Central Simple Algebras

Daniel Krashen

February 20, 2015

Contents

Chapter 1

Algebraic Preliminaries

1.1 Notation and conventions

1.1.1 Rings and conventions

Rings are not necessarily commutative. They are always assumed to be associative and unital. Ring homomorphisms are required to be unital. The elements 1 and 0 need not be distinct. The ring R itself is a (non-proper) ideal.

1.1.2 Modules and bimodules

Definition 1.1.1. *Let R be a ring. A left R-module is a set M together with a binary operation*

$$\begin{aligned} R \times M &\to M \\ (r, m) &\to rm \end{aligned}$$

such that

1. $1m = m$,
2. $(r_1 r_2)m = r_1(r_2 m)$,
3. $(r_1 + r_2)m = r_1 m + r_2 m$
4. $r(m_1 + m_2) = rm_1 + rm_2$

Definition 1.1.2. *Let R be a ring. A right R-module is a set M together with a binary operation*

$$\begin{aligned} M \times R &\to M \\ (m, r) &\to mr \end{aligned}$$

such that

1. $m1 = m$,

2. $m(r_1 r_2) = (mr_1)r2$,

3. $m(r_1 + r_2)m = mr_1 + mr_2$

4. $(m_1 + m_2)r = m_1 r + m_2 r$

Notation 1.1.3. *We will occasionally write M_R (respectively ${}_R M$) to denote the fact that M is a right (respectively left) R-module.*

Remark 1.1.4. *Recall that for a ring R, we may define its opposite R^{op} as the ring with the same underlying set and addition, but with the new multiplication rule $\cdot$ defined by $r \cdot s = sr$. In this way, we see that if M is a left R module, then we may define the structure of a right R^{op} module on M via $m \cdot r = rm$. This gives an equivalence of categories between left (right) R-modules and right (left) R^{op} modules.*

Definition 1.1.5. *Let R, S be rings. An $R - S$ bimodule is a set M endowed with a left R-module structure and a right S-module structure such that for all $r \in R, s \in S, m \in M$, we have*

$$r(ms) = (rm)s.$$

Remark 1.1.6. *We note that just as every Abelian group naturally has the structure of a $\mathbb{Z}$-module, every left (resp. right) R-module has the structure of a $R - \mathbb{Z}$ (resp. $\mathbb{Z} - R$) bimodule.*

Notation 1.1.7. *We will write ${}_R M_S$ to denote the fact that M is an $R - S$ bimodule.*

1.2 Some Structure Theory

1.2.1 Simple and Semisimple Modules

Definition 1.2.1. *Let R be a ring. We say that a left R-module P is simple if it is nonzero and if the only submodules of P are 0 and P.*

Definition 1.2.2. *Let R be a ring, P a left R-module. For a subset $X \subset P$, we define $\mathrm{ann}_R(X)$, the annihilator of P in R, to be the set*

$$\mathrm{ann}_R(X) = \{r \in R | rX = 0\}.$$

Note that $\mathrm{ann}_R(X)$ is itself always a left ideal of R. Further, in the case $X = P$, we find that $\mathrm{ann}_R(P)$ is a two-sided ideal of R.

Definition 1.2.3. *A left R-module M is called faithful if $\mathrm{ann}_R(M) = 0$.*

Definition 1.2.4. *An ideal $I < R$ is called left primitive if I is of the form $I = \mathrm{ann}_R(P)$ for some simple left R module P.*

Proposition 1.2.5. *Suppose that P is a nonzero right R-module. The following are equivalent:*

1. *P is simple,*
2. *for every $m \in P\backslash\{0\}$, $mR = P$,*
3. *$P \cong R/I$ for I a maximal right ideal of R,*

