_k K \cong M_n(K)$, so that $A$ has degree $n$ and is split by $K/k$. Moreover, if $\eta$ and $\eta'$ are two isomorphic semilinear actions on $M_n(K)$ then there is a $G$-equivariant $K$-algebra isomorphism $\phi : {}_\eta M_n(K) \stackrel{\sim}{\longrightarrow} {}_{\eta'} M_n(K)$. Taking $G$-invariants we obtain an isomorphism of $k$-algebras $({}_\eta M_n(K))^G \cong ({}_{\eta'} M_n(K))^G$. Thus we have a well-defined map of pointed sets

$$\left\{ \begin{array}{c} \text{semilinear actions on } M_n(K) \\ \text{up to isomorphism} \end{array} \right\} \stackrel{(-)^G}{\longrightarrow} CSA_n(K/k)$$

which we will show is a bijection. To see that this map is surjective, take a central simple algebra $A/k$ of degree $n$ and split by $K/k$, and fix a $K$-algebra isomorphism $\phi : A \otimes_k K \stackrel{\sim}{\longrightarrow} M_n(K)$. We can use $\phi$ to push the natural semilinear action on $A \otimes_k K$ across to a semilinear action

on $M_n(K)$. Specifically, the new semilinear action on $M_n(K)$ is given by $x \mapsto \phi(\sigma(\phi^{-1}(x)))$ with here the $\sigma$ denotes the action on $A \otimes_k K$. Denote by $\eta : G \to \mathrm{Bij}(M_n(K))$ the associated homomorphism. By construction, $\phi$ gives a $G$-equivariant $K$-algebra isomorphism $A \otimes_k K \xrightarrow{\sim} {}_\eta M_n(K)$. Taking $G$-invariants we obtain a $k$-isomorphism

$$A = (A \otimes_k K)^G \cong ({}_\eta M_n(K))^G.$$

To prove injectivity, take semilinear actions $\eta, \eta' : G \to \mathrm{Bij}(M_n(K))$ and suppose that we have a $k$-isomorphism $\phi : ({}_\eta M_n(K))^G \xrightarrow{\sim} ({}_{\eta'} M_n(K))^G$. Then $\phi \otimes 1$ gives a $G$-equivariant $K$-algebra isomorphism

$$\phi \otimes 1 : ({}_\eta M_n(K))^G \otimes_k K \xrightarrow{\sim} ({}_{\eta'} M_n(K))^G \otimes_k K.$$

However, by Theorem 6.7, $({}_\eta M_n(K))^G \otimes_k K$ is canonically isomorphic to ${}_\eta M_n(K)$, and similarly for $\eta'$, so that we may view $\phi \otimes 1$ as a $G$-equivariant $K$-algebra isomorphism from ${}_\eta M_n(K)$ to ${}_{\eta'} M_n(K)$. Thus the two actions are isomorphic.

Combing this bijection with Proposition 6.25 we obtain bijections of pointed sets

$$CSA_n(K/k) \longleftrightarrow \left\{ \begin{array}{c} \text{semilinear actions on } M_n(K) \\ \text{up to isomorphism} \end{array} \right\} \overset{\text{Prop 6.25}}{\longleftrightarrow} H^1(G, PGL_n(K))$$

and the result follows. □

*Remark* 6.29. If $A$ and $B$ are $K$-algebras equipped with fixed semilinear actions of $G$, then $\mathrm{Hom}_K(A, B)$ becomes a $G$-set via $\phi \mapsto {}^\sigma\phi = \sigma\phi\sigma^{-1}$, where here the leftmost $\sigma$ is the element of $\mathrm{Bij}(B)$ corresponsing to the fixed action on $B$, and the rightmost $\sigma$ is the element of $\mathrm{Bij}(A)$ corresponding to the action on $A$. Unwinding the explicit maps involved in the proof of Theorem 6.28, we see that the map from left to right in the statement is given explicitly as follows. Given a central simple algebra $A/k$ of degree $n$ split by $K/k$, fix a $K$-algebra isomorphism $\phi : A \otimes_k K \xrightarrow{\sim} M_n(K)$. Then $\rho : \sigma \mapsto \phi\, {}^\sigma\phi^{-1}$ is a 1-cocycle with values in $\mathrm{Aut}_K(M_n(K)) = PGL_n(K)$, and the map takes $A$ to the class of $\rho$.

## 7. The reduced norm

In this section, for a field $k$ and $A$ a central simple algebra over $k$, we define the *reduced norm* which is a multiplicative homomorphism

$$\mathrm{Nrd} : A \to k$$

generalising the quaternion norm of Definition Definition 2.7. Specifically, we define this map as follows. Let $K/k$ be a splitting field for $A$ and fix a $K$-algebra isomorphism $\phi : A \otimes_k K \xrightarrow{\sim} M_n(K)$. Then the reduced norm is the composition

$$A \to A \otimes_k K \xrightarrow{\phi} M_n(K) \xrightarrow{\det} K$$

with the first map embedding $A$ into $A \otimes_k K$ via $a \mapsto a \otimes 1$ as usual, and the last map is the determinant. For this definition to make sense we must show that the map above takes values in $k$, and is independent of both the choice of splitting field $K/k$ and the choice of splitting isomorphism $\phi$. This is a fairly straightforward computation, however to place it in a more conceptual framework we begin with a general discussion of norm maps.

## 7.1. **Generalities on norm maps.**

**Definition 7.1.** Let $A$ be a finite dimensional $k$-algebra and $V$ a finitely generated $A$-module. Note that this makes $V$ into a finite dimensional $k$-vector space. Associated to the $A$-module structure is a homomorphism $A \to \mathrm{End}_k(V)$ given by

$$a \mapsto (m \mapsto am).$$

We define the *norm map associated to* $V$ as the composition

$$N_{V/k} : A \longrightarrow \mathrm{End}_k(V) \xrightarrow{\det} k$$

where the last map is the usual matrix determinant. Note that $N_{V/k}$ is a multiplicative homomorphism.

*Remark* 7.2. The usual determinant $\det : M_n(k) \to k$ arises by taking $A = M_n(k)$ and $V = k^n$ (thought of as column vectors) with the usual matrix multiplication.

*Remark* 7.3. In the obvious way one can define the *trace map associated to* $V$ and *characteristic polynomial associated to* $V$.

The norm maps defined above satisfy the following basic properties.

**Lemma 7.4.** *Let $A$ be a finite dimensional $k$-algebra. Then the norm maps satisfy the following properties:*

(1) *If $V$ and $V'$ are two isomorphic finitely generated $A$-modules then*

$$N_{V/k} = N_{V'/k}.$$

(2) *If $V$ and $V'$ are two finitely generated $A$-modules then*

$$N_{V\oplus V'/k}(a) = N_{V/k}(a)N_{V'/k}(a)$$

*for all $a \in A$.*

(3) *Let $V$ be a finitely generated $A$-module and $K/k$ be any field extension, so that $V \otimes_k K$ is a finitely generated $A \otimes_k K$-module. Then (considering $A$ as a subring of $A \otimes_k K$ via $a \mapsto a \otimes 1$ as usual) we have*

$$N_{V\otimes_k K/K}(a) = N_{V/k}(a)$$

*for all $a \in A$.*

*Proof.* (1). Fix an $A$-module isomorphism $\phi : V \xrightarrow{\sim} V'$ and let $\mathcal{B} = \{x_i\}_{i=1}^n$ be a basis for $V$ as a $k$-vector space. Fix $a \in A$ and write

$$ax_i = \sum_{i=1}^{n} m_{ij}x_j \tag{7.5}$$

for some $m_{ij} \in k$, so that, with respect to the basis $\mathcal{B}$, multiplication by $a$ in $\mathrm{End}_k(V)$ is represented by the matrix $M$ whose $i$-$j$th coefficient $m_{ji}$. By definition, $N_{V/k}(a) = \det(M)$. One the other hand, $\{\phi(x_i)\}_{i=1}^n$ is a basis for $V'$ as a $k$-vector space and applying $\phi$ to (7.5) gives

$$a\phi(x_i) = \sum_{i=1}^{n} m_{ij}\phi(x_j),$$

whence $N_{V'/k}(a) = \det(M)$ also.

(2). Fix $k$-vector space bases $\mathcal{B}$ and $\mathcal{B}'$ for $V$ and $V'$ respectively. Fix $a \in A$, and denote by $M$ and $M'$ the matrices representing left multiplication by $a$ on $V$ and $V'$ with respect to these bases, so that $N_{V/k}(a) = \det(M)$ and $N_{V'/k}(a) = \det(M')$. Now the disjoint union $\mathcal{B} \sqcup \mathcal{B}'$ gives a $k$-basis for $V \oplus V'$, with respect to which multiplication by $a$ is represented by the black-diagonal matrix

$$\begin{pmatrix} M & \\ & M' \end{pmatrix}.$$

By definition $N_{V \oplus V'/k}(a)$ is the determinant of this matrix, which is $\det(M)\det(M')$.

(3). Once again, let $\mathcal{B}$ be a basis for $V$ as a $k$-vector space, fix $a \in A$, and let $M$ be the matrix representing left multiplication by $a$ on $V$ with respect to this basis. As usual, $N_{V/k}(a) = \det(M)$. Now $\mathcal{B}$ is also a $K$-basis for $V \otimes_k K$, with respect to which multiplication by $a = a \otimes 1$ on $V \otimes_k K$ is again represented by the matrix $M$. Thus

$$N_{V \otimes_k K/k}(a) = \det(M) = N_{V/k}(a)$$

as desired. □

*Remark* 7.6. Lemma 7.4 remain true with norms replaced by traces and characteristic polynomials, with the caveat that for traces part (2) requires a sum on the righthand side rather than a product.

## 7.2. **Definition and basic properties of the reduced norm.**

**Lemma 7.7.** *Let $A$ be a CSA/$k$, $K/k$ a splitting field and $\phi : A \otimes_k K \xrightarrow{\sim} M_n(K)$ an isomorphism of $K$-algebras. Then the composition*

$$A \otimes_k K \xrightarrow{\phi} M_n(K) \xrightarrow{\det} K$$

*is independent of the choice of $\phi$. If $K/k$ is Galois then it is moreover* $\mathrm{Gal}(K/k)$*-equivariant.*

*Proof.* More conceptually (cf. Remark 7.2) the composition $\det \circ \phi$ of the statement is the norm map $N_{V/K}$ associated to the $V = K^n$ viewed as an $A \otimes_k K$-module via $\phi$. Now $V$ is just the unique simple $A \otimes_k K$-module, so if we pick a different $\phi$ then the resulting $A \otimes_k K$-module structure on $K^n$ is necessarily isomorphic. It follows from Lemma 7.4 (1) that the norm does not depend on the choice of $\phi$.

Now suppose that $K/k$ is Galois. Note (e.g. from its formula in terms of matrix coefficients) that $\det : M_n(K) \to K$ is $\mathrm{Gal}(K/k)$-equivariant for the usual actions of $\mathrm{Gal}(K/k)$ on $M_n(K)$ and $K$. Borrowing ideas from § 6.7 (see Remark 6.29 in particular) let $\rho : \mathrm{Gal}(K/k) \to \mathrm{Aut}_K(M_n(K))$ be the map $\sigma \mapsto \phi\, {}^{\sigma}\phi^{-1}$. Then $\rho$ is a 1-cocycle and $M \mapsto \rho(\sigma)\sigma(M)$ defines a semilinear action of $\mathrm{Gal}(K/k)$ on $M_n(K)$ with respect to which $\phi$ is $\mathrm{Gal}(K/k)$-equivariant. Now, for each $\sigma \in \mathrm{Gal}(K/k)$, it follows from the Skolem–Noether theorem that $\rho(\sigma)$ is conjugation by an element of $GL_n(K)$, say $M_\sigma$. Then for any matrix $M \in M_n(K)$ and any $\sigma \in \mathrm{Gal}(K/k)$ we have

$$\det\left(\rho(\sigma)\sigma M\right) = \det\left(M_\sigma \sigma(M) M_\sigma^{-1}\right) = \det\left(\sigma(M)\right) = \sigma\left(\det(M)\right).$$

Thus $\det : M_n(K) \to K$ is $\mathrm{Gal}(K/k)$-equivariant for the new semilinear action on $M_n(K)$ also. Since $\phi : A \otimes_k K \to M_n(K)$ is $\mathrm{Gal}(K/k)$-equivariant for this action as well, the sought $\mathrm{Gal}(K/k)$-equivariance of the composition follows. □

**Corollary 7.8.** *Let $A$ be a CSA/$k$, $K/k$ a splitting field, and $\phi : A \otimes_k K \xrightarrow{\sim} M_n(K)$ an isomorphism of $K$-algebras. Then the composition*

$$\mathrm{Nrd}_K : A \to A \otimes_k K \xrightarrow{\phi} M_n(K) \xrightarrow{\det} K$$

*(the first map being the usual inclusion $a \mapsto a \otimes 1$) takes values in $k$. The resuting homomorphism $A \to k$ is independent of the choice of splitting field $K/k$.*

*Proof.* First suppose that $K/k$ is Galois. Since by Lemma 7.7 the composition

$$A \otimes_k K \xrightarrow{\phi} M_n(K) \xrightarrow{\det} K$$

is $\mathrm{Gal}(K/k)$-equivariant, we get an induced map

$$A = (A \otimes_k K)^{\mathrm{Gal}(K/k)} \xrightarrow{\det \circ \phi} K^{\mathrm{Gal}(K/k)} = k$$

which is precisely the map $\mathrm{Nrd}_K$ of the statement. In particular, $\mathrm{Nrd}_K$ takes values in $k$.

Next, no longer assuming $K/k$ to be Galois, we claim that if $K'/k$ is another splitting fields for $A$ with $K \subseteq K'$, then $\mathrm{Nrd}_K = \mathrm{Nrd}_{K'}$. Indeed, noting that $M_n(K) \otimes_K K'$ is canonically isomorphic to $M_n(K')$, $\phi \otimes 1$ gives a $K$-algebra isomorphism

$$\phi \otimes 1 : A \otimes_k K' = (A \otimes_K K) \otimes_K K' \xrightarrow{\sim} M_n(K) \otimes_K K' = M_n(K').$$

Under this isomorphism, an element $x \in A$ maps to $\phi(x) \in M_n(K)$ viewed inside $M_n(K')$ instead. In particular, it's clear that $\det((\phi \otimes 1)(x)) = \det(\phi(x))$ which proves the claim.

Now fix a Galois splitting field $K_0/k$, which exists by Corollary 4.40. Let $K/k$ be an arbitrary splitting field and denote by $K'$ the compositum of $K_0$ and $K$.[2] As above we have

$$\mathrm{Nrd}_{K_0} = \mathrm{Nrd}_{K'} = \mathrm{Nrd}_K.$$

In particular, since $\mathrm{Nrd}_{K_0}$ takes values in $k$, so must $\mathrm{Nrd}_K$. Moreover, since $K_0$ was fixed but $K/k$ was arbitrary, this also proves that $\mathrm{Nrd}_K$ does not depend on $K$. □

**Definition 7.9.** Let $A$ be a CSA/$k$ we define the *reduced norm*

$$\mathrm{Nrd} : A \to k$$

to be the homomorphism $\mathrm{Nrd}_K$ of Corollary 7.8 for any choice of splitting field $K/k$ for $A$. As above, this is intrinsic to $A$.

*Remark* 7.10. One can define the *reduced trace* (valued in $k$) and *reduced characteristic polynomial* (valued in $k[t]$) analagously. Again, these constructions are independent of all choices, by the identical argument.

For $A$ a quaternion algebra, we now show that the reduced norm agrees with the quaternion norm.

**Lemma 7.11.** *Suppose* $\mathrm{char}(k) \neq 2$ *and let $A = (a, b)$ be a quaternion algebra over $k$. Then the reduced norm agrees with the quaternion norm of Definition Definition 2.7.*

[2]The compositum of $K_0$ and $K$ only makes sense with respect to a field $L$ containing both of them (and does genuinely depend on the choice of such). If $K_0/k$ and $K/k$ are both algebraic then we may use the algebraic closure $\bar{k}$ to define the compositum, once we have chosen embeddings $K_0 \hookrightarrow \bar{k}$ and $K \hookrightarrow \bar{k}$. In general, we may choose a maximal ideal $\mathfrak{m}$ of $K_0 \otimes_k K$ and take $L = (K_0 \otimes_k K)/\mathfrak{m}$, along with the embeddings induced by the usual inclusions of $K_0$ and $K$ into the tensor product.

*Proof.* As in Theorem 4.19, $K = k(\sqrt{a})/k$ is a splitting field for $A$. Specifically, combining parts (1) and (3) of Lemma 2.8, an isomorphism between $A \otimes_k K$ (which is just $(a,b)$ viewed over $K$) and $M_2(K)$ is the map $\phi$ given by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \; j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \; ij \mapsto \begin{pmatrix} 0 & b\sqrt{a} \\ -\sqrt{a} & 0 \end{pmatrix}.$$

One computes that, for $\alpha, \beta, \gamma, \delta \in k$, the image of $x = \alpha + \beta i + \gamma j + \delta ij$ under $\phi$ is the matrix

$$\begin{pmatrix} \alpha + \beta\sqrt{a} & \gamma b + \delta b\sqrt{a} \\ \gamma - \delta\sqrt{a} & \alpha - \beta\sqrt{a} \end{pmatrix}$$

which has determinant

$$(\alpha + \beta\sqrt{a})(\alpha - \beta\sqrt{a}) - b(\gamma + \delta\sqrt{a})(\gamma - \delta\sqrt{a}) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2.$$

But this is precisely the quaternion norm of $x$. □

*Remark* 7.12. Lemma 7.11 shows that the quaternion norm is intrinsic to the algebra, and not dependent on it's presentation as $(a,b)$ for some $a, b \in k^\times$. This is something we remarked for quaternion division algebras in Remark 2.13 by comparing it to the field norm. See Proposition 7.16 below for a generalisation of this comparison to all central division algebras.

We saw in Proposition 2.11 that the quaternion norm can be used to detect when a quaternion algebra is division. The following proposition shows that the reduced norm does this for arbitrary central simple algebras.

**Proposition 7.13.** *Let $A$ be a CSA/$k$. Then $x \in A$ is invertible if and only if* $\mathrm{Nrd}(x) \neq 0$. *In particular, $A$ is a central division algebra if and only if* Nrd *has no non-trivial zero.*

*Proof.* Let $K/k$ be a Galois splitting field for $A$ and fix an isomorphism of $K$-algebras $\phi : A \otimes_k K \xrightarrow{\sim} M_n(K)$, so that we may compute Nrd as the composition

$$A \to A \otimes_k K \xrightarrow{\phi} M_n(K) \xrightarrow{\det} K.$$

If $x \in A$ is invertible then it maps to an invertible element of $M_n(K)$, which hence has non-zero determinant. Thus $\mathrm{Nrd}(x) \neq 0$. Similarly, if $\mathrm{Nrd}(x) \neq 0$ then the image of $x$ in $M_n(K)$ is invertible whence, as $\phi$ is an isomorphism, $x$ is invertible in $A \otimes_k K$. Since $x$ (viewed in $A \otimes_k K$) is fixed by the action of $\mathrm{Gal}(K/k)$, so must its inverse be. Thus $x^{-1} \in (A \otimes_k K)^{\mathrm{Gal}(K/k)} = A$ and we are done. □

*Remark* 7.14. If one wanted to avoid the use of a Galois splitting field in the above lemma, one could argue via the general result that if $B$ is any $k$-algebra containing $A$, then $x$ is invertible in $A$ if and only if $x$ is invertible in $B$ (define the minimal polynomial of $x$ over $k$ and show that $x$ is invertible if and only if this polynomial has non-zero constant term; the existence of this polynomial crucially uses that $A$ is finite dimensional over $k$).

We close our discussion of the reduced norm by relating it to some other natural norm maps.

7.3. **Comparison between norm maps on central simple algebras.** In what follows, for a finite dimensional $k$-algebra $A$, we write $N_{A/k}$ for the norm arising from viewing $A$ as a module over itself via left multiplication. The following is the reason for the word 'reduced' in reduced norm.