Proof.
(1 $\implies$ 2) Suppose P is a simple right R module, and let $m \in P\backslash\{0\}$. Then mR is a nonzero submodule of P and hence we must have $mR = P$.
(2 $\implies$ 3) Choose some $m \in P\backslash\{0\}$. By hypothesis, we have a surjective right R-module map

$$\begin{aligned} R &\to P \\ r &\mapsto mr, \end{aligned}$$

and it follows that $P \cong R/\operatorname{ann}_R(m)$. By the correspondence theorem, since P is simple, it follows that $\operatorname{ann}_R(m)$ must be a maximal right ideal of R.
(3 $\implies$ 1) Follows immediately from the definition of a maximal ideal. □

Definition 1.2.6. *Let R be a ring. We say that a left R-module P is semisimple if it is a direct sum of simple modules.*

Proposition 1.2.7. *Let A be an algebra over a field F, M a semisimple left A-module, finite dimensional as an F vector space, and $P < M$ a submodule. Then P and M/P are also semisimple. Further, we may find a submodule $L \subset M$ such that $L \oplus P = M$.*

We note that the finite dimensionality assumption is not necessary if one appeals to Zorn's Lemma, but we will keep it for simplicity of exposition.

Proof. Since M is semisimple, we may write $M = \oplus M_i$ where M_i are simple. By finite dimensionality, the number of summands is finite. Let $Q < M/P$ be maximal dimensional so that Q is semisimple. Arguing by contradiction, assume that $Q \neq M/P$. It follows that we may find some M_i with the image of M_i in M/P (i.e. $(M_i + P)/P$ not contained in Q. Set $Q_i = (M_i + P)/P$. Then as before, we have $Q \oplus Q_i < M/P$ a semisimple module of larger dimension.

For the remaining parts, choose k minimal such that there exists a decomposition $M = \oplus_{i=1}^{n} M_i$ with each M_i simple, such that the projection $\pi : P \to M \to N = \oplus_{i=1}^{k} M_i$ is injective. We claim that π is an isomorphism. It suffices to show that it is surjective. Regarding M_i as a submodule of N, we note that $\pi P \cap M_i \neq 0$ for each i, since otherwise, the projection onto $\oplus_{\substack{j=1 \\ j\neq i}}^{k} M_j$ would still be injective, contradicting the minimality of k. It therefore follows that, since M_i is simple, each M_i is a submodule of πP, for $i = 1, \ldots, k$, and hence $N \subset \pi P$. But since the reverse inclusion holds by definition, we have $\pi P = N$

and hence π is bijective. This gives an isomorphism $N \cong P$, proving the semismiplicity of P.

Finally, consider $L = \oplus_{i=k+1}^{n} M_i$. We claim that $L \cap P = 0$. To see this, suppose that $x \in L \cap P$. Then by definition of π, it follows that $\pi x = 0$. However, π is injective, and so $x = 0$ as claimed. Next, to finish, we show that $L + P = M$. Choosing $m \in M$, we may write $m = \ell + n$ for $\ell \in L$ and $n \in N$. Since π is an isomorphism, we cna write $n = \pi p$, and consequently, we have $p = n + x$ for $x \in L$. We therefore have

$$m = \ell + n = \ell + p - x = (\ell - x) + p \in L + P$$

as desired. □

1.2.2 Semiprimitive Algebras

Definition 1.2.8. *Let R be a ring. We define $J_r(R)$ (respectively $J_\ell(R)$), the right (left) Jacobson radical of R, to be the intersection of all the maximal right (left) ideals of R.*

In fact, we will show eventually that the right and left Jacobson radicals coincide.

Note that since the annihilator of any element in a simple module is a maximal ideal and every maximal ideal is the annihilator of some element in some simple module, it follows that the right Jacobson radical can also be characterized as the set of elements of R which annihilate every simple right module.

Lemma 1.2.9. *Let R be a ring. Then $J_r(R)$ is a two sided ideal of R.*

Proof. If M is a simple right module for R, then $\mathrm{ann}_R(M)$ is a two sided ideal. Since $J_r(R)$ is the intersection of all such ideals, it is itself an ideal. □

Lemma 1.2.10. *Suppose that A is a finite dimensional F algebra. Then A_A is a semisimple right A module if and only if $J_r(A) = 0$.*

Proof. Suppose that A_A is a semisimple module. Then we may write $A = \oplus P_i$ for some right ideal P_i's which are simple as right A-modules. Consequently, if we define $P_i' = \oplus_{j \neq i} P_i$, then P_i' is a right A-module with $A/P_i' \cong P_i$ simple, and so P_i' is a maximal ideal. But the intersection of the P_i' is 0 which implies $J_r(A) = 0$.

Conversely, if we assume that $J_r(A) = 0$. Since A is finite dimensional, we may find a finite collection of maximal ideals M_i with $\cap M_i = 0$. But this implies that that map $A \to \oplus A/M_i$ is injective, and hence A is isomorphic, as a right A-module, to a submodule of a semisimple module. By Proposition 1.2.7, it follows that A_A is semisimple as desired. □

1.2.3 An ambidextrous characterization of the Jacobson radical

Recall that $r \in R$ is called left invertible if there is some $s \in R$ so that $sr = 1$, and right invertible if there is some $t \in R$ so that $rt = 1$. The elements s and t in these cases are called, respectively, left and right inverses for R. In general it is possible to be right, but not left invertible (or the reverse), and it is not true in general that a one-sided inverse must be unique.

Example 1.2.11. *Let V be the vector space of real valued infinite sequences $(a_0, a_1, \ldots)$, and let R be the ring of linear transformations on R. The linear transformations*

$$\begin{aligned} \sigma, \tau : V &\to V \\ \sigma(a_0, a_1, a_2, \ldots) &= (0, a_0, a_1, \ldots) \\ \tau(a_0, a_1, a_2, \ldots) &= (a_1, a_2, a_3, \ldots) \\ \gamma(a_0, a_1, a_2, \ldots) &= (a_0, a_0, a_1, \ldots), \end{aligned}$$

satisfy $\tau\sigma = \tau\gamma = id$, so that σ and γ are both right inverses for τ. However since as a function, τ is not injective, it follows that it cannot have a left inverse.

Aside 1.2.12. *This situation described above is an "infinite dimensional phemomenon." In particular, if A is a finite dimensional algebra over a field F, then if $a \in A$ has a right (left) inverse, it must also have a left (right) inverse.*

Proof. To see this, we note that if a has a right inverse, then it must be, as a linear transformation from A to itself, surjective. By finite dimensionality, it must therefore also be injective, and hence invertible as a linear transformation. This means that its determinant must be nonzero. If we consider its characteristic polynomial (as a linear transformation),

$$\chi_a(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$$

then we have $c_0 = \pm det(a) \neq 0$, and since $\chi_a(a) = 0$, by the Cayley-Hamilton Theorem, we have

$$(-a_0^{-1})(a^{n-1} + c_{n-1}a^{n-2} + \cdots c_1)a = 1$$

and hence a has a left inverse as well. In fact, it quickly follows both from this explicit description, as well as the next result, that its right and left inverse are the same. □

In general, if an element of a ring has both a right and a left inverse, these must coincide and be unique:

Lemma 1.2.13. *Let R be a ring, $r \in R$ and suppose that $s, t \in R$ with $sr = 1 = rt$. Then $s = t$.*

Proof. We have $s = s1 = srt = 1t = t$. □

If $r \in R$ has both a left and a right inverse, we simply say that it is invertible, and can speak of its uniquely defined inverse.