**Lemma 7.15.** *Let $A$ be a CSA/$k$ of degree $n$. Then for any $a \in A$, we have*

$$\mathrm{Nrd}(a)^n = N_{A/k}(a).$$

*Proof.* Let $K/k$ be a splitting field for $A$ and fix an isomorphism of $K$-algebras

$$\phi : A \otimes_k K \xrightarrow{\sim} M_n(K).$$

Via $\phi$, we view both $M_n(K)$ and $V = K^n$ as $A \otimes_k K$-modules. Now by construction, $A \otimes_k K$ (as a module over itself) and $M_n(K)$ are isomorphic $A \otimes_k K$-modules, whilst we have $M_n(K) \cong V^n$ as $A \otimes_k K$-modules. Thus for $a \in A$ we have

$$N_{A/k}(a) = N_{A \otimes_k K/K}(a) = N_{V/K}(a)^n = \mathrm{Nrd}(a)^n$$

the first and second equalities following from Lemma 7.4 and the last equality following immediately from the definition of the reduced norm. □

**Proposition 7.16.** *Let $A$ be a CSA/$k$ of degree $n$, and let $k \subseteq K \subseteq A$ be a field with $[K : k] = n$ (e.g. $A$ could be a central division algebra and $K$ a maximal subfield). Then the restriction of the reduced norm to $K$ is the usual field norm $N_{K/k}$.*

*Proof.* Since $\dim_k A = n^2$ and $[K : k] = n$, as a $K$-vector space we have $A \cong K^n$. We thus have $N_{K/k}^n = N_{A/k}$ and by Lemma 7.15 we deduce that for all $x \in K$ we have

$$N_{K/k}(x)^n = \mathrm{Nrd}(x)^n. \tag{7.17}$$

We can now use a trick to deduce that we in fact have this equality with $n$th powers removed.

Let $k(t)$ be the function field in one variable $t$, and consider the central simple algebra $A \otimes_k k(t)$ over $k(t)$. Now $K \otimes_k k(t) = K(t)$ is a maximal subfield of $A \otimes_k k(t)$, and for $x \in K$ we have by Lemma 7.4 (3) that $N_{K/k}(x) = N_{K(t)/k(t)}(x)$. Consider the element $x + t \in K(t)$. Since $t$ is in the base-field $k(t)$, as an element of $\mathrm{End}_{k(t)}(K(t))$ it acts as $t$id. Fixing a basis for $K/k$ as a $k$-vector space, the same set gives a basis for $K(t)$ as a $k(t)$-vector space, and viewing multiplication by $x + t$ as a matrix with respect to this basis it's clear that the determinant of this matrix is a monic polynomial in $t$, say $P_1(t)$. Evaluating $P_1(t)$ at $t = 0$ recovers $N_{K/k}(x)$.

On the other hand, we may consider the reduced norm associated to $A \otimes_k k(t)$, which by an abuse of notation we also denote by Nrd. Let $F/k$ be a finite extension splitting $A$. Then $F(t) = F \otimes_k k(t)$ is a splitting field for $A \otimes_k k(t)$. Fixing an isomorphism of $F(t)$-algebras

$$\phi : A \otimes_k F(t) \xrightarrow{\sim} M_n(F(t)),$$

the image of $t$ under $\phi$ is once again the matrix $t$id, and again it's clear that the determinant of the matrix $\phi(x + t)$ is a monic polynomial in $t$, $P_2(t)$ say. This time, setting $t = 0$ recovers $\mathrm{Nrd}(x)$. However, applying (7.17) with $K$ and $A$ replaced by $K(t)$ and $A \otimes_k k(t)$ gives

$$P_1(t)^n = P_2(t)^n.$$

Since both polynomials are monic, the only way this can happen is if $P_1(t) = P_2(t)$. Evaluating this polynomial identity at $t = 0$ gives

$$N_{K/k}(x) = \mathrm{Nrd}(x)$$

as desired. □

*Remark* 7.18. If one is permitted to use some more advanced theory then there is a much more satisfactory proof of Proposition 7.16 (which simultaneously proves the same statement for characteristic polynomials rather than just norms). Maintining the notation of the statement, let $F$ be any splitting field for $A$. Then by Lemma 7.4 (3), for any $x \in K$ we have

$$N_{K/k}(x) = N_{K \otimes_k F/F}(x).$$

Fixing an $F$-algebra isomorphism

$$\phi : A \otimes_k F \xrightarrow{\sim} M_n(F)$$

we can use $\phi$ to make $F^n$ into a module over $K \otimes_k F$. By definition we then have

$$\mathrm{Nrd}(x) = N_{F^n/F}(x).$$

Since both $K \otimes_k F$ and $F^n$ are $F$-vector spaces of dimension $n$, it is natural to ask if they are isomorphic as $K \otimes_k F$-modules. If this were true then we would have the desired equality of norms by Lemma 7.4 (1). In general, for arbitrary $F$, modules over $K \otimes_k F$ can be fairly complicated and I do not know if the proposed isomorphism holds in general. However, we are at liberty to choose a particular $F$ and with a careful choice we can get everything to work. Specifically, in [Ami55] (see Theorem 9.1 in particular), Amitsur constructs, for any central simple algebra $A$ over $k$, a splitting field $F$ for $A$ which has transcendence degree $n-1$ over $k$ and such that $F/k$ is a regular extension (the existence of such a field is not surprising, in geometric language it is the function field of the *Severi–Brauer variety* associated to $A$, see e.g. [GS06, Section 5] for more information; the fact that it is a regular extension is a consequence of the Severi–Brauer variety being geometrically integral). In particular, $\bar{k}$ and $F$ are linearly disjoint and it follows that $L = K \otimes_k F$ is a field. Thus having the same finite $F$-dimension, $L$ and $F^n$ are necessarily isomorphic as $L$-modules, and we are done.

*Remark* 7.19. The existence of the field $F$ in the previous remark can also be used to circumvent the use of Galois theory in showing that the reduced norm takes values in $k$. Specifically, for a central simple algebra $A$ take $K/k$ any finite extension splitting $A$, and let $F/k$ be the field of Remark 7.18. Then $k$ is algebraically closed in $F$, whilst $K/k$ is algebraic. In particular, inside any extension containing both $F$ and $K$ we have $F \cap K = k$. However, arguing as in Corollary 7.8, the reduced norm takes values in this intersection.

## Part 2. Group cohomology

### 8. Introduction

Let $G$ be a finite group (finiteness will not be necessary, but usually in the infinite case different variants of group cohomology are used, of which more later) and let $M$ be a $G$-module. That is, an abelian group $M$ on which $G$ acts $\mathbb{Z}$-linearly. To the pair $(G, M)$ we'll associate abelian groups $H^i(G, M)$ for each $i \geq 0$, the *ith (group-) cohomology groups*. In a sense that can be made precise via the theory of classifying spaces these can be thought of as being analagous to the way that one associates (singuar) cohomology groups $H^i(X, A)$ to a topological space $X$ and coefficient system $A$. Like singular cohomology of topological spaces, these cohomology groups can be complicated to compute in specific examples but have several good 'functorial' properties which facilitate 'new-from-old' computations. For example, we'll see that:

(1) For any $G$-module $M$ we have

$$H^0(G, M) = M^G = \{m \in M \mid gm = m \ \forall g \in G\}.$$

(2) A homomorphism of $G$-modules (i.e. a homomorphism of abelian groups commuting with the $G$-action) $M \to M'$ induces (functorially) a homomorphism $H^i(G, M) \to H^i(G, M')$ for each $i$.

(3) Given a short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

of $G$-modules (i.e. a short exact sequence of abelian groups in which all maps are $G$-module homomorphisms) there is a long exact sequence of cohomology

$$\begin{array}{l} 0 \longrightarrow M_1^G \longrightarrow M_2^G \longrightarrow M_3^G \longrightarrow \\ \quad H^1(G, M_1) \longrightarrow H^1(G, M_2) \longrightarrow H^1(G, M_3) \longrightarrow \\ \quad H^2(G, M_1) \longrightarrow H^2(G, M_2) \longrightarrow H^2(G, M_3) \longrightarrow \cdots . \end{array}$$

(4) If $H$ is a subgroup of $G$ and $M$ a $G$-module, then there are *restriction* and *corestriction* maps

$$\mathrm{res} : H^i(G, M) \to H^i(H, M)$$

and

$$\mathrm{cor} : H^i(H, M) \to H^i(G, M)$$

for each $i$ (if $G$ is not finite, the corestriction map needs $H$ to have finite index in $G$). If moreover $H$ is normal in $G$ then there is an *inflation* map

$$\mathrm{inf} : H^i(G/H, M^H) \to H^i(G, M).$$

(5) For each $i \geq 0, j \geq 0$ and $G$-modules $M$ and $N$ there are cup-product maps

$$\cup : H^i(G, M) \times H^i(G, N) \to H^{i+j}(G, M \otimes N)$$

(here and in the rest of this section, '$\otimes$' without a subscript denotes tensor product over $\mathbb{Z}$, and given $G$-modules $M$ and $N$, we make $M \otimes N$ into a $G$-module with the action of $g \in G$ given by $g \cdot (m \otimes n) = gm \otimes gn$). If $M = R$ is a ring such that the multiplication map $R \otimes R \to R$ is $G$-equivariant (e.g. if the action is trivial) then

$$H^*(G, R) = \bigoplus_{i \geq 0} H^i(G, R)$$

inherits from the cup-product the structure of a graded-commutative ring.

There is also an analagous theory of *Group homology*, which assigns to the pair $G$ and $M$ abelian groups $H_i(G, M)$ for each $i \geq 0$. In the case that $G$ acts trivially on $M$, like in topology, the *universal coefficient theorem* relates these to cohomology groups: there is short exact sequence

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}\left(H_{i-1}(G, \mathbb{Z}), M\right) \longrightarrow H^i(G, M) \longrightarrow \mathrm{Hom}\left(H_i(G, \mathbb{Z}), M\right) \to 0.$$

After developing the basic theory of group cohomology we'll apply it to the study of Brauer groups. Specifically, let $k$ be a field and $K/k$ a finite Galois extension. Then we'll see that the subgroup of the Brauer group of $k$ consisting of elements split by $K$ may be described as the cohomology group $H^2(\mathrm{Gal}(K/k), K^\times)$ (with $K^\times$ carrying its natural Galois action), and there is also an analogue of this for the full Brauer group. This allows us to bring the full machinery of group cohomology to bear on the study of Brauer groups.

## 9. Some homological algebra (UNDER DEVELOPMENT)

Throughout this section $R$ denotes a (possibly noncommutative) ring. All maps are $R$-module homomorphisms unless stated otherwise.

9.1. **Projective modules.** In this section we will be concerned with the functor $\mathrm{Hom}_R(M,-)$ for a fixed $R$-module $M$. To see that this is a functor, note that if $f : M_1 \to M_2$ is an $R$-module homomorphisms, then we have a homomorphism $\tilde{f} : \mathrm{Hom}_R(M, M_1) \to \mathrm{Hom}_R(M, M_2)$ given by $\phi \mapsto f \circ \phi$.

**Lemma 9.1.** *For any $R$-module $M$, the functor $\mathrm{Hom}_R(M,-)$ is left exact. That is, for any exact sequence*

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$$

*of $R$-modules, the sequence*

$$0 \longrightarrow \mathrm{Hom}_R(M, M_1) \xrightarrow{\tilde{f}_1} \mathrm{Hom}_R(M, M_2) \xrightarrow{\tilde{f}_2} \mathrm{Hom}_R(M, M_3) \qquad (\dagger)$$

*is exact also.*

*Proof.* First take $\phi \in \mathrm{Hom}_R(M, M_1)$ such that $0 = \tilde{f}_1(\phi) = f_1 \circ \phi$. Since $f_1$ is injective, the only way the composition can be zero is if $\phi$ itself is zero, thus $(\dagger)$ is injective on the left. Moreover, the composition $\tilde{f}_2 \circ \tilde{f}_1$ sends $\phi \in \mathrm{Hom}_R(M, M_1)$ to $(f_2 \circ f_1) \circ \phi$. By exactness of the initial sequence we have $f_2 \circ f_1 = 0$ so that $\tilde{f}_2 \circ \tilde{f}_1 = 0$, or in other words $\mathrm{im}(\tilde{f}_1) \subseteq \ker(\tilde{f}_2)$. Finally, suppose $\phi \in \ker(\tilde{f}_2)$, so that $f_2 \circ \phi = 0$. Then $\mathrm{im}(\phi) \subseteq \ker(f_2) = \mathrm{im}(f_1)$. Since the initial sequence is injective on the left, $f_1$ is invertible when restricted to its image. Then

$$\phi' = \left(f_1|_{\mathrm{im}(f_1)}\right)^{-1} \circ \phi : M \to M_1$$

maps to $\phi$ under $\tilde{f}_1$, showing that $\ker(\tilde{f}_2) \subseteq \mathrm{im}(\tilde{f}_1)$ and completing the proof that $(\dagger)$ is exact. □

**Definition 9.2.** An $R$-module $P$ is *projective* if for every surjection $\pi : M \to M'$ of $R$-modules, any homomorphism $\gamma : P \to M'$ lifts to a homomorphism $\gamma' : P \to M$ such that $\gamma = \pi \circ \gamma'$. Put another way, in any diagram of the shape below for which the bottom row is exact, we can always find a map fitting along the dotted line making the diagram commute[3]

$$\begin{array}{ccccc} & & & & P \\ & & \overset{\exists \gamma'}{\swarrow} & & \downarrow \gamma \\ M & \xrightarrow{\pi} & M' & \longrightarrow & 0. \end{array}$$

*Remark* 9.3. An $R$-module $P$ is projective if and only if the functor $\mathrm{Hom}_R(P,-)$ is exact. Indeed, another way of writing the lifting property of Definition 9.2 is that, for any surjection $\pi : M \to M'$ of $R$-modules, the map

$$\tilde{\pi} : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M')$$

is surjective (here as usual, for $\phi \in \mathrm{Hom}_R(P, M)$ we set $\tilde{\pi}(\phi) = \pi \circ \phi$). Since, as in Lemma 9.1, the functor $\mathrm{Hom}_R(P,-)$ is left exact without any assumptions on $P$, $\mathrm{Hom}_R(P,-)$ is exact if and only if the lifting property holds for $P$.

**Lemma 9.4.** *A free $R$ module is projective.*

[3]We make no claim about the uniqueness of such a map; when one exists there are often many.

*Proof.* Let $P$ be a free $R$-module and $S = \{p_i\}_{i\in I}$ a basis for $P$. Now given a surjection $\pi : M \to M'$ and a homomorphism $\gamma : P \to M'$, pick, for each $i \in I$, an arbitrary lift $m_i$ of $\gamma(p_i)$. Then the map $\gamma' : P \to M$ given by sending each $p_i$ to $m_i$ and extending $R$-linearly gives the sought lifting of $\gamma$. □

*Remark* 9.5. That free modules are projective proves the important fact that any $R$-module $M$ is a quotient of a projective module. Indeed, picking any generating set $S = \{m_i\}_{i\in I}$ for $M$, the map $\oplus_{i\in I} R \to M$ sending 1 in the $i$-th factor to $m_i$ (and extending $R$-linearly) gives a surjection from a free (and in particular projective) module to $M$.

**Proposition 9.6.** *Let $P$ be an $R$-module. Then the following are equivalent:*

(1) *$P$ is projective,*
(2) *every short exact sequence*

$$0 \to M' \to M \to P \to 0$$

*of $R$-modules splits*[4]*,*
(3) *$P$ is a direct summand of a free module.*

*Proof.* (1)⇒ (2). Since $P$ is projective we may split the sequence by lifting the identity map $P \to P$ to a map $P \to M$. (2)⇒ (3). Let $S = \{p_i\}_{i\in I}$ be a generating set for $P$ as an $R$-module (e.g. we can just take $S$ to consist of all elements of $P$). Then we have a natural surjection $\bigoplus_{i\in I} R \to P$ sending $1 \in R$ in the $i$-th summand corresponding to $p_i$ (and extending $R$-linearly). Letting $K$ be the kernel we have a short exact sequence

$$0 \to K \to \bigoplus_{i\in I} R \to P \to 0.$$

By assumption this sequence splits, whence

$$\bigoplus_{i\in I} R = K \oplus P$$

and we are done. (3)⇒(1). Let $\pi : M \to M'$ be a surjection of $R$-modules and $\gamma : P \to M'$ a homomorphism. Write $P \oplus N = F$ where $F$ is a free module, and write $p : F \to P$ for the projection onto $P$. By Lemma 9.4 $F$ is projective, so we may lift the composition $\gamma\circ p : F \to M$ to a map $(\gamma \circ p)' : F \to M'$. Denoting by $i : P \to F$ for the inclusion of $P$ into $F$ (sending $x \in P$ to $(x, 0)$), the composition $\gamma' = (\gamma \circ p)' \circ i$ gives the desired of $\gamma$ to $M$. □

9.2. **Injective modules.** Here we essentially repeat § 9.1 but this time for the (contravariant) functor $\mathrm{Hom}_R(-, M)$ for a fixed $R$-module $M$ (i.e. we have swapped the 'slot' that $M$ appears in). This leads to the notion of injective modules as opposed to projective modules. This time, give an $R$-module homomorphism $f : M_1 \to M_2$ then we have a homomorphism $\tilde{f} : \mathrm{Hom}_R(M_2, M) \to \mathrm{Hom}_R(M_1, M)$ give by $\phi \mapsto \phi \circ f$.

**Lemma 9.7.** *For any $R$-module $M$, the functor $\mathrm{Hom}_R(-, M)$ is left exact. That is, for any exact sequence*

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

[4]We say a short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *splits* if the map $g : B \to C$ admits a section, i.e. if there is a map $s : C \to B$ such that $g \circ s = \mathrm{id}_C$. If this is the case then $B \cong A \oplus C$ via the map sending $(a, c) \in A \oplus C$ to $f(a) + s(c)$.

*of $R$-modules, the sequence*

$$0 \longrightarrow \mathrm{Hom}_R(M_3, M) \xrightarrow{\tilde{f}_2} \mathrm{Hom}_R(M_2, M) \xrightarrow{\tilde{f}_1} \mathrm{Hom}_R(M_1, M) \qquad (\dagger)$$

*is exact also.*

*Proof.* First suppose that $\phi \in \mathrm{Hom}_R(M_3, M)$ is such that $0 = \tilde{f}_2(\phi) = \phi \circ f_2$. Since $f_2$ is surjective, the only way the composition can be zero is if $\phi$ itself is zero, thus $(\dagger)$ is injective on the left. Moreover, the composition $\tilde{f}_1 \circ \tilde{f}_2$ sends $\phi \in \mathrm{Hom}_R(M_3, M)$ to $\phi \circ (f_2 \circ f_1) = 0$ so that $\mathrm{im}(\tilde{f}_2) \subseteq \ker(\tilde{f}_1)$. Finally, suppose $\phi \in \ker(\tilde{f}_1)$, so that $\phi \circ f_1 = 0$. Then $\ker(\phi) \supseteq \mathrm{im}(f_1) = \ker(f_2)$. Thus $\phi$ factors through

$$M_2/\ker(f_2) \xrightarrow{\sim} \mathrm{im}(f_2) = M_3.$$

The induced map $\bar{\phi} : M_3 \to M$ then maps to $\phi$ under $\tilde{f}_2$ and exactness of $(\dagger)$ follows. □

**Definition 9.8.** An $R$-module $I$ is *injective* if for every injection $i : M \to M'$ of $R$-modules, any homomorphism $\gamma : M \to I$ extends to a homomorphism $\gamma' : M' \to I$ such that $\gamma = \gamma' \circ i$. That is, in any diagram of the shape below for which the bottom row is exact, we can always find a map fitting along the dotted line making the diagram commute[5]

$$\begin{array}{ccccc} & & & & I \\ & & & \overset{\gamma}{\nearrow} & \uparrow{\scriptstyle \exists \gamma'} \\ 0 & \longrightarrow & M & \xrightarrow{i} & M'. \end{array}$$

*Remark* 9.9. Another way of phrasing the extension property of Definition 9.8 is that for any injection $i : M \to M'$ of $R$-modules, the 'restriction' map

$$\tilde{i} : \mathrm{Hom}_R(M', I) \to \mathrm{Hom}_R(M, I)$$

is surjective. In particular, in light of the left exactness of the functor $\mathrm{Hom}_R(-, I)$ for $I$ arbitrary, it's clear that an $R$-module $I$ is injective if and only if the functor $\mathrm{Hom}_R(-, I)$ is exact.

## 9.3. **The Snake Lemma.**

**Lemma 9.10** (Snake Lemma)**.** *Suppose we have a commutative diagram of $R$-modules*

$$\begin{array}{ccccccc} & & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \longrightarrow 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 \end{array}$$

*whose rows are exact. Then there is an exact sequence of $R$-modules*

$$\ker(f_1) \to \ker(f_2) \to \ker(f_3) \xrightarrow{\delta} \mathrm{coker}(f_1) \to \mathrm{coker}(f_2) \to \mathrm{coker}(f_3)$$

*with all maps induced by those in the initial diagram, with the exception of $\delta$ which is defined as follows. Given $m \in \ker(f_3)$ lift $m$ to $\tilde{m} \in M_2$. Then $f_2(\tilde{m}) \in N_2$ maps to $0$ in $N_3$ (since by commutativity of the diagram, its image in $N_3$ is $f_3(m) = 0$). Thus $f_2(\tilde{m})$ is the image of a unique $x \in N_1$. We define $\delta(m)$ to be the class of $x$ in* $\mathrm{coker}(f_1)$.

[5]Again, we make no claim about the uniqueness of such an extension.

*Proof.* We first check that the map $\delta$ is well defined. Fix $m \in \ker(f_3)$ and let $\tilde{m}$ and $\tilde{m}'$ be two lifts of $m$ to $M_2$. Then

$$\tilde{m}' - \tilde{m} \in \ker(M_2 \to M_3) = \operatorname{im}(M_1 \to M_2).$$

Writing $\alpha$ for the map from $M_1 \to M_2$ we have $\tilde{m}' = \tilde{m} + \alpha(n)$ for some $n \in M_1$. Denoting by $x$ the unique element of $N_1$ mapping to $f_2(\tilde{m})$, by commutativity of the diagram we find that the unique element of $N_1$ mapping to $f_2(\tilde{m}')$ is $x + f_1(n)$. Since $x$ and $x + f_1(n)$ have the same class in $\operatorname{coker}(f_1)$, $\delta$ is well defined. Having shown that $\delta$ is a well defined function $\ker(f_3) \to \operatorname{coker}(f_1)$, it's now easy to check that it is in fact an $R$-module homomorphism.

That the sequence is exact as claimed is now a straightforward check, which we omit. □

*Remark* 9.11. In the statement of the Snake Lemma, if the map $M_1 \to M_2$ is injective then so is the map $\ker(f_1) \to \ker(f_2)$. Similarly, if the map $N_2 \to N_3$ is surjective, so is that map $\operatorname{coker}(f_2) \to \operatorname{coker}(f_2)$. In particular, a commutative diagram of $R$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

with exact rows induces an exact sequence

$$0 \to \ker(f_1) \to \ker(f_2) \to \ker(f_3) \xrightarrow{\delta} \operatorname{coker}(f_1) \to \operatorname{coker}(f_2) \to \operatorname{coker}(f_3) \to 0.$$

9.4. **Chain complexes.**

9.5. **Projective and injective resolutions.**

9.6. **Ext functors.**

## 10. The basics of Group cohomology

Let $G$ be a group (in most applications this will be finite, though we do not assume this). In what follows, unless stated otherwise, we always view $\mathbb{Z}$ as a $G$-module with trivial action (i.e. by making every element of $G$ act as the identity).

10.1. **The group ring.**

**Definition 10.1.** The *group ring* $\mathbb{Z}[G]$ is the free $\mathbb{Z}$-module generated by the elements of $G$, with multiplication induced by the usual group multiplication $g \cdot g' = gg'$ on the generators.

*Remark* 10.2. The ring $\mathbb{Z}[G]$ is associative and has unit the identity element of $G$, but is commutative if and only if $G$ is abelian. Note that a module over $\mathbb{Z}[G]$ is precisely a $G$-module in the sense of Definition 6.17 (given a $G$-module $X$ we extend the action of $G$ to $\mathbb{Z}[G]$ by linearity; this makes $X$ into a $\mathbb{Z}[G]$-module). Similarly, a homomorphism of $G$-modules is precisely the same data as a $G$-equivariant homomorphism of abelian groups.

*Remark* 10.3. Note that $\mathbb{Z}[G] \cong \mathbb{Z}[G]^{\mathrm{opp}}$ via $g \mapsto g^{-1}$.

**Definition 10.4.** We define the *augmentation ideal* $I_G$ to be the kernel of the ring homomorphism

$$\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$$

sending each $g \in G$ to 1 and extending linearly.

*Remark* 10.5. The augmentation ideal is generated (as an abelian group even) by the elements $g-1$ for $g \in G$. Indeed, clearly everything of this form is in $I_G$, and if $x = \sum_{g\in G} \lambda_g g \in I_G$ then $\sum_{g\in G} \lambda_g = 0$ so that $x = \sum_{g\in G} \lambda_g(g-1)$.

**Notation 10.6.** To lighten notation, for $G$-modules $M$ and $N$ we write $\mathrm{Hom}_G(M,N)$ for the (abelian group of) $\mathbb{Z}[G]$-module homomorphisms for $M$ to $N$.

Since it will be usual later, we record the following observation.

**Lemma 10.7.** *For any $G$-module $M$, evaluation at $1 \in \mathbb{Z}$ gives an isomorphism of abelian groups*

$$\mathrm{Hom}_G(\mathbb{Z}, M) \xrightarrow{\sim} M^G.$$

*(Here $M^G$ denotes the subgroup of $M$ consisting of elements invariant under the $G$-action.)*

*Proof.* As $\mathbb{Z}$ is free of rank 1 as an abelian group, evaluation at 1 gives an isomorphism between $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M)$ and $M$. Now note that, since $G$ acts trivially on $\mathbb{Z}$, a homomorphism of abelian groups $\mathbb{Z} \to M$ is $G$-equivariant if and only if the image of 1 is $G$-invariant, i.e. is in $M^G$. □

In light of this lemma, for a $G$-module $M$ we will frequently identify $\mathrm{Hom}_G(\mathbb{Z}, M)$ with $M^G$ in what follows.

10.2. **The standard resolution.** We now construct a canonical free (and hence projective) resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module.

For each $n \geq 0$, we make $\mathbb{Z}[G^{n+1}]$ into a $G$-module via $g \cdot (g_0, ..., g_n) = (gg_0, ..., gg_n)$.

**Lemma 10.8.** *For each $n \geq 0$ we have*

$$\mathbb{Z}[G^{n+1}] = \bigoplus_{g_1,...,g_n} \mathbb{Z}[G](1, g_1, g_2, ..., g_n).$$

*In particular, $\mathbb{Z}[G^{n+1}]$ is a free $\mathbb{Z}[G]$-module.*

*Proof.* It's clear that the set $S = \{(1, g_1, ..., g_n) \mid g_1, ..., g_n \in G\}$ spans $\mathbb{Z}[G^{n+1}]$ as a $\mathbb{Z}[G]$-module, since for any $g_0, ..., g_n \in G$ we have

$$(g_0, ..., g_n) = g_0(1, g_0^{-1}g_1, ..., g_0^{-1}g_n)$$

and elements of this form span $\mathbb{Z}[G^{n+1}]$ as a $\mathbb{Z}$-module. Moreover, using $\mathbb{Z}$-linear independence of the elements $(g_0, ..., g_n)$ as we vary over $g_0, ..., g_n \in G$, one easily checks that $S$ is $\mathbb{Z}[G]$-linearly independent. □

*Remark* 10.9. It will be useful for later to rewrite this basis slightly. Note that the set of all elements of $G^{n+1}$ with first coordinate 1 is precisely the set

$$\{(1, g_1, g_1g_2, ..., g_1g_2...g_n) \mid g_1, ..., g_n \in G\}.$$

Thus by the lemma this set gives a basis for $\mathbb{Z}[G^{n+1}]$ as a $\mathbb{Z}[G]$-module.

**Definition 10.10.** For each $i \geq 0$, define $d_i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$ be setting

$$\partial_i(g_0, ..., g_i) = \sum_{j=0}^{i} (-1)^j (g_0, ..., g_{j-1}, g_{j+1}, ..., g_i)$$

and extending $\mathbb{Z}$-linearly. Note that this is $G$-equivariant, so that $d_i$ is a $G$-module homomorphism. Note that $\partial_0$ is just the map $\epsilon$ whose kernel is the augmentation ideal.

**Proposition 10.11.** *The complex*

$$\cdots \xrightarrow{\partial_{i+1}} \mathbb{Z}[G^{i+1}] \xrightarrow{\partial_i} \mathbb{Z}[G^i] \xrightarrow{\partial_{i-1}} \cdots \xrightarrow{\partial_1} \mathbb{Z}[G] \xrightarrow{\partial_0} \mathbb{Z} \longrightarrow 0$$

*gives a free (and in particular projective) resolution of* $\mathbb{Z}$ *as a* $\mathbb{Z}[G]$*-module.*

*Proof.* Each term is free by Lemma 10.8 so we just need to prove exactness of the sequence. We first check that it is indeed a complex, i.e. that $d_{i-1}d_i = 0$. Clearly it suffices to check this on each of the basis elements $(g_0, ..., g_i)$. To ease notation we write $(g_0, ..., \hat{g_j}, ..., g_i)$ to indicate that we have removed $g_j$. Then for all $0 \leq j \leq i$ we have

$$\partial_{i-1}(g_0, ..., \hat{g_j}, ..., g_i) = \sum_{k<j}(-1)^k(g_0, ..., \hat{g_k}, ..., \hat{g_j}, ..., g_i) + \sum_{k>j}(-1)^{k-1}(g_0, ..., \hat{g_j}, ..., \hat{g_k}, ..., g_i).$$

Thus

$$\begin{aligned}\partial_{i-1}\partial_i(g_0, ..., g_i) &= \sum_{j=0}^{i}(-1)^j d_{i-1}(g_0, ..., \hat{g_j}, ..., g_i) \\ &= \sum_{k<j}(-1)^{j+k}(g_0, ..., \hat{g_k}, ..., \hat{g_j}, ..., g_i) + \sum_{k>j}(-1)^{j+k-1}(g_0, ..., \hat{g_j}, ..., \hat{g_k}, ..., g_i).\end{aligned}$$

Relabelling indices in the second sum we find

$$\partial_{i-1}\partial_i(g_0, ..., g_i) = \sum_{k<j}(-1)^{j+k}(g_0, ..., \hat{g_k}, ..., \hat{g_j}, ..., g_i) - \sum_{k<j}(-1)^{j+k}(g_0, ..., \hat{g_k}, ..., \hat{g_j}, ..., g_i) = 0$$

as desired.

Now fix $s \in G$ and use it to define, for each $i \geq 0$, maps $h_i : \mathbb{Z}[G^i] \to \mathbb{Z}[G^{i+1}]$ by setting

$$h_i\left((g_0, ..., g_{i-1})\right) = (s, g_0, ..., g_{i-1})$$

and extending $\mathbb{Z}$-linearly (this map is not $G$-equivariant, but it shall not matter). We claim that, for all $i \geq 0$, $h_i\partial_i + \partial_{i+1}h_{i+1} = 1$ as an endomorphism of $\mathbb{Z}[G^{i+1}]$ (note that it's clear that the same formula, suitably interpreted, also holds as a map from $\mathbb{Z}$ to itself). Again, it suffices to check this on basis elements $(g_0, ..., g_i)$. We now compute

$$h_i\partial_i(g_0, ..., g_i) = \sum_{j=0}^{i}(-1)^j(s, g_0, ..., \hat{g_j}, ..., g_i)$$

whilst

$$\partial_{i+1}h_{i+1}(g_0, ..., g_i) = (g_0, ..., g_i) + \sum_{j=0}^{i}(-1)^{j+1}(s, g_0, ..., \hat{g_j}, ..., g_i)$$

and summing the two expressions gives the claim.

To conclude, since the sequence is a complex we have $\mathrm{im}(\partial_{i+1}) \subseteq \ker(\partial_i)$ for each $i$. To show the reverse inclusion, fix $x \in \ker \partial_i$. Then hittiting this with $h_i\partial_i + \partial_{i+1}h_{i+1}$, the claim gives

$$x = (h_i\partial_i + \partial_{i+1}h_{i+1})(x) = \partial_{i+1}(h_{i+1}(x))$$

where $x$ is in the image of $\partial_{i+1}$. Thus $\mathrm{im}(\partial_{i+1}) = \ker(\partial_i)$ and the sequence is exact. □

*Remark* 10.12. In the above proof, as another way of phrasing the last step, note that the equation $h\partial + \partial h = 1$ is saying that, for the complex in question, $h$ is a chain homotopy (as a complex of abelian groups since $h$ is not $G$-equivariant) between the 0 map and the identity map. Since chain homotopic maps induce the same maps on homology, the identity map is equal to the zero map on all homology groups of the complex. Thus all homology groups are zero and the sequence is exact.

10.3. **Definition of group cohomology.**

**Definition 10.13.** Let $M$ be a $G$-module. First consider the complex

$$\cdots \xrightarrow{\partial_3} \mathbb{Z}[G^3] \xrightarrow{\partial_2} \mathbb{Z}[G^2] \xrightarrow{\partial_1} \mathbb{Z}[G] \longrightarrow 0$$

obtained from the one of Proposition 10.11 by removing $\mathbb{Z}$ on the right. Applying $\mathrm{Hom}_G(-, M)$ to this sequence we obtain a complex of abelian groups

$$0 \longrightarrow \mathrm{Hom}_G\left(\mathbb{Z}[G], M\right) \xrightarrow{\tilde{\partial}_1} \mathrm{Hom}_G\left(\mathbb{Z}[G^2], M\right) \xrightarrow{\tilde{\partial}_2} \mathrm{Hom}_G\left(\mathbb{Z}[G^3], M\right) \xrightarrow{\tilde{\partial}_3} \cdots$$

where $\tilde{\partial}_i$ takes $\phi \in \mathrm{Hom}_G\left(\mathbb{Z}[G^i], M\right)$ to the composition $\phi \circ \partial_i \in \mathrm{Hom}_G\left(\mathbb{Z}[G^{i+1}], M\right)$.

We define the *$i$-th cohomology group of $G$ with coefficients in $M$*, denoted $H^i(G, M)$, to be the $i$-cohomology group of this complex. That is, we define

$$H^i(G, M) = \ker(\tilde{\partial}_{i+1})/\mathrm{im}(\tilde{\partial}_i).$$

*Remark* 10.14. Since the complex of Proposition 10.11 is a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module, we have

$$H^i(G, M) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

In particular, as the same is true for Ext groups, we can use any projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module in place of the standard resolution, and the resulting cohomology groups will be canonically isomorphic to the ones above.

*Remark* 10.15. It's a general fact about Ext groups that we could instead have computed group cohomology by: taking an injective resolution

$$0 \to M \to I_0 \to I_1 \to I_2 \to \cdots$$

of $M$ as a $\mathbb{Z}[G]$-module, applying the functor $\mathrm{Hom}_G(\mathbb{Z}, -)$ to the complex formed by removing the $M$ on the left to get the complex

$$0 \to \mathrm{Hom}_G(\mathbb{Z}, I_0) \to \mathrm{Hom}_G(\mathbb{Z}, I_1) \to \mathrm{Hom}_G(\mathbb{Z}, I_2) \to \cdots$$

and then computing $H^i(G, M)$ as the cohomology of this sequence. By Lemma 10.7, this is precisely saying that we can compute $H^i(G, M)$ as the cohomology of the complex

$$0 \to (I_0)^G \to (I_1)^G \to (I_2)^G \to \cdots.$$

In otherwords, the groups $H^i(G, -)$ are the *right derived functors* of the $G$-invariants functor.

**Lemma 10.16.** *For any $G$-module $M$ we have (canonically)*

$$H^0(G, M) \cong M^G.$$

*Proof.* By definition we have $H^0(G, M) = \ker(\tilde{\partial}_1)$. Consider the exact sequence

$$\mathbb{Z}[G^2] \xrightarrow{\partial_1} \mathbb{Z}[G] \xrightarrow{\partial_0} \mathbb{Z} \longrightarrow 0$$

given by truncating the standard resolution. Applying $\mathrm{Hom}_G(-, M)$ to this yields the sequence

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, M) \xrightarrow{\tilde{\partial}_0} \mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{\tilde{\partial}_1} \mathrm{Hom}_G\left(\mathbb{Z}[G^2], M\right). \qquad (\dagger)$$

It's a general fact that for any ring $R$ and $R$-module $N$, the functor $\mathrm{Hom}_R(-, N)$ is left exact, so that the sequence (†) is in fact exact also.[6] Thus

$$H^0(G, M) = \ker(\tilde{\partial}_1) = \mathrm{im}(\tilde{\partial}_0) \cong \mathrm{Hom}_G(\mathbb{Z}, M)$$

and we conclude by Lemma 10.7. □

10.4. **Long exact sequence for cohomology.**

**Proposition 10.17.** *We have:*

(1) *If $f : M \to M'$ is a homomorphism of $G$-modules then there is an induced homomorphism $\tilde{f} : H^i(G, M) \to H^i(G, N)$. This is functorial in the sense that given also $f' : M' \to M''$, we have $\widetilde{f' \circ f} = \tilde{f}' \circ \tilde{f}$.*

(2) *Suppose we have a short exact sequence of $G$-modules*

$$0 \to M_1 \longrightarrow M_2 \longrightarrow M_3 \to 0.$$

*Then we have a long exact sequence of cohomology groups*

$$\begin{array}{l} 0 \longrightarrow M_1^G \longrightarrow M_2^G \longrightarrow M_3^G \longrightarrow \\ \quad H^1(G, M_1) \longrightarrow H^1(G, M_2) \longrightarrow H^1(G, M_3) \longrightarrow \\ \quad H^2(G, M_1) \longrightarrow H^2(G, M_2) \longrightarrow H^2(G, M_3) \longrightarrow \cdots. \end{array}$$

*We denote the maps $H^i(G, M_3) \to H^{i+1}(G, M_1)$ by $\delta_i$ (or just by $\delta$ if the index is understood) and refer to them as the* boundary homomorphism.

(3) *The sequence of (2) is natural in the sense that if we have a commutative diagram of $G$-modules*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

[6] To prove exactness of (†) explicitly, first suppose that $\phi \in \mathrm{Hom}_G(\mathbb{Z}, M)$ is such that $0 = \tilde{\partial}_0(\phi) = \phi \circ \partial_0$. Since $\partial_0$ is surjective, the only way the composition can be zero is if $\phi$ itself is zero, thus (†) is injective on the left. Moreover, the composition $\tilde{\partial}_1 \circ \tilde{\partial}_0$ sends $\phi \in \mathrm{Hom}_G(\mathbb{Z}, M)$ to $\phi \circ (\partial_0 \partial_1) = 0$ so that $\mathrm{im}(\tilde{\partial}_0) \subseteq \ker(\tilde{\partial}_1)$. Finally, suppose $\phi \in \ker(\tilde{\partial}_1)$, so that $\phi \circ \partial_1 = 0$. Then $\ker(\phi) \supseteq \mathrm{im}(\partial_1) = \ker(\partial_0)$. Thus $\phi$ factors through

$$\mathbb{Z}[G]/\ker(\partial_0) \xrightarrow{\sim} \mathrm{im}(\partial_0) = \mathbb{Z}.$$

The induced map $\bar{\phi} : \mathbb{Z} \to M$ then maps to $\phi$ under $\tilde{\partial}_0$ and exactness of (†) follows. The same argument works in general to prove that $\mathrm{Hom}_R(-, N)$ is left exact for any $R$ and $M$.

*with exact rows, then the diagram*

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & H^i(G, M_2) & \longrightarrow & H^i(G, M_3) & \xrightarrow{\delta} & H^{i+1}(G, M_1) & \longrightarrow & H^{i+1}(G, M_2) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & H^i(G, N_2) & \longrightarrow & H^i(G, N_3) & \xrightarrow{\delta} & H^{i+1}(G, N_1) & \longrightarrow & H^{i+1}(G, N_2) & \longrightarrow & \cdots
\end{array}$$

*commutes.*

*Proof.* (1). For each $i$, the homomorphism $f$ induces a homomorphism $\tilde{f} : \mathrm{Hom}_G(\mathbb{Z}[G^i], M) \to \mathrm{Hom}_G(\mathbb{Z}[G^i], M')$, sending $\phi \in \mathrm{Hom}_G(\mathbb{Z}[G^i], M)$ to $f \circ \phi$. The resulting diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_G\left(\mathbb{Z}[G], M\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_G\left(\mathbb{Z}[G^2], M\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_G\left(\mathbb{Z}[G^3], M\right) & \longrightarrow & \cdots \\
 & & \downarrow \tilde{f} & & \downarrow \tilde{f} & & \downarrow \tilde{f} & & \\
0 & \longrightarrow & \mathrm{Hom}_G\left(\mathbb{Z}[G], M'\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_G\left(\mathbb{Z}[G^2], M'\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_G\left(\mathbb{Z}[G^3], M'\right) & \longrightarrow & \cdots
\end{array}$$

commutes, since for $\phi \in \mathrm{Hom}_G(\mathbb{Z}[G^i], M)$ we have

$$\tilde{f}\tilde{\partial}_i(\phi) = f \circ (\phi \circ \partial_i) = (f \circ \phi) \circ \partial_i = \tilde{\partial}_i \tilde{f}\phi.$$

In particular, the $\tilde{f}$ induce homomorphims between the cohomology of these complexes, i.e. postcomposition with $f$ gives a homomorphism

$$H^i(G, M) \to H^i(G, \tilde{M}).$$

Finally, that these induced maps respect composition is clear.

(2). The construction of (1) produces a commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G], M_1) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G], M_2) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G], M_3) & \longrightarrow & 0 \\
 & & \downarrow \tilde{\partial}_1 & & \downarrow \tilde{\partial}_1 & & \downarrow \tilde{\partial}_1 & & \\
0 & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^2], M_1) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^2], M_2) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^2], M_3) & \longrightarrow & 0 \\
 & & \downarrow \tilde{\partial}_2 & & \downarrow \tilde{\partial}_2 & & \downarrow \tilde{\partial}_2 & & \\
0 & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^3], M_1) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^3], M_2) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^3], M_3) & \longrightarrow & 0 \\
 & & \downarrow \tilde{\partial}_3 & & \downarrow \tilde{\partial}_3 & & \downarrow \tilde{\partial}_3 & & \\
 & & \vdots & & \vdots & & \vdots & & .
\end{array}$$

Since each $\mathbb{Z}[G^i]$ is a projective $\mathbb{Z}[G]$-module, each row in the diagram is exact (i.e. we have a *short exact sequence of complexes*). It's a general fact that a short exact sequence of complexes induces a long exact sequence on its cohomology groups. To prove this, for each $i$, from the

diagram above we extract from each 'horizontal rectangle' the commutative diagram

$$\begin{array}{ccccccc} & & \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], M_1)/\mathrm{im}(\tilde{\partial}_{i,M_1}) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], M_2)/\mathrm{im}(\tilde{\partial}_{i,M_2}) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], M_3)/\mathrm{im}(\tilde{\partial}_{i,M_3}) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \tilde{\partial}_{i+1}} & & \downarrow{\scriptstyle \tilde{\partial}_{i+1}} & & \downarrow{\scriptstyle \tilde{\partial}_{i+1}} \\ 0 & \longrightarrow & \ker(\tilde{\partial}_{i+2,M_1}) & \longrightarrow & \ker(\tilde{\partial}_{i+2,M_2}) & \longrightarrow & \ker(\tilde{\partial}_{i+2,M_3}) \end{array}$$

(we have added the subscripts on the $\tilde{\partial}_i$ to indicate which column they come from). The rows of this diagram are exact (the exactness can either be checked by hand, or proven by applying the Snake Lemma to the rectangles which partially overlap above and below the one we are considering) so by the Snake Lemma we deduce an exact sequence

$$H^i(G, M_1) \to H^i(G, M_2) \to H^i(G, M_3) \xrightarrow{\delta} H^{i+1}(G, M_1) \to H^{i+1}(G, M_2) \to H^{i+1}(G, M_3).$$

Splicing these sequences together for each $i$ we deduce the sought long exact sequence.

(3). The only thing that doesn't follow from the functoriality in (1) is that the squares

$$\begin{array}{ccc} H^i(G, M_3) & \xrightarrow{\delta} & H^{i+1}(G, M_1) \\ \downarrow & & \downarrow \\ H^i(G, N_3) & \xrightarrow{\delta} & H^{i+1}(G, N_1) \end{array}$$

commute for each $i$. This can be proven by a simple computation using the explicit recipe for computing the boundary homomorphisms $\delta$, which is given in the following remark. □

*Remark* 10.18. We record here the explicit formula for the boundary map

$$\delta : H^i(G, M_3) \to H^{i+1}(G, M_1)$$

which can be extracted from the proof of part (2) above (c.f. Lemma 9.10). Start with $x \in H^i(G, M_3)$. Lift this to $x' \in \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], M_2)$. Then $\tilde{\partial}_{i+1}(x') \in \ker(\tilde{\partial}_{i+2,M_2})$ is in the image of $y \in \ker(\tilde{\partial}_{i+2,M_1})$. The class of $y$ in $H^{i+1}(G, M_1)$ is then precisely $\delta(x)$.

10.5. **Cohomology and direct products.** The following Lemma says that group cohomology commutes with direct products in the second variable.

**Lemma 10.19.** *For any index set $J$ and collection $(M_j)_{j\in J}$ of $G$-modules, we have a canonical isomorphism*

$$H^i(G\ ,\ \prod_{j\in J} M_j) \cong \prod_{j\in J} H^i(G, M_j)$$

*for all $i \geq 0$, where $G$ acts 'diagonally' on $\prod_{j\in J} M_j$.*

*Proof.* For any $G$-module $P$, we have (canonically)

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P\ ,\ \prod_{j\in I} M_j) \cong \prod_{j\in J} \mathrm{Hom}_{\mathbb{Z}[G]}(P, M_j).$$

Thus applying the functor $\mathrm{Hom}_{\mathbb{Z}[G]}\left(-\ ,\ \prod_{j\in I} M_j\right)$ to the standard resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module we obtain a comutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_G\left(\mathbb{Z}[G], \prod_{j\in I} M_j\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_G\left(\mathbb{Z}[G^2], \prod_{j\in I} M_j\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_G\left(\mathbb{Z}[G^3], \prod_{j\in I} M_j\right) & \longrightarrow & \cdots \\
 & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & \prod_{j\in J} \mathrm{Hom}_G\left(\mathbb{Z}[G], M_j\right) & \xrightarrow{\tilde{\partial}_1} & \prod_{j\in J} \mathrm{Hom}_G\left(\mathbb{Z}[G^2], M_j\right) & \xrightarrow{\tilde{\partial}_2} & \prod_{j\in J} \mathrm{Hom}_G\left(\mathbb{Z}[G^3], M_j\right) & \longrightarrow & \cdots
\end{array}$$

in which all vertical isomorphisms are isomorphisms. Since arbitrary direct products preserve exactness in the category of abelian groups[7] the top complex computes the cohomology groups $H^i\left(G\ ,\ \prod_{j\in J} M_j\right)$, whilst the bottom row computes $\prod_{j\in J} H^i(G, M_j)$ the result follows. □

10.6. **Cochains, cocycles, and coboundaries.** For any $G$-module $M$, we can make the complex

$$0 \longrightarrow \mathrm{Hom}_G\left(\mathbb{Z}[G], M\right) \xrightarrow{\tilde{\partial}_1} \mathrm{Hom}_G\left(\mathbb{Z}[G^2], M\right) \xrightarrow{\tilde{\partial}_2} \mathrm{Hom}_G\left(\mathbb{Z}[G^3], M\right) \xrightarrow{\tilde{\partial}_3} \cdots \qquad (\star)$$

which yields the cohomology groups $H^i(G, M)$ very explicit.

**Definition 10.20** (Cochains)**.** For a $G$-module $M$ and $i \geq 0$, we define the abelian group of *$i$-cochains with values in $M$*, $C^i(G, M)$, to be the abelian group of set maps $G^i \to M$ (for $i = 0$ our convention is that $G^0$ is the trivial group consisting just of the identity).

**Lemma 10.21.** *Let $M$ be any $G$-module. Then for all $i \geq 0$ the map sending $f \in \mathrm{Hom}_G\left(\mathbb{Z}[G^{i+1}], M\right)$ to the function $\phi : G^i \to M$ defined by*

$$\phi(g_1, ..., g_i) = f((1, g_1, g_1g_2, ..., g_1g_2...g_i))$$

*gives an isomorphism*

$$\mathrm{Hom}_G\left(\mathbb{Z}[G^{i+1}], M\right) \xrightarrow{\sim} C^i(G, M).$$

*Proof.* As in Remark 10.9, the set

$$S = \{(1, g_1, g_1g_2, ..., g_1g_2...g_i) \ \mid \ g_1, ..., g_i \in G\}$$

gives a basis for $\mathbb{Z}[G^i]$ as a $\mathbb{Z}[G]$-module. Thus a $G$-module homomorphism $\mathbb{Z}[G^{i+1}] \to M$ is the same thing as a set map $S \to M$, the correspondence given explicitly by evaluating homomorphisms on elements of $S$. Since the map $G^i \to S$ sending $(g_1, ..., g_i)$ to $(1, g_1, g_1g_2, ..., g_1g_2...g_i)$ is visibly a bijection, the result follows. □

The idea is now to replace each of the terms $\mathrm{Hom}_G\left(\mathbb{Z}[G^{i+1}], M\right)$ in $(\star)$ with the corresponding group $C^i(G, M)$ of $i$-cochains. To do this, we need to understand the $\tilde{\partial}_i$ as maps $C^{i-1}(G, M) \to C^i(G, M)$.

**Definition 10.22.** For a $G$-module $M$, define the map $d_i : C^{i-1}(G, M) \to C^i(G, M)$ by the formula

$$(d_i(\phi))(g_1, ..., g_i) = g_1\phi(g_2, ..., g_i) + \sum_{j=1}^{i-1} (-1)^j \phi(g_1, ..., g_{j-1}, g_jg_{j+1}, g_{j+2}, ..., g_i) + (-1)^i \phi(g_1, ..., g_{i-1}).$$

[7] See [Wei94, Appendix A.4], especially Exercise A.4.5. We caution that this does not hold in an arbitrary abelian category. On the other hand, if one is just concerned with finite direct products then everything is easy by hand.

*Remark* 10.23. Since the above formula for $d_i$ takes some interpreting when $i = 0$, we note here that, thinking of $C^0(G, M) = \{\text{fns} : \{1\} \to M\} = M$ with the last equality given by identifying a function with the image of 1, our definition of $d_0$ is to take $m \in M$ to the map $G \to M$ given by

$$g \mapsto gm - m.$$

**Lemma 10.24.** *For each $G$-module $M$ and $i \geq 0$, the diagram*

$$\begin{array}{ccc} \mathrm{Hom}_G\left(\mathbb{Z}[G^i], M\right) & \longrightarrow & C^{i-1}(G, M) \\ \downarrow{\scriptstyle \tilde{\partial}_i} & & \downarrow{\scriptstyle d_i} \\ \mathrm{Hom}_G\left(\mathbb{Z}[G^{i+1}], M\right) & \longrightarrow & C^i(G, M) \end{array}$$

*commutes, where the horizontal arrows are the bijections provided by Lemma 10.21.*

*Proof.* We first compute

$$\partial_i(1, g_1, g_1g_2, ..., g_1g_2...g_i) \quad = \quad \sum_{j=0}^{i} (-1)^j (1, g_1, g_1g_2, ..., \widehat{g_1...g_j}, ..., g_1g_2...g_i)$$

$$= g_1(1, g_2, g_2g_3, ..., g_2g_3...g_i) + \sum_{j=1}^{i-1} (-1)^j (1, g_1, g_1g_2, ..., \widehat{g_1g_2...g_j}, ..., g_1g_2...g_i) + (1, g_1, g_1g_2, ..., g_1g_2...g_{i-1}).$$

Now take $f \in \mathrm{Hom}_G(\mathbb{Z}[G^i], M)$, and denote by $\phi$ the corresponding element in $C^{i-1}(G, M)$, so that we have

$$\phi(g_1, ..., g_{i-1}) = f((1, g_1, g_1g_2, ..., g_1g_2...g_{i-1})).$$

Now the element of $C^i(G, M)$ corresponding to $\tilde{\partial}_i(f) = f \circ \partial_i$ is the function sending $(g_1, ..., g_i)$ to

$$(f \circ \partial_i)((1, g_1, g_1g_2, ..., g_1g_2...g_i))$$

which by the initial computation is equal to

$$g_1 f((1, g_2, g_2g_3, ..., g_2g_3...g_i)) + \sum_{j=1}^{i-1} (-1)^j f((1, g_1, g_1g_2, ..., \widehat{g_1g_2...g_j}, ..., g_1g_2...g_i)) + f((1, g_1, g_1g_2, ..., g_1g_2...g_{i-1}))$$

$$= g_1\phi(g_2, ..., g_i) + \sum_{j=1}^{i-1} (-1)^j \phi(g_1, ..., g_{j-1}, g_jg_{j+1}, g_{j+2}, ..., g_i) + (-1)^i \phi(g_1, ..., g_{i-1}).$$

Since this is precisely $(d_i(\phi))(g_1, ..., g_i)$ we are done. □

**Definition 10.25** (Cocycles and coboundaries)**.** Define the abelian group

$$Z^i(G, M) = \ker\left(d_{i+1} : C^i(G, M) \longrightarrow C^{i+1}(G, M)\right).$$

We refer to its elements as *$i$-cocycles*. Further, define the abelian group

$$B^i(G, M) = \mathrm{im}\left(d_i : C^{i-1}(G, M) \longrightarrow C^i(G, M)\right).$$

We refer to its elements as *$i$-coboundaries*.

**Corollary 10.26.** *For any $G$-module $M$ and $i \geq 0$, we have a canonical identification*

$$H^i(G, M) = Z^i(G, M)/B^i(G, M).$$

*Proof.* By Lemma 10.24, the sequence

$$0 \longrightarrow C^0(G,M) \xrightarrow{d_1} C^1(G,M) \xrightarrow{d_2} C^2(G,M) \xrightarrow{d_3} \cdots$$

is a complex, and its cohomology compute the groups $H^i(G,M)$. That is, we have

$$H^i(G,M) = \ker(d_{i+1})/\mathrm{im}(d_i).$$

But by definition $Z^i(G,M) = \ker(d_{i+1})$ and $B^i(G,M) = \mathrm{im}(d_i)$, whence the result. □

*Remark* 10.27. Suppose

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is a short exact sequence of $G$-modules. Using Remark 10.18 we can describe, for each $i$, the boundary map $\delta : H^i(G,M_3) \to H^{i+1}(G,M_1)$ in terms of cochains, cocycles are coboundaries. Specifically, start with the class $[f]$ of an $i$-cocycle $f \in Z^i(G,M_3)$. Since $M_2$ surjects onto $M_3$, we may lift $f$ to a function $f' \in C^i(G,M_2)$. Then $d_{i+1}(f')$ is an $i+1$-cocycle in $Z^{i+1}(G,M_2)$. In fact, since $f$ was a cocycle, $d_{i+1}(f')$ take values in $M_1 \subseteq M_2$, hence can be viewed as an element of $Z^{i+1}(G,M_1)$. The class of this cocycle is $\delta([f])$.

10.7. **Low degree cohomology groups.** Here, for a $G$-module $M$, we write out explicitly the definition of $i$-cochain, $i$-cocycle and $i$-coboundary for $i = 0$,1, and 2.

- As in Remark 10.23 we have $C^0(G,M) = M$ with $d_1 : C^0(G,M) \to C^1(G,M)$ sending $m \in M$ to the function

  $$g \mapsto gm - m.$$

  Thus $Z^0(G,M) = \{m \in M \mid gm = m\} = M^G$. Moreover, since there are no cochains of degree $-1$ we find $B^0(G,M) = 0$ and

  $$H^0(G,M) = Z^0(G,M)/B^0(G,M) = M^G$$

  in agreement with Lemma 10.16.

- We have $C^1(G,M) = \{\text{fns } G \to M\}$ and for $f \in C^1(G,M)$, we have

  $$d_2(f)(g_1,g_2) = g_1 f(g_2) - f(g_1g_2) + f(g_1).$$

  In particular, a 1-cocycle is a map $f : G \to M$ such that

  $$f(g_1g_2) = f(g_1) + g_1 f(g_2)$$

  and $Z^1(G,M)$ is the group of all such. Note in particular that any such function satisfies $f(1) = 0$ (taking $g_1 = g_2 = 1$), and $f(g^{-1}) = -g^{-1}f(g)$ for all $g \in G$ (taking $g_1 = g^{-1}$ and $g_2 = g$). Moreover, 1-coboundaries are functions $f : G \to M$ of the form

  $$g \mapsto gm - m$$

  for some $m \in M$, and $B^1(G,M)$ is the group of all such. The quotient $H^1(G,M) = Z^1(G,M)/B^1(G,M)$ then agrees with that of Definition 6.21 for possibly non-abelian coefficients $X$ in place of $M$. Here we reiterate that if $G$ acts trivially on $M$ then $H^1(G,M) = \mathrm{Hom}_{\mathrm{gp}}(G,M)$, since a 1-cocycle is precisely a homomorphism, and all boundaries are 0.

- We have $C^2(G,M) = \{\text{fns } G^2 \to M\}$. For $f \in C^2(G,M)$ we have
$$d_3(f)(g_1,g_2,g_3) = g_1 f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2).$$
In particular, a 2-cocycle is a map $f : G^2 \to M$ such that
$$g_1 f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2) = 0. \tag{10.28}$$
Note in particular that setting $g_2 = g_3 = 1$ forces $gf(1,1) = f(g,1)$ for all $g \in G$, and setting $g_1 = g_2 = 1$ forces $f(1,g) = f(1,1)$ for all $g \in G$. Moreover, a 2-coboundary is a map $f : G^2 \to M$ of the form
$$f(g_1,g_2) = \phi(g_1) + g_1\phi(g_2) - \phi(g_1g_2)$$
for some function $\phi : G \to M$.

10.8. **Low degree boundary homomorphims.** Suppose we have a short exact sequence of $G$-modules
$$0 \to M_1 \to M_2 \to M_3 \to 0.$$
Here we explicate the boundary homomorphism $\delta : H^i(G,M_3) \to H^{i+1}(G,M_1)$ for $i = 0, 1$.

- For the map $\delta : M_3^G \to H^1(G,M_1)$, take $m \in M_3^G$ and lift it to $m' \in M_2$. Then $g \mapsto gm' - m'$ is a 1-cocycle which *a priori* takes values in $M_2$, but in fact takes values in (the injective image of $M_2$ of) $M_1$. The class of this cocycle in $H^1(G,M_1)$ is precisely $\delta(m)$.

- For the map $\delta : H^1(G,M_3) \to H^2(G,M_1)$, take $f \in Z^1(G,M_3)$. Lift it to a function $f' \in C^1(G,M_2)$. Then the function $a$ defined by
$$a(g_1,g_2) = g_1 f'(g_2) - f'(g_1g_2) + f'(g_1)$$
in fact takes values in $M_1$ and is a 2-cocycle. It's class in $H^2(G,M_1)$ is precisely $\delta(f)$.

10.9. $H^2$ **and group extensions.** We now show (Theorem 10.36) that the second cohomology group $H^2(G,M)$, for an arbitrary $G$-module $M$, can be described in terms of certain extensions of $G$ by $M$.

**Definition 10.29.** Let $G$ and $M$ be groups. An *extension of $G$ by $M$* is a group $E$ sitting in a short exact sequence
$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1.$$
We say that extensions $E$ and $E'$ of $G$ by $M$ are *isomorphic* if there is an isomorphism[8] $\phi : E \xrightarrow{\sim} E'$ fitting in a commutative diagram
$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle\phi} & & \| & & \\ 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

**Lemma 10.30.** *Let $M$ be an abelian group and $E$ and extension of $G$ by $M$. Then conjugation in $E$ induces an action of $G$ on $M$. More precisely, for $g \in G$ the rule $g \cdot m = \tilde{g}m\tilde{g}^{-1}$, where $\tilde{g}$ is any lift of $g$ to $E$, defines an action of $G$ on $M$.*

[8] In fact, one checks easily that any homomorphism $E \to E'$ fitting into the diagram is automatically an isomorphism.

*Proof.* Since $M$ is normal in $E$, $E$ acts on $M$ by conjugation, and since $M$ is abelian, $M$ is contained in the kernel of this action. Thus the action of $E$ on $M$ descends to the quotient $G = E/M$. □

We'll be interested in the set of (isomorphism classes of) extensions of $G$ by an abelian group $M$, inducing a given action on $M$. The simplest examples of such extensions are semidirect products.

**Definition 10.31** (Semidirect product)**.** Let $G$ be a group and $M$ a $G$-module. The *semidirect product of* $G$ by $M$, written $M \rtimes G$, is the group whose underlying set is $M \times G$, with group structure given by

$$(m_1, g_1) \cdot (m_2, g_2) = (m_1 + g_1 m_2, g_1 g_2).$$

Note that the maps $M \to M \rtimes G$, given by $m \mapsto (m, 1)$, and $M \rtimes G \to G$, given by $(m, g) \mapsto g$, realise $M \rtimes G$ as an extension of $G$ by $M$, and that the conjugation action in $M \rtimes G$ induces the initial $G$-module structure on $M$.

*Remark* 10.32. Let $M$ be a $G$-module and $\pi : M \rtimes G \to G$ the projection onto $G$. Then the map $s : G \to M \rtimes G$ given by $s(g) = (0, g)$ is a homomorphism giving a section to $\pi$. Conversely, if

$$1 \longrightarrow M \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$$

is an extension of $G$ by $M$ with conjugation in $E$ inducing the given $G$-module structure on $M$, and $s : G \to E$ is a homomorphism giving a section to $\pi$, then the map $(m, g) \mapsto m \cdot s(g)$ gives an isomorphism $M \rtimes G \xrightarrow{\sim} E$.

*Remark* 10.33. As in the previous remark, suppose

$$1 \longrightarrow M \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$$

is an extension of $G$ by $M$ with conjugation in $E$ inducing the given $G$-module structure on $M$, but that $s : G \to E$ is only a set-section to $\pi$ rather than a homomorphism. Then the map $\phi : M \times G \to E$ given by $\phi((m, g)) = m \cdot s(g)$ still gives a bijection of sets $M \times G \to E$, with inverse the map $E \to M \times G$ given by $e \mapsto \big(e \cdot s(\pi(e))^{-1}, \pi(e)\big)$, but pushing the group structure on $E$ across this map in general gives a different group structure on $M \times G$ to the one of the semidirect product. Specifically, given $m_1, m_2 \in M$ and $g_1, g_2 \in G$, we compute

$$\begin{aligned} \phi^{-1}\left(\phi((m_1, g_1)) \cdot \phi((m_2, g_2))\right) &= \phi^{-1}\left(m_1 s(g_1) m_2 s(g_2)\right) \\ &= \big(m_1 s(g_1) m_2 s(g_2) s(g_1 g_2)^{-1}, g_1 g_2\big) \\ &= (m_1 + g_1 m_2 + f(g_1, g_2), g_1 g_2) \end{aligned}$$

where $f : G \times G \to M$ is the function $(g_1, g_2) \mapsto s(g_1)s(g_2)s(g_1 g_2)^{-1}$. This observation motivates the following constructions.

**Construction 10.34** (Extensions to cocycles)**.** Let $M$ be a $G$-module and

$$1 \longrightarrow M \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

an extension of $G$ by $M$ inducing the given $G$-action on $M$. Pick a set-section $s : G \to E$ to $\pi$ (i.e. a map of sets $s : G \to E$ such that $\pi \circ s = \mathrm{id}$). From $s$ we define the map $f : G \times G \to M$ given by

$$f(g_1, g_2) = s(g_1)s(g_2)s(g_1 g_2)^{-1}.$$

We note that:

- **$f$ is a 2-cocycle valued in M:** Since $s$ is a (set-) section to $\pi$ it's clear that $f$ takes values in $M$. To check that $f$ is a 2-cocycle we compute (cf. § 10.7)

$$g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2)$$

$$\begin{aligned} = \quad & \left(s(g_1)\left(s(g_2)s(g_3)s(g_2g_3)^{-1}\right)s(g_1)^{-1}\right)\cdot\left(s(g_1g_2)s(g_3)s(g_1g_2g_3)^{-1}\right)^{-1} \\ & \cdot\left(s(g_1)s(g_2g_3)s(g_1g_2g_3)^{-1}\right)\cdot\left(s(g_1)s(g_2)s(g_1g_2)^{-1}\right)^{-1} \end{aligned}$$

  with the right hand side taking place in $E$. Since $M$ is abelian we can swap the order of the second and third factors. Upon doing this and expanding out the resulting product we see that everything cancels so that the value of the whole expression is $1 \in E$ (i.e. $0 \in M$) as desired.
- **If $s'$ is another set-section to $\pi$ with associated 2-cocycle $f'$, then $f$ and $f'$ represent the same class in $H^2(G, M)$:** Since both $s$ and $s'$ are sections to $\pi$, the difference $s'(g)s(g)^{-1}$ is an element of $M$ for all $g \in G$. Thus we may define $\alpha : G \to M$ by $\alpha(g) = s'(g)s(g)^{-1}$. Then (inside $E$) $s'(g) = \alpha(g)s(g)$ so that

$$\begin{aligned} f'(g_1, g_2) &= \alpha(g_1)s(g_1)\alpha(g_2)s(g_2)s(g_1g_2)^{-1}\alpha(g_1g_2)^{-1} \\ &= \alpha(g_1)\cdot\left(s(g_1)\alpha(g_2)s(g_1)^{-1}\right)\cdot\left(s(g_1)s(g_2)s(g_1g_2)^{-1}\right)\cdot\alpha(g_1g_2)^{-1} \\ &= \alpha(g_1) + g_1\alpha(g_2) + f(g_1, g_2) - \alpha(g_1g_2) \\ &= f(g_1, g_2) + (d\alpha)(g_1, g_2) \end{aligned}$$

  as desired.

**Construction 10.35** (Cocycles to extensions)**.** Let $M$ be a $G$-module and $f \in Z^2(G, M)$ be a 2-cocycle valued in $M$. Define the group $E$ whose underlying set is $M \times G$, with group structure given by

$$(m_1, g_1)\cdot(m_2, g_2) = (m_1 + g_1 m_2 + f(g_1, g_2), g_1 g_2).$$

Define maps $i : M \to E$ given by $m \mapsto (m - f(1,1), 1)$ and $\pi : E \to G$ given by $(m, g) \mapsto g$. We note that:

- **$E$ is a group:** We check the group axioms hold.
  *Identity:* For any $m \in M$ and $g \in G$ we have

$$(m, g)\cdot(-f(1,1), 1) = (m - gf(1,1) + f(g,1), g) = (m, g)$$

  the last equality following since the cocycle condition forces $f(g,1) = gf(1,1)$ (cf. § 10.7). Similarly

$$(-f(1,1), 1)\cdot(m, g) = (m - f(1,1) + f(1,g), g) = (m, g)$$

  since, again as in § 10.7, the cocycle condition forces $f(1,g) = f(1,1)$. Thus $(-f(1,1), 1)$ is a 2-sided identity in $E$.
  *Inverse:* Let $m \in M$ and $g \in G$. We claim that

$$(-g^{-1}m - f(g^{-1}, g) - f(1,1), g^{-1})$$

  is a 2-sided inverse for $(m, g)$ in $E$. Indeed, we compute

$$(-g^{-1}m - f(g^{-1}, g) - f(1,1), g^{-1})\cdot(m, g) = (-f(1,1), 1)$$

and

$$\begin{aligned}(m,g)\cdot(-g^{-1}m - f(g^{-1},g) - f(1,1), g^{-1}) &= (f(g,g^{-1}) - gf(g^{-1},g) - gf(1,1), 1)\\ &= (-f(1,1),1)\end{aligned}$$

where for the last equality we take $g_1 = g$, $g_2 = g^{-1}$ and $g_3 = g$ in the cocycle condition (10.28) for $f$, and combine this with the equalities $f(g,1) = gf(1,1)$ and $f(1,g) = f(1,1)$ noted previously.

*Associativity:* Let $m_1, m_2, m_3 \in M$ and $g_1, g_2, g_3 \in G$. Then

$$\begin{aligned}((m_1,g_1)\cdot(m_2,g_2))\cdot(m_3,g_3) &= (m_1 + g_1m_2 + f(g_1,g_2), g_1g_2)\cdot(m_3,g_3)\\ &= (m_1 + g_1m_2 + g_1g_2m_3 + f(g_1,g_2) + f(g_1g_2,g_3), g_1g_2g_3)\end{aligned}$$

whilst

$$\begin{aligned}(m_1,g_1)\cdot((m_2,g_2)\cdot(m_3,g_3)) &= (m_1,g_1)\cdot(m_2 + g_2m_3 + f(g_2,g_3), g_2g_3)\\ &= (m + g_1m_2 + g_1g_2m_3 + g_1f(g_2,g_3) + f(g_1,g_2g_2), g_1g_2g_3).\end{aligned}$$

Thus associativity is equivalent to the condition

$$f(g_1,g_2) + f(g_1g_2,g_3) = g_1f(g_2,g_3) + f(g_1,g_2g_3)$$

for all $g_1, g_2, g_3 \in G$. Since this is precisely the 2-cocycle condition (10.28) for $f$, we are done.

- **The maps $i$ and $\pi$ are homomorphisms realising $E$ as an extension**

$$1 \longrightarrow M \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

**of $G$ by $M$:**

*$i$ is a homomorphism:* We have

$$i(m_1 + m_2) = (m_1 + m_2 - f(1,1), 1)$$

whilst

$$\begin{aligned}i(m_1)\cdot i(m_2) &= (m_1 - f(1,1),1)\cdot(m_2 - f(1,1),1)\\ &= (m_1 + m_2 - f(1,1),1)\end{aligned}$$

as desired.

*$\pi$ is a homomorphism:* Clear.

*The sequence is exact:* Injectivity of $i$ and surjectivity of $\pi$ is clear, as it the fact that $\pi \circ i = 0$. Finally, if $e = (m,g) \in \ker(\pi)$ then we have $g = 1$ whence $e = i(m + f(1,1))$ as we are done.

- **Conjugation in $E$ induces the initial $G$-module structure on $M$:** Let $m \in M$ so that its image in $E$ is $(m - f(1,1),1)$. Then for $g \in G$ we lift $g$ to $(gf(1,1),g) \in E$ and compute (noting that $f(g,1) = gf(1,1)$ as above)

$$\begin{aligned}(gf(1,1),g)\cdot(m - f(1,1),1)\cdot(gf(1,1),g)^{-1} &= (gm + gf(1,1),g)\cdot(-f(g^{-1},g) - 2f(1,1), g^{-1})\\ &= (gm - gf(g^{-1},g) - gf(1,1) + f(g,g^{-1}),1).\end{aligned}$$

As above we have $f(g,g^{-1}) - gf(g^{-1},g) - gf(1,1) = -f(1,1)$ so that

$$(gf(1,1),g)\cdot(m - f(1,1),1)\cdot(gf(1,1),g)^{-1} = (gm - f(1,1),1).$$

Since this is just $i(gm)$ we are done.

Combining the constructions above we obtain:

**Theorem 10.36.** *Let $M$ be a $G$-module. Then Constructions 10.34 and 10.35 give mutually inverse bijections*

$$\left\{ \begin{array}{c} \text{iso. classes of extensions of } G \text{ by } M \\ \text{inducing the given } G\text{-action on } M \end{array} \right\} \leftrightarrow H^2(G, M)$$

*with the (class of the) trivial cocycle corresponding to $M \rtimes G$.*

*Proof.* Given an extension

$$1 \longrightarrow M \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

of $G$ by $M$, and a set-section $s : G \to E$ to $\pi$, Construction 10.34 associates a cocycle $f \in Z^2(G, M)$ whose class in $H^2(G, M)$ does not depend on the choice of section. Suppose that $E'$ is an extension isomorphic to $E$ and fix $\phi : E \to E'$ realising this isomorphism. Then $\phi \circ s$ gives a set-section to the projection $E' \to G$. Since $\phi$ induces identity on $M$ the associated cocycle is precisely $f$, whence Construction 10.34 descends to a map from isomorphism classes of extensions inducing the given $G$-action, to $H^2(G, M)$.

Next, suppose that we have cocycles $f, f' \in Z^2(G, M)$ with $f' = f + d\alpha$ for a function $\alpha : G \to M$. Let $E$ (resp. $E'$) denote the extension corresponding to $f$ (resp. $f'$) via Construction 10.35. Then the map $\phi : E \to E'$ given by $(m, g) \mapsto (m - \alpha(g), g)$ is an isomorphism of extensions. Indeed, $\phi$ is a homomorphism since

$$\begin{aligned} \phi\left((m_1, g_1) \cdot (m_2, g_2)\right) &= \phi\left(m_1 + g m_2 + f(g_1, g_2), g_1 g_2\right) \\ &= \left(m_1 + g m_2 + f(g_1, g_2) - \alpha(g_1 g_2), g_1 g_2\right) \end{aligned}$$

whilst

$$\begin{aligned} \phi\left((m_1, g_1)\right) \cdot \phi\left((m_2, g_2)\right) &= (m_1 - \alpha(g_1), g_1) \cdot (m_2 - \alpha(g_2), g_2) \\ &= \left(m_1 + g_1 m_2 - \alpha(g_1) - g_1 \alpha(g_2) + f'(g_1, g_2), g_1 g_2\right) \\ &= \left(m_1 + g_1 m_2 + f(g_1, g_2) - \alpha(g_1 g_2), g_1 g_2\right). \end{aligned}$$

Moreover, it's clear that $\phi$ restricts to the identity on $M$ (note that $f'(1, 1) = f(1, 1) + \alpha(1)$) and induces the identity on $G$. Thus Construction 10.35 gives a well defined map from $H^2(G, M)$ to isomorphism classes of extensions inducing the given $G$-action.

To see that the maps induced by Constructions 10.34 and 10.35 are inverse to each other, suppose we start with (the class of) a cocycle $f \in Z^2(G, M)$, and let

$$1 \longrightarrow M \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

be the extension corresponding to $f$ via Construction 10.35. A set-section to $\pi$ is provided by the map $s : G \to E$ given by $g \mapsto (0, g)$. Now for $g_1, g_2 \in G$ we have

$$s(g_1)s(g_2)s(g_1 g_2)^{-1} = (0, g_1) \cdot (0, g_2) \cdot (0, g_1 g_2)^{-1} = \left(f(g_1, g_2), g_1 g_2\right) \cdot (0, g_1 g_2)^{-1}.$$

Now as above, $f(1, g) = f(1, 1)$ for all $g \in G$, so that

$$\left(f(g_1, g_2) - f(1, 1), 1\right) \cdot (0, g_1 g_2) = \left(f(g_1, g_2) - f(1, 1) + f(1, g_1 g_2), g_1 g_2\right) = \left(f(g_1, g_2), g_1 g_2\right).$$

Thus

$$s(g_1)s(g_2)s(g_1 g_2)^{-1} = \left(f(g_1, g_2) - f(1, 1), 1\right) \cdot (0, g_1 g_2) \cdot (0, g_1 g_2)^{-1} = \left(f(g_1, g_2) - f(1, 1), 1\right).$$

Since this is $i(f(g_1, g_2)$ we see that the cocycle associated to $E$ and the set-section $s$ via Construction 10.34 is the original cocycle $f$ as desired. Conversely, suppose that we start with (the class of) an extension

$$1 \longrightarrow M \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

of $G$ by $M$, fix a set-section $s$ to $\pi$, and let $f(g_1, g_2) = s(g_1)s(g_2)s(g_1g_2)^{-1}$ be the 2-cocycle corresponding to this data via Construction 10.34. As in Remark 10.33, the map $\phi : M \times G \to E$ given by

$$\phi((m, g)) = m \cdot s(g)$$

is a bijections of sets, and that pushing the groups structure on $E$ across this bijection endows $M \times G$ with the same group structure as that corresponding to $f$ via Construction 10.35. Thus $\phi$ is a group isomorphism when $M \times G$ is given the group structure corresponding to $f$, and since $(m - f(1,1), 1)$ maps to

$$m \cdot f(1,1)^{-1} \cdot s(1) = m \cdot f(1,1)^{-1} \cdot f(1,1) = m$$

it's clear that this is in fact an isomorphism of extensions.

Finally, it's immediate from the definition of the semidirect product $M \rtimes G$ that it is the extension corresponding via Construction 10.35 to the trivial coycle . □

*Remark* 10.37. One can tidy up the correspondence of Theorem 10.36 and its proof by working instead with *normalised* cocycles. Specifically, call a cocycle $f \in Z^n(G, M)$ *normalised* if $f(g_1, ..., g_n) = 0$ whenever $g_i = 1$ for some $1 \leq i \leq n$. One can show (see [GS06, Example 3.2.5]) that every cohomology class may be represented by a normalised cocycle. The formulae for the group structure corresponding to a normalised cocycle via Construction 10.35 are then neater than the general case, and to obtain a normalised cocycle from a group extension one picks a *normalised* set-section, i.e. one mapping the identity in $G$ to the identity in $E$. However, we have chosen to work with general cocycles since, as above, there is still a natural way of producing a group extension from such a cocycle without first replacing it with a equivalent normalised one, and this can be useful in practice.

10.10. **Pullback and pushout of extensions.** Given maps $\theta : G \to G'$ and $f : M \to M'$, we now describe the induced maps $\theta^* : H^2(G', M) \to H^2(G, M)$ and $\tilde{f} : H^i(G, M) \to H^i(G, M')$ in terms of group extensions. These turn out to correspond to the group theoretic notions of pullback and pushout respectively. TO BE COMPLETED.

10.11. **Baer sum of extensions.**

10.12. **Cohomology of finite cyclic groups.** If $G$ is a finite cyclic group then there is a free resolution of $G$ that is significantly simpler than the standard one. As a consequence, the cohomology of finite cyclic groups is particularly pleasant. Recall that $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is the map sending each $g \in G$ to 1 and extending $\mathbb{Z}$-linearly. Note that $\mathbb{Z}[G]$ is commutative since $G$ is abelian.

**Proposition 10.38.** *Let $G$ be a finite cyclic group of order $n$. Fix a generator $\sigma$ for $G$ and define the elements $\Delta = \sigma - 1$ and $N = 1 + \sigma + ... + \sigma^{n-1}$ of $\mathbb{Z}[G]$. Then, denoting by $\Delta$ (resp. $N$) also the $\mathbb{Z}[G]$-endomorphism of $\mathbb{Z}[G]$ given by multiplication by $\Delta$ (resp. $N$), the complex*

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\Delta} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\Delta} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

*gives a free (and in particular projective) resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module.*

*Proof.* It's clear that each element of the sequence is free. Moreover, $\epsilon(\Delta) = 0$ and we have $N\sigma = N$ inside $\mathbb{Z}[G]$, so that

$$\Delta N = N\Delta = (\sigma - 1)N = 0$$

whence the sequence is a complex. To prove exactness, first note that $\epsilon$ is surjective, and as in Remark 10.5 its kernel is generated (as a $\mathbb{Z}$-module) by all elements of the form $\sigma^i - 1$ for $1 \leq i \leq n-1$. But since

$$\sigma^i - 1 = (\sigma - 1)(1 + \sigma + ...\sigma^{i-1})$$

we see that $\ker(\epsilon) \subseteq \mathrm{im}(\Delta)$, giving exactness at the rightmost copy of $\mathbb{Z}[G]$. Next, as $Ng = N$ for each $g \in G$, the map $N$ sends $x = \sum_{i=0}^{n-1} \lambda_i \sigma^i$ to $\epsilon(x)N$ Thus $\ker(N) = \ker(\epsilon) = \mathrm{im}(\Delta)$. Finally, we compute that for $x = \sum_{i=0}^{n-1} \lambda_i \sigma^i$ we have

$$\Delta(x) = (\lambda_{n-1} - \lambda_1) + \sum_{i=1}^{n-1} (\lambda_{i-1} - \lambda_i)\sigma^i.$$

In particular, if $x \in \ker(\Delta)$ then $\lambda_1 = \lambda_2 = ... = \lambda_{n-1}$ so that $x = N(\lambda_0)$ is in the image of $N$. □

**Corollary 10.39.** *Let $G$ be a finite cyclic group and $M$ a $G$-module. Then we have*

$$H^i(G, M) \cong \begin{cases} M^G & i = 0, \\ \ker(N : M \to M)/\Delta(M) & i \text{ odd}, \\ M^G/N(M) & i > 0 \text{ even}. \end{cases}$$

*Proof.* As in Remark 10.14, we may compute the cohomology groups $H^i(G, M)$ from any projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module, and we do this using the resolution of Proposition 10.38. Specifically, to do this we first remove $\mathbb{Z}$ to obtain the complex

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\Delta} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\Delta} \mathbb{Z}[G] \longrightarrow 0.$$

We now apply the functor $\mathrm{Hom}_G(-, M)$ to obtain the complex

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{\tilde{\Delta}} \mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{\tilde{N}} \mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{\tilde{\Delta}} \cdots$$

whose cohomology groups are $H^i(G, M)$, where here the map $\tilde{N}$ (resp. $\tilde{\Delta}$) sends $f \in \mathrm{Hom}_G(\mathbb{Z}[G], M)$ to $f \circ N$ (resp. $f \circ \Delta$). Now $\mathrm{Hom}_G(\mathbb{Z}[G], M) \cong M$ with the map given by evaluation of homomorphisms at $1 \in \mathbb{Z}[G]$. Under this identification, $\tilde{N}$ (resp. $\tilde{\Delta}$ just becomes the map $N : M \to M$ (resp. the map $\Delta : M \to M$). Thus the complex above becomes identified with the complex

$$0 \longrightarrow M \xrightarrow{\Delta} M \xrightarrow{N} M \xrightarrow{\Delta} \cdots$$

and the result follows, noting that $\ker(\Delta : M \to M) = M^G$. □

*Remark* 10.40. For $i = 1$, the explicit isomorphism

$$Z^1(G, M)/B^1(G, M) \xrightarrow{\sim} \ker(N : M \to M)/\Delta(M)$$

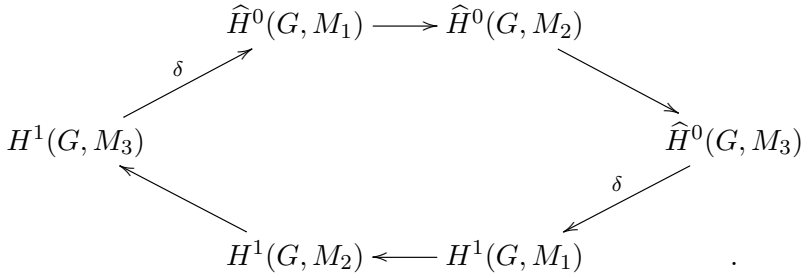
is given by evaluating a cocycle at the chosen generator of $G$.

**Notation 10.41.** For $G$ a finite cyclic group and $G$-module $M$, write $\widehat{H}^0(G, M) = M^G/N(M)$.

*Remark* 10.42. If $G$ is just finite rather than cyclic, we can also make this definition, where $N$ is taken to be $\sum_{g \in G} g \in \mathbb{Z}[G]$.

**Proposition 10.43.** *Let $G$ be a finite cyclic group.*

(1) *If* $0 \to M_1 \to M_2 \to M_3 \to 0$ *is a short exact sequence of* $G$*-modules, then we have an exact hexagon*




(2) *If* $M$ *is a finite* $G$*-module then*

$$\#\widehat{H}^0(G, M) = \#H^1(G, M).$$

*Proof.* (1). In light of Corollary 10.39, this is just the long exact sequence for cohomology of Proposition 10.17 (strictly speaking, to check that the maps in the long exact sequence are periodic, one should run the argument of Proposition 10.17 with the standard resultion replaced with the free resolution of Proposition 10.38. (2). We have

$$M/\ker(\Delta) \cong \mathrm{im}(\Delta) \quad \text{and} \quad M/\ker(N) \cong \mathrm{im}(N).$$

Since $M$ is finite, we can take orders of everything to find

$$\#\ker(\Delta) \cdot \#\mathrm{im}(\Delta) = \#M = \#\ker(N)\#\mathrm{im}(N).$$

Rearranging gives

$$\#\ker(N)/\#\mathrm{im}(\Delta) = \#\ker(\Delta)/\#\mathrm{im}(N).$$

Now note that the left hand side is equal to $\#H^1(G, M)$ whilst the right hand side is equal to $\#\widehat{H}^0(G, M)$. □

10.13. **Operations on modules.** So far we have kept the group $G$ fixed, but considered how the cohomology groups $H^i(G, M)$ vary with $M$. Now we change $G$. Note that if $\theta : H \to G$ is a group homomorphism then it induces a ring homomorphism $\mathbb{Z}[H] \to \mathbb{Z}[G]$ sending $h$ to $\theta(h)$ and extending $\mathbb{Z}$-linearly. By an abuse of notation we denote this by $\theta$ also.

**Definition 10.44.** Let $R$ and $S$ be rings, and $\theta : R \to S$ a ring homomorphism. Given an $S$-module $N$, we can consider $N$ as an $R$-module via

$$r \cdot n = \theta(r) \cdot n.$$

We call this $R$-module the *restriction of scalars* of $N$. On the other hand, if $M$ is an $R$-module then, considering $S$ as an $R$-module via $\theta$, $\mathrm{Hom}_R(S, M)$ is an $S$-module by defining, for $s \in S$ and $\phi \in \mathrm{Hom}_R(S, M)$,

$$(s \cdot \phi)(x) = \phi(xs)$$

for all $x \in S$.[9] We call this $S$-module the *coextension of scalars* of $M$.

[9]Exercise: check this really is a left module structure on $\mathrm{Hom}_R(S, M)$ even though we're multipliying by $s$ on the right.

**Lemma 10.45.** *Let $\theta : R \to S$ be a ring homomorphism, $M$ a $R$-module and $N$ a $S$-module (thought of as an $R$-module via restriction of scalars). Then we have an isomorphism (of abelian groups)*

$$\alpha : \mathrm{Hom}_R(N, M) \xrightarrow{\sim} \mathrm{Hom}_S\left(N, \mathrm{Hom}_R(S, M)\right)$$

*given by defining, for $n \in N$, $\alpha(\phi)(n) \in \mathrm{Hom}_R(S, M)$ to be the homomorphism*

$$s \mapsto \phi(sn).$$

*Proof.* The inverse map is given by sending $\phi \in \mathrm{Hom}_S\left(N, \mathrm{Hom}_R(S, M)\right)$ to the homomorphism $n \mapsto \phi(n)(1)$ (one readily checks that both maps are homomorphisms and land in the places claimed). □

*Remark* 10.46. Lemma 10.45 is saying that restriction is left-adjoint to coextension.

10.14. **Restriction and inflation.**

**Lemma 10.47.** *Let $G$ and $G'$ be groups and $\theta : G \to G'$ a homomorphism. Let $M$ be a $G'$-module and view $M$ as a $G$-module via $\theta$ (i.e. by restriction of scalars). Then we have an induced homomorphism*

$$\theta^* : H^i(G', M) \to H^i(G, M)$$

*for each $i \geq 0$. On cocycles, this if just the map $Z^i(G', M) \to Z^i(G, M)$ given by $f \mapsto f \circ \theta$ (here we are denoting the 'coordinatewise' map $G^i \to (G')^i$ induced by $\theta$ as $\theta$ also).*

*These maps are functorial in the sense that if $\phi : G' \to G''$ is another homomorphism, and $M$ is a $G''$-module, then we have $(\phi \circ \theta)^* = \theta^* \circ \phi^*$.*

*Proof.* We indicate two proofs of this (although these are really the same). First, one can simply check that the map $C^i(G', M) \to C^i(G, M)$ sending $f \mapsto f \circ \theta$ sends $i$-cocycles to $i$-cocycles, and $i$-coboundaries to $i$-coboundaries, and hence induces a map on cohomology as claimed.

More conceptually, if we think of $\mathbb{Z}[(G')^i]$ as $G$-modules (again by restriction of scalars), $\theta$ (and the induced maps $G^i \to (G')^i$ for all $i$) give a commutative diagram of $G$-modules[10]

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{\partial_3} & \mathbb{Z}[G^3] & \xrightarrow{\partial_2} & \mathbb{Z}[G^2] & \xrightarrow{\partial_2} & \mathbb{Z}[G] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \\
\cdots & \xrightarrow{\partial_3} & \mathbb{Z}[(G')^3] & \xrightarrow{\partial_2} & \mathbb{Z}[(G')^2] & \xrightarrow{\partial_2} & \mathbb{Z}[G'] & \longrightarrow & 0.
\end{array}$$

Now note that if we have two $G'$-modules $M_1$ and $M_2$, viewed as $G$-modules via $\theta$, then a $G'$-modules homomorphism from $M_1$ and $M_2$ is in particular a $G$-module homomorphism (this is how restriction of scalars is a functor). Applying the functor $\mathrm{Hom}_G(-, M)$ to the diagram,

[10] Exercise: why would a diagram like this still exist if we'd just taken arbitrary projective resolutions of $\mathbb{Z}$ as a $G$ (resp. $G'$-module) in place of the standard ones?

we obtain another commutative diagram of complexes

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_{G'}\left(\mathbb{Z}[G'], M\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_{G'}\left(\mathbb{Z}[(G')^2], M\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_{G'}\left(\mathbb{Z}[(G')^3], M\right) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_{G}\left(\mathbb{Z}[G'], M\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_{G}\left(\mathbb{Z}[(G')^2], M\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_{G}\left(\mathbb{Z}[(G')^3], M\right) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \tilde{\theta}} & & \downarrow{\scriptstyle \tilde{\theta}} & & \downarrow{\scriptstyle \tilde{\theta}} & & \\
0 & \longrightarrow & \mathrm{Hom}_{G}\left(\mathbb{Z}[G], M\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_{G}\left(\mathbb{Z}[G^2], M\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_{G}\left(\mathbb{Z}[G^3], M\right) & \longrightarrow & \cdots
\end{array}$$

In particular, we get induced maps from the cohomology groups of the top complex, i.e. the $H^i(G', M)$, to the cohomology groups of the bottom complex, i.e. the $H^i(G, M)$. The claimed functoriality, and the fact that these maps induce the claimed maps on cocycles is clear. □

**Definition 10.48** (Restriction)**.** Let $G$ be a group and $H$ a subgroup. For a $G$-module $M$, associated to the inclusion $H \hookrightarrow G$ we have, for all $i$, a *restriction homomorphism*

$$\mathrm{res} : H^i(G, M) \to H^i(H, M)$$

afforded by Lemma 10.47. Note that thinking in terms of cocycles this is just restriciton of functions from $G^i$ to $H^i$.

**Definition 10.49** (Inflation)**.** Let $G$ be a group, $M$ a $G$-module and $H$ a normal subgroup of $G$. Note that $M^H$ is naturally a $G/H$-module[11] via $g \cdot m = gm$. Associated to the quotient homomorphism $G \to G/H$ we have, by Lemma 10.47, a homomorphism

$$H^i(G/H, M^H) \to H^i(G, M^H)$$

for all $i$. Composing these with the maps $H^i(G, M^H) \to H^i(G, M)$ induced by the inclusion of $G$-modules from $M^H$ into $M$, we obtain, for each $i$, an *inflation homomorphism*

$$\mathrm{inf} : H^i(G/H, M^H) \to H^i(G, M).$$

Note that thinking in terms of cocyles, this is just precomposition with the quotient homomorphism $G^i \to (G/H)^i$ (followed by postcomposition with the inclusion $M^H \to M$).

The restriction and inflation maps are related by the *inflation-restriction exact sequence*, but to prove this we first need to develop a little more theory.

10.15. **Coinduction and Shapiro's lemma.** Now let $G$ be a group and $H$ a subgroup. We view $\mathbb{Z}[G]$ as a $\mathbb{Z}[H]$-module via $h \cdot g = hg$ (i.e. via restriction of scalars for the natural inclusion of $H$ into $G$).

**Lemma 10.50.** *Let $H$ be a subgroup of $G$. Then $\mathbb{Z}[G]$ is free as a $\mathbb{Z}[H]$-module.*

*Proof.* Let $S = \{g_i\}_{i \in I}$ be a right transversal for $H$ in $G$, i.e. such that $S$ consists of precisely one representative of each of the right cosets of $H$ in $G$. Then we have

$$\mathbb{Z}[G] = \bigoplus_{i \in I} \mathbb{Z}[H] g_i$$

and we are done. □

[11] Normality of $H$ shows that the action of $G$ on $M$ restricts to an action on $M^H$, and this descends to a $G/H$-action since $H$ acts trivially on $M^H$.

**Corollary 10.51.** *If $P$ is a projective $G$-module then (the restriction of scalars of) $P$ is also projective as an $H$-module.*

*Proof.* Since $\mathbb{Z}[G]$ is free as a $\mathbb{Z}[H]$-module, any free $G$-module is also free as a $H$-module. Since projective modules are characteristed by being direct summands of free modules (cf. Proposition 9.6), the result follows. □

**Notation 10.52.** If $H$ is a subgroup of $G$, and $M$ a $H$-module, then by coextension of scalars we get a $G$-module. That is, $\mathrm{Hom}_H(\mathbb{Z}[G], M)$ is a $G$-module via $(g \cdot \phi)(x) = \phi(xg)$. We refer to this as the *coinduction* of $M$ from $H$ to $G$, and denote it $\mathrm{coInd}_H^G(M)$.

**Lemma 10.53** (Shapiro's lemma)**.** *Let $H$ be a subgroup of $G$ and $M$ be a $H$-module. Then there is a canonical isomorphism*

$$H^i\left(G, \mathrm{coInd}_H^G(M)\right) \cong H^i(H, M)$$

*for all $i$.*

*Proof.* Since any free $G$-module is also free as a $H$-module, the standard resolution of $\mathbb{Z}$ as a $G$-module is also a free resolution of $\mathbb{Z}$ as a $H$-module. Thus the groups $H^i(H, M)$ can be computed by applying the functor $\mathrm{Hom}_H(-, M)$ to this resolution. On the other hand, to compute the groups $H^i\left(G, \mathrm{coInd}_H^G(M)\right)$, we apply the functor $\mathrm{Hom}_G\left(-, \mathrm{coInd}_H^G(M)\right)$ to this resolution. However, for any $G$-module $P$, Lemma 10.45 gives an isomorphism

$$\mathrm{Hom}_G\left(P, \mathrm{coInd}_H^G(M)\right) \xrightarrow{\sim} \mathrm{Hom}_H(P, M)$$

sending $\phi$ to $p \mapsto \phi(p)(1)$. In particular, we have an isomorphism of complexes

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_G\left(\mathbb{Z}[G], \mathrm{coInd}_H^G(M)\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_G\left(\mathbb{Z}[G^2], \mathrm{coInd}_H^G(M)\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_G\left(\mathbb{Z}[G^3], \mathrm{coInd}_H^G(M)\right) & \longrightarrow & \cdots \\
 & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & \mathrm{Hom}_H\left(\mathbb{Z}[G], M\right) & \xrightarrow{\tilde{\partial}_1} & \mathrm{Hom}_H\left(\mathbb{Z}[G^2], M\right) & \xrightarrow{\tilde{\partial}_2} & \mathrm{Hom}_H\left(\mathbb{Z}[G^3], M\right) & \longrightarrow & \cdots .
\end{array}$$

Since the cohomology of the top row is $H^i\left(G, \mathrm{coInd}_H^G(M)\right)$ whilst the cohomology of the bottom row is $H^i(H, M)$, we are done. □

*Remark* 10.54. For any $G$-module $M$, and subgroup $H$ of $G$, we have a natural map $M \to \mathrm{coInd}_H^G M$ given by $m \mapsto (g \mapsto gm)$. That such a map should exist is clear, since Lemma 10.45 gives

$$\mathrm{Hom}_G\left(M, \mathrm{coInd}_H^G(M)\right) \xrightarrow{\sim} \mathrm{Hom}_H(M, M)$$

and there is a distinguished element on the right, namely the identity map $M \to M$ (one checks the this does indeed correspond to the map above under the isomorphism of Lemma 10.45). In particular, we get an induced map

$$H^i(G, M) \to H^i\left(\mathrm{coInd}_H^G(M)\right) \overset{\text{Shapiro}}{=\!=} H^i(H, M).$$

One readily checks that this is precisely the restriction map.

10.15.1. *Coinduced modules.*

**Definition 10.55.** We say that a $G$-module $M$ is *coinduced* if we have

$$M \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \Lambda)$$

for some abelian group $\Lambda$. That is, if $M$ is obtained via coinduction from a module over the trivial group.

**Corollary 10.56** (of Shapiro's lemma)**.** *If $M$ is coinduced then*

$$H^i(G, M) = 0$$

*for all $i > 0$.*

*Proof.* Writing $M \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \Lambda)$, Shapiro's lemma gives, for all $i$,

$$H^i(G, M) = H^i(\{1\}, \Lambda).$$

Now (e.g. thinking in terms of cocycles) $H^0(\{1\}, \Lambda) = \Lambda$, whilst $H^i(\{1\}, \Lambda) = 0$ for $i > 0$. □

*Remark* 10.57. Since this will allow 'dimension shifting' arguments, we note here than any $G$-module $M$ can naturally be embedded in a coinduced $G$-module. Indeed, we have an injective $G$-module homomorphism

$$M \to \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G], M\right)$$

given by

$$m \mapsto (g \mapsto gm).$$

(What's really happening here is that we are first restricting scalars and the coextending scalars along the unique ring homomorphism $\mathbb{Z} \to \mathbb{Z}[G]$; the adjunction provides the map $M \to \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G], M\right)$.)

10.15.2. *Induced modules.* Let $\Lambda$ be an abelian group. We make $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ into a $G$-module via

$$g \cdot (\lambda \otimes x) = \lambda \otimes gx.$$

**Definition 10.58.** We say a $G$-module $M$ is *induced* if we have

$$M \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}[G]$$

for some abelian group $\Lambda$.

In the special case of finite groups, this turns out to be the same notion as a coinduced module.

**Lemma 10.59.** *Let $G$ be a finite group and $\Lambda$ any abelian group. Then we have an isomorphism*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \Lambda) \xrightarrow{\sim} \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}[G]$$

*given by*

$$\phi \longmapsto \sum_{g \in G} \phi\left(g^{-1}\right) \otimes g.$$

*Proof.* It's clear that the given map is a homomorphism of abelian groups, and it's $G$-equivariant for if $h \in G$ then

$$h \cdot \phi \longmapsto \sum_{g \in G} \phi\left(g^{-1}h\right) \otimes g.$$

Relabelling the sum by setting $\sigma = h^{-1}g$ we see that this is equal to

$$\sum_{\sigma \in G} \phi\left(\sigma^{-1}\right) \otimes h\sigma = h\left(\sum_{\sigma \in G} \phi\left(\sigma^{-1}\right) \otimes \sigma\right)$$

as desired. To construct the inverse, note that any $x \in \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ can be uniquely written as

$$x = \sum_{g \in G} \lambda_g \otimes g$$

for $\lambda_g \in \Lambda$. We now define the element $\phi_x \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \Lambda)$ by setting $\phi_x(g) = \lambda_{g^{-1}}$ and extending $\mathbb{Z}$-linearly. Since this is visibly inverse to the map of the statement, the result follows. □

**Corollary 10.60.** *Let $G$ be a finite group and $M$ an induced $G$-module. Then $H^i(G, M) = 0$ for all $i > 0$.*

*Proof.* Since $M$ is induced, by Lemma 10.59 it is also coinduced, and we conclude by Corollary 10.56. □

10.16. **The inflation-restriction exact sequence.**

**Proposition 10.61** (Inflation-restriction exact sequence)**.** *Let $G$ be a group, $H$ a normal subgroup, and $M$ a $G$-module. Then we have:*

(1) *The sequence*

$$0 \to H^1(G/H, M^H) \xrightarrow{\inf} H^1(G, M) \xrightarrow{\mathrm{res}} H^1(H, M)$$

*is exact.*

(2) *If moreover, for some $q \geq 1$ we have $H^i(H, M) = 0$ for all $1 \leq i < q$, then we additionally have an exact sequence*

$$0 \to H^q(G/H, M^H) \xrightarrow{\inf} H^q(G, M) \xrightarrow{\mathrm{res}} H^q(H, M)$$

*and inflation gives an isomorphism*

$$\inf : H^i(G/H, M^H) \xrightarrow{\sim} H^i(G, M)$$

*for all $1 \leq i < q$.*

*Proof.* (1). We'll prove exactness by computing explicitly with cocycles and coboundaries. Write $\pi : G \to G/H$ for the quotient homomorphism, and $i : H \to G$ for the inclusion of $H$ into $G$.

**Injectivity of** inf**:** Let $f \in Z^1(G/H, M^H)$ and suppose that $f$ maps to 0 under inf. Then there is $m \in M$ such that $(f \circ \pi)(g) = gm - m$ for all $g \in G$. Now since $f$ is a 1-cocycle, for all $h \in H$ we have

$$hm - m = (f \circ \pi)(h) = f(1) = 0.$$

Thus $m \in M^H$, $f$ is the coboundary of $m$, and the class of $f$ is zero in $H^1(G/H, M^H)$.

**Exactness at** $H^1(G, M)$**:** Since $\pi \circ i = 0$ it's clear that $\mathrm{res} \circ \inf = 0$. It remains to show that $\ker(\mathrm{res}) \subseteq \mathrm{im}(\inf)$. Let $f \in Z^1(G, M)$ and suppose that $\mathrm{res}(f) = 0 \in H^1(H, M)$. Then there is $m \in M$ such that $f(h) = hm - m$ for all $h \in H$. Subtracting from $f$ the coboundary $d_1 m$, we may assume that $f(h) = 0$ for all $h$. Now for any $h \in H$ and $g \in G$, the cocycle condition gives

$$f(gh) = f(g) + gf(h) = f(g)$$

so that $f$ is constant on the left cosets of $H$ in $G$. Moreover, $f$ is valued in $M^H$. Indeed, since $H$ is normal in $G$, for any $g \in G$ and $h \in H$, we have $g^{-1}hg = h'$ for some $h' \in H$. Then

$$f(g) = f(hgh'^{-1}) = f(h) + hf(gh'^{-1}) = hf(g).$$

Thus $f$ factors as $f' \circ \pi$ for some function $f' : G \to M^H$. Now clearly $f'$ is a cocycle and $f = \inf(f')$.

(2). We prove this using 'dimension shifting'. TO BE COMPLETED

□

*Remark* 10.62. In fact, the inflation restriction sequence can be extended into a five term exact sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{res}} H^1(H, M)^{G/H} \xrightarrow{\tau} H^2(G/H, M^H) \xrightarrow{\text{inf}} H^2(G, M),$$

where $\tau$ is the *transgression* map, and the action of $G/H$ on $H^1(H, M)$ is the *conjugation* action (see [GS06, Construction 3.3.12]). For a description of the transgression map in terms of cocycles see [NSW08, Proposition 1.6.6].

10.17. **Corestriction.** Now let $H$ be a finite index subgroup of $G$ and $M$ a $G$-module. We'll construct a map $\text{cor} : H^i(H, M) \to H^i(G, M)$ for all $i \geq 0$. For $i = 0$, this will be the 'norm' map: $M^H \to M^G$ given by $m \mapsto \sum_{i=1}^n g_i m$, where here $n$ is the index of $H$ in $G$ and $g_1, ..., g_n$ is a left transversal for $H$ in $G$. Note that the result is $G$-invariant since for any $g \in G$, $\{gg_i\}_{i=1}^n$ is another set of left coset representatives for $H$ in $G$.

**Lemma 10.63.** *Let $M$ be a $G$-module and $H$ be a finite index subgroup of $G$, say $n = [G : H]$. Further, let $g_1, ..., g_n$ be a left transversal for $H$ in $G$. Then the map*

$$\alpha : \text{coInd}_H^G(M) = \text{Hom}_H(\mathbb{Z}[G], M) \to M$$

*given by*

$$\alpha(\phi) = \sum_{j=1}^n g_j \phi(g_j^{-1})$$

*is a homomorphism of $G$-modules which does not depend on the choice of left transversal.*

*Proof.* Let $g_1', ..., g_n'$ be another left transversal for $H$ in $G$. Then, reordering the $g_j'$ if necessary, we can assume that for each $j$, $g_j' = g_j h_j$ for some $h_j \in H$. Then for each $\phi \in \text{Hom}_H(\mathbb{Z}[G], M)$ we have

$$\sum_{j=1}^n g_j' \phi((g_j')^{-1}) = \sum_{j=1}^n g_j h_j \phi(h_j^{-1} g_j^{-1}) = \sum_{j=1}^n g_j \phi(g_j^{-1}),$$

where for the last equality we are using that $\phi$ is a $H$-module homomorphism. Thus $\alpha$ is independent of the choice of left transversal. Moreover, $\alpha$ is $G$-equivariant since for any $g \in G$, we have

$$\alpha(g \cdot \phi) = \sum_{j=1}^n g_j \phi(g_j^{-1} g) = g \left( \sum_{j=1}^n g^{-1} g_j \phi\left( (g^{-1} g_j)^{-1} \right) \right).$$

Since $\{g^{-1} g_j\}_{j=1}^n$ is also a left transversal for $H$ in $G$, the above is equal to $g\alpha(\phi)$ as desired. □

**Definition 10.64.** Let $M$ be a $G$-module and $H$ be a finite index subgroup of $G$. For each $i \geq 0$, we define the *corestriction homomorphism* as the composition

$$\text{cor} : H^i(H, M) \overset{\text{Shapiro}}{=\!=} H^i\left(G, \text{coInd}_H^G(M)\right) \overset{\text{Lem 10.63}}{\longrightarrow} H^i(G, M).$$

**Lemma 10.65.** *Let $M$ be a $G$-module and $H$ a finite index subgroup of $G$. Writing $n = [G : H]$, we have, for all $i \geq 0$, $\text{cor} \circ \text{res} = n$ on $H^i(G, M)$.*

*Proof.* The composition $\text{cor} \circ \text{res} : H^i(G, M) \to H^i(G, M)$ is the map on cohomology (of $G$) induced by the composition

$$M \longrightarrow \text{coInd}_H^G M \overset{\text{Lem 10.63}}{\longrightarrow} M$$

where the first map is given by $m \mapsto (g \mapsto gm)$ (cf. Remark 10.54). Thus it suffices to show that this composition is multiplication by $n$. For $m \in M$, letting $\phi_m$ be the map $g \mapsto gm$ we have (choosing a left transversal $g_1, ..., g_n$ for $H$ in $G$)

$$\sum_{j=1}^{n} g_j \phi_m(g_j^{-1}) = \sum_{j=1}^{n} (g_j g_j^{-1} m) = nm$$

as desired. □

A consequence is the following important and fundamental fact.

**Corollary 10.66.** *Let $G$ be a finite group of order $n$. Then for any $G$-module $M$, and $i \geq 1$, $H^i(G, M)$ is $n$-torsion.*

*Proof.* Multiplication by $n$ on $H^i(G, M)$ factors as

$$n : H^i(G, M) \xrightarrow{\text{res}} H^i(\{1\}, M) \xrightarrow{\text{cor}} H^i(G, M),$$

but for each $i \geq 1$, the middle group is 0. □

10.18. **Cup products.** TO BE ADDED.

10.19. **Relation to nonabelian $H^1$.**

**Lemma 10.67.** *Let $G$ be a group and let*

$$1 \to X_1 \to X_2 \to X_3 \to 1$$

*be a short exact sequence of $G$-groups. Then we have a long exact sequences of pointed sets*[12]

$$1 \to X_1^G \to X_2^G \to X_3^G \xrightarrow{\delta} H^1(G, X_1) \to H^1(G, X_2) \to H^1(G, X_3).$$

*If moreover $X_1$ is central in $X_2$ (so that in particular $X_1$ is abelian), then this can be extended to an exact sequence of pointed sets*

$$\cdots \to H^1(G, X_3) \xrightarrow{\delta} H^2(G, X_3).$$

*Moreover, this sequence is natural in the sense that given a commutative diagram of $G$-groups*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & X_1 & \longrightarrow & X_2 & \longrightarrow & X_3 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & Y_1 & \longrightarrow & Y_2 & \longrightarrow & Y_3 & \longrightarrow & 1 \end{array}$$

*with exact rows, the diagram*

$$\begin{array}{ccccccccccccc} 1 & \longrightarrow & X_1^G & \longrightarrow & X_2^G & \longrightarrow & X_3^G & \xrightarrow{\delta} & H^1(G, X_1) & \longrightarrow & H^1(G, X_2) & \longrightarrow & H^1(G, X_3) \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & Y_1^G & \longrightarrow & Y_2^G & \longrightarrow & Y_3^G & \xrightarrow{\delta} & H^1(G, Y_1) & \longrightarrow & H^1(G, Y_2) & \longrightarrow & H^1(G, Y_3) \end{array}$$

[12] we say a sequence

$$S_1 \xrightarrow{f} S_2 \xrightarrow{g} S_3$$

of pointed sets is *exact* if $f(S_1) = g^{-1}(\bullet)$, where $\bullet$ is the distinguished element of $S_3$. We caution that the sequence $S_2 \to S_3 \to 1$ being exact *does* imply that $S_2 \to S_3$ is surjective, but that exactness of $1 \to S_1 \to S_2$ *does not* imply that $S_1 \to S_2$ is injective: it merely says that the distinguished element of $S_2$ has a unique preimage.

*commutes. If moreover $X_1$ is central in $X_2$, and $Y_1$ is central in $Y_2$, the extended diagram*

$$\begin{array}{ccccc} \cdots & \longrightarrow & H^1(G, X_3) & \xrightarrow{\delta} & H^2(G, X_1) \\ & & \downarrow & & \downarrow \\ \cdots & \longrightarrow & H^1(G, Y_3) & \xrightarrow{\delta} & H^2(G, Y_2) \end{array}$$

*commutes also.*

*Proof.* We will define the boundary maps appearing in the sequences, and leave exactness (and the fact that the maps are well defined), as well as the naturality, as an exercise.

**Definition of $\delta : X_3^G \to H^1(G, X_1)$:** Let $x \in X_3^G$. Since the map $X_2 \to X_3$ is surjective, we can lift $x$ to $x' \in X_2$. As in Remark 6.20, the map $\rho : g \mapsto (x')^{-1} g(x')$ is a 1-cocycle taking values in $X_2$. Its image in $X_3$ is $x^{-1}g(x) = 1$ since $X$ is $G$-invariant. Thus $\rho$ takes values in $X_1$ (viewed as a subgroup of $X_2$ via the first map of the short exact sequence) and we define $\delta(x)$ to be the class of $\rho$ in $H^1(G, X_1)$.

**Definition of $\delta : H^1(G, X_3) \to H^2(G, X_1)$ when $X_1$ is central in $X_2$:** Let $x \in H^1(G, X_3)$ and suppose that $x$ is the equivalence class of a 1-cocycle $\rho : G \to X_3$. Since the map $X_2 \to X_3$ is surjective, we may lift $\rho$ to a function $\rho' : G \to X_2$. Since $\rho$ is a 1-cocycle, for each $g, h \in G$,

$$a(g, h) := \rho'(g) g(\rho'(h))(\rho'(gh))^{-1} \in X_2$$

maps to the identity in $X_3$. Thus in fact $a(g, h)$ is an element of $X_1$ for all $g, h \in G$. One checks that the association

$$(g, h) \mapsto a(g, h) \in X_1$$

is a 2-cocycle, and we define $\delta(x)$ to be its class in $H^2(G, X_1)$. □

*Remark* 10.68. One can say slightly more about the various maps involved in Lemma 10.67 than simply that they are maps of pointed sets. For a thorough discussion of this, and a proof of the following assertions, see [Ser02, Chapter 1 §5]. We'll just state what happens in the case where the theory works the best, which is when $X_1$ is central in $X_2$. In this case, the maps

$$X_1^G \longrightarrow X_2^G \longrightarrow X_2^G \longrightarrow H^1(G, X_1)$$

are all homomorphisms. Moreover, the fibres over elements of the image of the map

$$H^1(G, X_1) \longrightarrow H^1(G, X_2)$$

are all cosets of the kernel, which is a subgroup of $H^1(G, X_1)$ (equal to the image of $X_3^G$ under the connecting homomorphism). Moreover, the formula $\rho \mapsto f \cdot \rho$ gives an action of the group $H^1(G, X_1)$ on the set $H^1(G, X_2)$. The fibres over elements of the image of the map $H^1(G, X_2) \to H^1(G, X_3)$ are precisely the $H^1(G, X_1)$-orbits for this action (with exactness at $H^1(G, X_2)$ in Lemma 10.67 implying that the orbit of the trivial cocycle is the kernel of the map).

Finally, suppose that $X_3$ is also abelian, so that $X_2$ is an extension of two abelian groups. Then the commutator pairing

$$X_3 \times X_3 \longrightarrow X_1$$

associated to the extension (sending $(x, x')$ to the commutator $[\tilde{x}, \tilde{x}'] = \tilde{x}\tilde{x}'\tilde{x}^{-1}\tilde{x}'^{-1}$ viewed as an element of $X_1$, where here $\tilde{x}$ and $\tilde{x}'$ are lifts of $x$ and $x'$ to $X_2$ respectively) induces a cup-product map

$$H^1(G, X_3) \times H^1(G, X_3) \longrightarrow H^2(G, X_1).$$

The connecting map $\delta : H^1(G, X_3) \longrightarrow H^2(G, X_1)$ (in general *not* a homomorphism) then satisfies

$$\delta(\rho + \rho') - \delta(\rho) - \delta(\rho') = -\rho \cup \rho'.$$

See [PR11, Proposition 2.9] for details.

We will also need the following Lemma (whose (much more general) abelian counterpart is Lemma 10.19) in the next section, so we record it here.

**Lemma 10.69.** *Let $G$ be a group and $X$ and $Y$ be $G$-groups. Then the map*

$$H^1(G, X) \times H^1(G, Y) \longrightarrow H^1(G, X \times Y)$$

*gives on cocycles by*

$$(f, f') \mapsto \big(g \mapsto (f(g), f'(g))\big)$$

*is a bijection of pointed sets (with $G$ acting diagonally on $X \times Y$).*

*Proof.* Straightforward computation. □

## 11. Cohomology of profinite groups

TO BE ADDED.

# Part 3. The Brauer group revisited

## 12. The Brauer group in terms of cohomology

### 12.1. Statement of the main theorem and applications.

**Theorem 12.1.** *Let $K/k$ be a finite Galois extension with Galois group $\mathrm{Gal}(K/k)$. Then there is an isomorphism of abelian groups*

$$\mathrm{Br}(K/k) \cong H^2\left(\mathrm{Gal}(K/k), K^\times\right).$$

Before proving this we first make some remarks and show the utility of the cohomological approach.

*Remark* 12.2. Given a tower of field extensions $L/K/k$ with both $L/k$ and $K/k$ Galois, one can show that the natural inclusion of Brauer classes $\mathrm{Br}(K/k) \hookrightarrow \mathrm{Br}(L/k)$ corresponds on the cohomology side to the map

$$H^2\left(\mathrm{Gal}(K/k), K^\times\right) \xrightarrow{\inf} H^2\left(\mathrm{Gal}(L/k), L^\times\right).$$

By Remark 5.9 we then have

$$\mathrm{Br}(k) = \varinjlim H^2\left(\mathrm{Gal}(K/k), K^\times\right)$$

where the direct limit is taken over all finite Galois extension $K/k$ with respect to the inflation maps above. In fact, this limit is equal to

$$H^2\left(\mathrm{Gal}(k^{\mathrm{sep}}/k), k^{\mathrm{sep}\times}\right)$$

with the caveat that this cohomology group is to be interpreted as a slight variant of the group cohomology of the previous section which takes into account the topology on $\mathrm{Gal}(k^{\mathrm{sep}}/k)$. See, for example, [Gru67].

**Corollary 12.3.** *For any finite Galois extension $K/k$ of degree $n$, $\mathrm{Br}(K/k)$ is $n$-torsion. In particular, the full Brauer group $\mathrm{Br}(k)$ is a torsion abelian group.*

*Proof.* Since $\mathrm{Gal}(K/k)$ is finite of order $n$, the group $H^2\left(\mathrm{Gal}(K/k), K^\times\right)$ is $n$-torsion by Corollary 10.66. The claim about the whole Brauer group follows since $\mathrm{Br}(k)$ is the union of the groups $\mathrm{Br}(L/k)$ as $L$ ranges over all finite Galois extensions of $k$ (cf. Remark 5.9). □

*Remark* 12.4. Corollary 12.3 says that if $A/k$ is a central simple algebra split by a Galois extension $K/k$ of degree $n$, then $A^{\otimes n} \cong M_r(K)$ (counting $k$-dimensions we have $r = \deg(A)^n$).

**Corollary 12.5** (Wedderburn's Little Theorem, second proof)**.** *Let $k$ be a finite field. Then* $\mathrm{Br}(k) = 0$.

*Proof.* Since every Brauer class is split by a finite Galois extension it suffices to show that $\mathrm{Br}(K/k) = 0$ for every finite Galois extension $K/k$. Fixing one such, $\mathrm{Gal}(K/k)$ is cyclic, and $K^\times$ is a finite abelian group. Thus by Proposition 10.43 we have

$$\#H^2\left(\mathrm{Gal}(K/k), K^\times\right) = \#H^1\left(\mathrm{Gal}(K/k), K^\times\right).$$

Since

$$H^1\left(\mathrm{Gal}(K/k), K^\times\right) = 0$$

by Hilbert's Theorem 90, we are done. □

**Corollary 12.6** (The Brauer group of $\mathbb{R}$, second proof)**.** *We have* $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

*Proof.* Since $\mathbb{C}$ is algebraically closed we have

$$\mathrm{Br}(\mathbb{R}) = \mathrm{Br}(\mathbb{C}/\mathbb{R}) \cong H^2\left(\mathbb{C}/\mathbb{R}, \mathbb{C}^\times\right).$$

Since $\mathrm{Gal}\left(\mathbb{C}/\mathbb{R}\right)$ is cyclic of order 2, generated by complex conjugation, Corollary 10.39 gives

$$H^2\left(\mathbb{C}/\mathbb{R}, \mathbb{C}^\times\right) \cong \mathbb{R}^\times/N_{\mathbb{C}/\mathbb{R}}\left(\mathbb{C}^\times\right).$$

Since $N_{\mathbb{C}/\mathbb{R}}$ just maps a complex number $x$ to $x\bar{x} = |x|^2$ we have

$$N_{\mathbb{C}/\mathbb{R}}\left(\mathbb{C}^\times\right) = \mathbb{R}^\times_{>0}.$$

Thus

$$H^2\left(\mathbb{C}/\mathbb{R}, \mathbb{C}^\times\right) \cong \mathbb{R}^\times/\mathbb{R}^\times_{>0} = \{\pm 1\}$$

and we are done. □

12.2. **Proof of Theorem 12.1.** Fix a finite Galois extension $K/k$, and let $G = \mathrm{Gal}(K/k)$ denote its Galois group. As usual, denote by $CSA_n(K/k)$ the set of isomorphism classes of central simple algebras over $k$ which are split by $K/k$, and have degree $n$. As in Theorem 6.28 we have a bijection of pointed sets

$$CSA_n(K/k) \leftrightarrow H^1\left(G, PGL_n(K)\right)$$

with the explicit map from left to right described in Remark 6.29. Moreover, by Proposition 5.10, as $n, m$ range over all positive integers, the maps $CSA_n(K/k) \to CSA_{mn}(K/k)$ given by $A \mapsto M_m(A)$ make $\{CSA_n(K/k)\}_n$ into a direct system, and we have

$$\varinjlim CSA_n(K/k) = \mathrm{Br}(K/k)$$

via the natural map sending the class of a central simple algebra on the left hand side to its Brauer class on the right hand side. Note that the group operation on $\mathrm{Br}(K/k)$ corresponds to the operation on

$$\varinjlim CSA_n(K/k)$$

induced by the maps

$$CSA_n(K/k) \times CSA_m(K/k) \to CSA_{nm}(K/k)$$

given by $(A, A') \mapsto A \otimes_k A'$ on all finite levels $n, m$.

**Definition 12.7.** For each $n, m \geq 1$, denote by $\lambda_{n,m}$ the homomorphism of $G$-groups

$$\lambda_{n,m} : GL_n(K) \to GL_{nm}(K)$$

given by

$$M \mapsto \begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix}.$$

Note that this induces a homomorphism of $G$-groups $PGL_n(K) \to PGL_{nm}(K)$ which we denoted $\lambda_{n,m}$ also. We denote by $\tilde{\lambda}_{n,m}$ the map of pointed sets

$$\tilde{\lambda}_{n,m} : H^1(G, PGL_n(K)) \longrightarrow H^1(G, PGL_{nm}(K))$$

induced by $\lambda_{n,m}$.

**Lemma 12.8.** *For all $n, m \geq 1$, the diagram*

$$\begin{array}{ccc} CSA_n(K/k) & \longrightarrow & H^1(G, PGL_n(K)) \\ \downarrow & & \downarrow{\scriptstyle \tilde{\lambda}_{n,m}} \\ CSA_{nm}(K/k) & \longrightarrow & H^1(G, PGL_{nm}(K)) \end{array}$$

*commutes (here the leftmost vertical map is $A \mapsto M_m(A)$ and the horizontal maps are provided by Theorem 6.28). In particular, the maps $\tilde{\lambda}_{n,m}$ form a direct system and we have a bijection of pointed sets*

$$\mathrm{Br}(K/k) \leftrightarrow \varinjlim H^1(G, PGL_n(K)).$$

*Proof.* Let $A \in CSA_n(K/k)$ and fix an isomorphism $\phi : A \otimes_k K \xrightarrow{\sim} M_n(K)$. Then, as in Remark 6.29, the image of $A$ in $H^1(G, PGL_n(K))$ is represented by the cocycle $\rho : \sigma \mapsto \phi\, {}^{\sigma}\phi^{-1}$. Moreover,

$$\begin{pmatrix} \phi & & \\ & \ddots & \\ & & \phi \end{pmatrix}$$

gives an isomorphism

$$M_m(A) \otimes_k K = M_m(A \otimes_k K) \xrightarrow{\sim} M_{nm}(K)$$

and the corresponding cocyle is $\tilde{\lambda}_{n,m}(\rho)$, whence the result. □

**Notation 12.9.** Let $M \in GL_n(K)$ and $M' \in GL_m(K)$. With respect to the standard bases for $K^n$ (resp. $K^m$), which we denote $e_1, ..., e_n$ (resp. $f_1, ..., f_m$), we view $M$ (resp. $M'$) as a linear automorphisms of $K^n$ (resp. $K^m$). Denote these automorphisms $\alpha$ and $\alpha'$ respectively. Then we denote by $M \otimes M'$ the matrix in $GL_{nm}(K)$ representing the automorphism $\alpha \otimes \alpha'$ (i.e. $v \otimes v' \mapsto \alpha(v) \otimes \alpha'(v')$) with respect to the basis $\{e_i \otimes f_j\}$, ordered by increasing $i$ followed by increasing $j$.[13]

[13]To make things correct throughout this section, we need to fix once and for all this identification of $K^n \otimes K^m$ with $K^{nm}$.

**Lemma 12.10.** *For any $n, m \geq 1$, the homomorphism of $G$-modues*

$$GL_n(K) \times GL_m(K) \longrightarrow GL_{nm}(K)$$

*given by $(M, M') \mapsto M \otimes M'$ descends to a homomorphism of $G$-modules*

$$PGL_n(K) \times PGL_m(K) \to PGL_{nm}(K)$$

*and the resulting maps on cohomology endows*

$$\varinjlim H^1\left(G, PGL_n(K)\right)$$

*with the structure of an abelian group with respect to which the bijection of Lemma 12.8 is an isomorphism.*

*Proof.* It's clear that the map $(M, M') \mapsto M \otimes M'$ descends to a map

$$PGL_n(K) \times PGL_m(K) \to PGL_{nm}(K)$$

as claimed, and hence induces a map

$$H^1\left(G, PGL_n(K)\right) \times H^1\left(G, PGL_m(K)\right) \to H^1\left(G, PGL_{nm}(K)\right)$$

on cohomology (here we are using Lemma 10.69). Since we already know that $\otimes_k$ gives a group law on $\mathrm{Br}(K/k)$, we need only show that these maps correspond to the maps

$$CSA_n(K/k) \times CSA_m(K/k) \to CSA_{nm}(K/k)$$

gives by $(A, A') \mapsto A \otimes_k A'$. But if we fix isomorphisms $\phi : A \otimes_k K \to M_n(K)$ and $\phi' : A' \otimes_k K \to M_m(K)$, then $\phi \otimes \phi'$ gives an isomorphism

$$\left(A \otimes_k A'\right) \otimes_k K = \left(A \otimes_k K\right) \otimes_K \left(A' \otimes_k K\right) \xrightarrow{\sim} M_n(K) \otimes_K M_m(K) = M_{nm}(K)$$

and the result follows from Remark 6.29. □

**Notation 12.11.** For each $n \geq 1$, denote by $\delta_n$ the map

$$\delta_n : H^1\left(G, PGL_n(K)\right) \longrightarrow H^2\left(G, K^\times\right)$$

arising as the boundary homomorphism in the long exact sequence of pointed sets associated to the short exact sequence of $G$-modules

$$1 \longrightarrow K^\times \longrightarrow GL_n(K) \longrightarrow PGL_n(K) \longrightarrow 1$$

defining $PGL_n(K)$ (cf. Lemma 10.67).

**Lemma 12.12.** *For each $m, n \geq 1$, the diagram (of pointed sets)*

$$\begin{array}{ccc} H^1\left(G, PGL_n(K)\right) & \xrightarrow{\delta_n} & H^2\left(G, K^\times\right) \\ \downarrow{\scriptstyle \tilde{\lambda}_{n,m}} & & \| \\ H^1\left(G, PGL_{nm}(K)\right) & \xrightarrow{\delta_{nm}} & H^2\left(G, K^\times\right) \end{array}$$

*commutes.*

*Proof.* Noting that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & GL_n(K) & \longrightarrow & PGL_n(K) & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \lambda_{n,m}} & & \downarrow{\scriptstyle \lambda_{n,m}} & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & GL_{nm}(K) & \longrightarrow & PGL_{nm}(K) & \longrightarrow & 1 \end{array}$$

commutes for all $m, n$, the result follows from functoriality of the bounary homomorphism in the long exact sequences for cohomology associated to the top and bottom rows of the diagram (cf. Lemma 10.67 once again). □

By Lemma 12.12 the maps $\delta_n : H^1(G, PGL_n(K)) \to H^2(G, K^\times)$ are compatible with the maps $\tilde{\lambda}_{n,m}$, and hence induce a map

$$\lim_{\to} H^1(G, PGL_n(K)) \to H^2\left(G, K^\times\right)$$

where the direct limit is taken with respect to the $\tilde{\lambda}_{n,m}$.

**Notation 12.13.** We denote by $\delta_\infty$ the map

$$\lim_{\to} H^1(G, PGL_n(K)) \to H^2\left(G, K^\times\right)$$

induced by the maps $\delta_n$.

**Lemma 12.14.** *The map*

$$\delta_\infty : \lim_{\to} H^1(G, PGL_n(K)) \to H^2\left(G, K^\times\right)$$

*is an injective group homomorphism.*

*Proof.* Note that the group operation on $H^2(G, K^\times)$ is induced by the map on cohomology associated to the homomorphism of $G$-modules $K^\times \times K^\times \to K^\times$ sending $(\lambda, \lambda')$ to $\lambda\lambda'$ along with the identification of $H^2(G, K^\times \times K^\times)$ with $H^2(G, K^\times) \times H^2(G, K^\times)$ provided by Lemma 10.19. Moreover, we have defined the group structure on

$$\lim_{\to} H^1(G, PGL_n(K))$$

as the one induced by the maps on cohomology induced by the maps $PGL_n(K) \times PGL_m(K) \to PGL_{nm}(K)$ on the finite levels.[14] That $\delta_\infty$ is a group homomorphism now follows from taking (for all $n, m$) the long exact sequences for cohomology associated to the commutative diagram of $G$-modules

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times \times K^\times & \longrightarrow & GL_n(K) \times GL_m(K) & \longrightarrow & PGL_n(K) \times PGL_m(K) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & GL_{nm}(K) & \longrightarrow & PGL_{nm}(K) & \longrightarrow & 1 \end{array}$$

whose rows are exact.

Next, for any $n \geq 1$, considering the long exact sequence for cohomology associated to the short exact sequence

$$1 \longrightarrow K^\times \longrightarrow GL_n(K) \longrightarrow PGL_n(K) \longrightarrow 1$$

defining $PGL_n(K)$ and applying Hilbert's Theorem 90, we see that we have an exact sequence of pointed sets

$$1 \longrightarrow H^1(\mathrm{Gal}(K/k), PGL_n(K)) \xrightarrow{\delta_n} H^2\left(\mathrm{Gal}(K/k), K^\times\right).$$

This alone is not enough to show that $\delta_n$ is injective, it only says that the distinguished element in $H^2(\mathrm{Gal}(K/k), K^\times)$ (i.e. 0) has a unique preimage under $\delta_n$. However, since this is true for

[14] Note that if $X$ is not an abelian group then the multiplication map $X \times X \to X$ is *not* a homomorphism, and hence does not induce a product operation on nonabelian $H^1$, unlike in the case of abelian coefficients.

all $n$, $0 \in H^2\left(\mathrm{Gal}(K/k), K^\times\right)$ has a unique preimage under $\delta_\infty$ also. But since $\delta_\infty$ is actually a group homomorphism, this now *is* enough to prove that $\delta_\infty$ is injective. □

**Lemma 12.15.** *When $n = [K : k]$ the map*

$$\delta_n : H^1\left(G, PGL_n(K)\right) \longrightarrow H^2\left(G, K^\times\right)$$

*is surjective.*

*Remark* 12.16. This should not be so surprising in light of the fact that the inclusion of $\mathrm{CSA}_n(K/k)$ into $\mathrm{Br}(K/k)$ is surjective when $n = [K : k]$. Indeed, let $A$ be any central simple algebra over $k$ split by $K/k$. Then its underlying division algebra $D$ is split by $K/k$ also, whence by Theorem 4.30 $\deg(D)$ divides $n$. Writing $n = r\deg(D)$ we see that $A$ is Brauer equivalent to $M_r(D) \in \mathrm{CSA}_n(K/k)$.

*Proof.* The idea of the proof is quite simple, however we spell out the details at length since there are a lot of potential places for confusion due to the many different 'natural' maps between the objects involved.

Consider the (commutative) ring $K \otimes_k K$. We view this as a $K$-algebra (and hence a $K$-vector space) via $\lambda \mapsto 1 \otimes \lambda$, and endow it with the $G$-action given by $g \cdot (x \otimes \lambda) = x \otimes g\lambda$ (this is the usual way of viewing $A \otimes_k K$ as a $K$-algebra with (semilinear) $G$-action for any $k$-algebra $A$; here we are just taking $A = K$). Fix a basis $e_1, ..., e_n$ for $K$ as a $k$-vector space, so that the elements $e_1 \otimes 1, ..., e_n \otimes 1$ give a $K$-vector space basis for $K \otimes_k K$. Now $K \otimes_k K$ acts $K$-linearly on itself by left multiplication so, having fixed the basis above, we obtain a homomorphism $K \otimes_k K \to M_n(K)$. Restricting this to units gives a map

$$(K \otimes_k K)^\times \longrightarrow GL_n(K)$$

which is $G$-equivariant since our chosen basis for $K \otimes_k K$ is $G$-invariant. We now have a commutative diagram of $G$-groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & (K \otimes_k K)^\times & \longrightarrow & (K \otimes_k K)^\times / K^\times & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & GL_n(K) & \longrightarrow & PGL_n(K) & \longrightarrow & 1 \end{array} \tag{12.17}$$

with exact rows, where the inclusion of $K^\times$ into $(K \otimes_k K)^\times$ is via the right factor (i.e. coming from how we view $K \otimes_k K$ as a $K$-algebra) and the rightmost vertical map is induced by the diagram.

**Claim:** As a $G$-module we have

$$(K \otimes_k K)^\times \cong \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G], K^\times\right) = \mathrm{Map}(G, K^\times)$$

with trivial action on $K^\times$ on the right hand side. That is, $(K \otimes_k K)^\times$ is coinduced as a $G$-module.

**Proof of claim:** We'll in fact prove something stronger. We make the $G$-ring

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G], K^\times\right) = \mathrm{Map}(G, K)$$

into a $K$-algebra via

$$(\lambda\phi)(\sigma) = \sigma^{-1}(\lambda)\phi(\sigma)$$

(so that the structure map $K \to \mathrm{Map}(G, K)$ is given by $\lambda \mapsto (\sigma \mapsto \sigma^{-1}\lambda)$). Since for all $\sigma, \tau \in G$, $\lambda \in K$ and $\phi \in \mathrm{Map}(G, K)$ we have

$$\sigma \cdot (\lambda\phi)(\tau) = (\lambda\phi)(\sigma^{-1}\tau) = (\tau^{-1}\sigma)(\lambda)\phi(\sigma^{-1}\tau) = (\sigma(\lambda)\sigma\phi)(\tau)$$

we see that the $G$-action on $\mathrm{Map}(G,K)$ is semilinear. Moreover, $\mathrm{Map}(G,K)^G$ just consists of constant functions, thus is equal to $K$ as a $k$-algebra (but does not have the usual $K$-algebra structure). Thus by Galois decent (Theorem 6.7 and the surrounding discussion), the map

$$K \otimes_k K = \mathrm{Map}(G,K)^G \otimes_k K \xrightarrow{\sim} \mathrm{Map}(G,K)$$

sending $x \otimes y$ to the function $\sigma \mapsto x\sigma^{-1}(y)$ is a $G$-equivariant isomorphism of $K$-algebras. Taking units on each side gives the claim since the invertible functions in $\mathrm{Map}(G,K)$ are precisely those valued in $K^\times$.

Returning to the proof of the lemma, since coinduced modules have no cohomology in degrees greater than 0 (Corollary 10.60) the claim gives $H^2\left(G,(K\otimes_k K)^\times\right)=0$. Taking the long exact sequence(s) for cohomology associated to the commutative diagram (12.17) we find a commutative diagram

$$\begin{array}{ccc} H^1\left(G,(K\otimes_k K)^\times/K^\times\right) & \xrightarrow{\sim} & H^2\left(G,K^\times\right) \\ \downarrow & & \| \\ H^1\left(G,PGL_n(K)\right) & \longrightarrow & H^2\left(G,K^\times\right) \end{array}$$

where the top horizontal map is an isomorphism. In particular, we deduce the surjectivity of the bottom horizontal map and we have the result. □

*Proof of Theorem 12.1.* By Lemma 12.14 $\delta_\infty$ is an injective homomorphism. Moreover, for $n=[K:k]$ the map $\delta_n$ is surjective, whence $\delta_\infty$ is also. Thus $\delta_\infty$ is an isomorphism. Combining this with Lemma 12.8 which gives an isomorphism of groups

$$\mathrm{Br}(K/k) \cong \varinjlim H^1\left(G,PGL_n(K)\right)$$

proves the theorem. □

*Remark* 12.18. There is another, arguably more direct, approach to establishing Theorem 12.1. In general, for any group $G$ and $G$-module $M$, $H^2(G,M)$ is the set of isomorphism classes of group extensions

$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1$$

of $G$ by $M$, such that conjugation in $E$ induces the given $G$-action on $M$ (see [GS06, Example 3.2.6] for the precise statement and proof). Now suppose that we have a central simple algebra $A/k$, split by a Galois extension $K/k$. Then there is a unique central simple algebra (up to $k$-isomorphism) $A'/k$ which is split by $K/k$, is Brauer equivalent to $A$, and has degree $n=[K:k]$ (cf. Remark 12.16). As in Remark 4.31, $K$ embeds in $A'$ as a maximal subfield. Defining $E=\{a\in A'^\times \mid aLa^{-1}\subseteq L\}$ (which is a group under multiplication in $A$), we have a homomorphism $E\to \mathrm{Gal}(K/k)$ sending $a$ to the automorphism $x\mapsto axa^{-1}$ of $K$. By the Skolem–Noether theorem this map is surjective, and its kernel is $C_{A'}(K)\cap A'^\times = K^\times$ since $K$ is a maximal subfield of $A'$. Thus we have a short exact sequence of groups

$$1 \longrightarrow K^\times \longrightarrow E \longrightarrow \mathrm{Gal}(K/k) \longrightarrow 1$$

with conjugation in $E$ inducing the Galois action on $K^\times$. Passing to the isomorphism class of this extension gives an element $H^2\left(\mathrm{Gal}(K/k),K^\times\right)$. In this way we get a map

$$\mathrm{Br}(K/k) \to H^2\left(\mathrm{Gal}(K/k),K^\times\right).$$

We caution that this turns out the be $-1$-times the map considered earlier in this section.

Moreover, given any 2-cocycle (representing a class) in $H^2\left(\mathrm{Gal}(K/k), K^\times\right)$ there is an explicit construction of a central simple algebra $A/k$, a *crossed product algebra*, having $K$ as a maximal subfield. See [Jac89, Section 8.4] for a discussion of crossed product algebras.

## References


[Ami55] S. A. Amitsur, *Generic splitting fields of central simple algebras*, Ann. of Math. (2) **62** (1955), 8–43. MR0070624

[Ami72] ———, *On central division algebras*, Israel J. Math. **12** (1972), 408–420. MR0318216

[Cla] Pete L. Clark, *Noncommutative algebra*, Lecture notes, available at **math.uga.edu/ pete/noncommutativealgebra.pdf**.

[Con] Keith Conrad, *Separability*, Lecture notes, available at **https://kconrad.math.uconn.edu/blurbs/galoistheory/sepa**

[CR90] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1990. With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication. MR1038525

[Gru67] K. Gruenberg, *Profinite groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 1967, pp. 116–127. MR0225922

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR2266528

[Jac89] Nathan Jacobson, *Basic algebra. II*, Second, W. H. Freeman and Company, New York, 1989. MR1009787

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Second, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026

[PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, Math. Res. Lett. **18** (2011), no. 6, 1305–1318. MR2915483

[Ser02] Jean-Pierre Serre, *Galois cohomology*, English, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author. MR1867431

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR1269324



School of Mathematics and Statistics, University of Glasgow, University Place, Glasgow, G12 8QQ.

*Email address*: adam.morgan@glasgow.ac.uk