Definition 1.2.14. *Let R be a ring, and $r \in R$. We say that r is left quasiregular if $1 - r$ has a left inverse, right quasiregular if $1 - r$ has a right inverse, and simply quasiregular it is both left and right quasiregular.*

Lemma 1.2.15. *Suppose that I is a right ideal all of whose element are right quasiregular. Then all of its elements are quasiregular.*

Proof. Let $x \in I$. We have by hypothesis that $(1-x)s = 1$. Writing $y = 1 - s$ we may write this as $(1-x)(1-y) = 1$ and so $xy - x - y = 0$, yielding $y = -x(1-y) \in I$. Consequently, y is right quasiregular, and it follows that $(1-y)$ is right invertible. But since $(1-x)$ is a left inverse for $(1-y)$, it is invertible with $(1-x)$. But this means that $(1-x)$ is also invertible with inverse $(1-y)$. This means that x is quasiregular as claimed. □

Lemma 1.2.16. *Let R be a ring. Then every element $x \in J_r(R) \cup J_\ell(R)$ is quasiregular.*

Proof. By the previous result, and by symmetry, it suffices to show that every element of $J_r(R)$ is right quasiregular. Let $x \in J_r(R)$. Since x is contained in every maximal right ideal, it follows that $1 - x$ is contained in no maximal ieals. But this implies that the right ideal generated by $1 - x$ must be the whole right R, which tells us in turn that it is right invertible, and hence x is right quasiregular as claimed. □

Lemma 1.2.17. *Suppose that I is an ideal of R such that every element of I is quasiregular. Then $I \subset J_r(R) \cap J_\ell(R)$.*

Proof. By symmetry, it suffices to show that $I \subset J_r(R)$. Suppose that K is a maximal right ideal of R, and consider $K + I$. We will show that $I \subset K$ by contradiction. Since $J_r(R)$ is the intersection of all maximal ideals, it will follow that $I \subset J_r(R)$. If $I \not\subset K$, we would have, by maximality of K, that $K + I = R$. But then we can write $1 = k + x$, with $k \in K$ and $x \in I$, so that $k = 1 - x$. But since x is quasiregular, k is invertible and hence $K = R$ would not be maximal. Therefore $I \subset K$ as desired. □

Corollary 1.2.18. *Let R be a ring. Then $J_r(R) = J_\ell(R)$ is the ideal of R which is maximal with respect to the property that each of its elements are quasiregular.*

It therefore makes sense to define the Jacobson radical of R, to be $J(R) = J_r(R) = J_\ell(R)$.

Definition 1.2.19. *We say that a ring R is* ***semiprimitive*** *if $J(R) = 0$.*

1.2.4 Endomorphisms: Schur and Wedderburn-Artin

The main observation of this section is that if R is a ring, then regarding R as a right module over itself, we have a natural identification $R \cong End_R(R_R)$. This means that by studying the structure of Endomorphism rings of modules, we can get to the structure of arbitrary rings.

Let us first consider the structure of endomorphism rings of simple modules:

Theorem 1.2.20 (Schur's Lemma)**.** *Let P be a simple right R module, and let $D = End_R(P_R)$. Then D is a division ring.*

Proof. Suppose that $f \in D\backslash\{0\}$. We must show that f is invertible. But note that f, considered as a homomorphism from P to itself, has a kernel and image which are both submodules of P. Since P has no submodules other than 0 and P, and since f is not the 0 map, it follows that the kernel must be 0 and the image must be P. But this implies that

f is both injective and surjective, and hence f is invertible as a map of sets. Writing g for f^{-1}, one may check that g is also a right R-module homomorphism, and hence $g \in D$ is an inverse for f as desired. $\square$

To examine semisimple modules, it will be useful to consider matrix notation. Let $M = \oplus_{j=1}^{m} M_j$ and $N = \oplus_{i=1}^{n} N_i$ be right R-modules, each written as a finite direct sum. If $f : M \to N$ is a homomorphism, f is determined by its values on each of the submodules M_j. Moreover, $f_j = f|_{M_j}$ can be written as a tuple of maps $(f_{1,j}, f_{2,j}, \ldots, f_{m,j})$ where each $f_{i,j}$ is a homomorphism from M_j to N_i. We may represent this in matrix notation as follows:

$$f = \begin{bmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,n} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,n} \\ \vdots & \vdots & & \vdots \\ f_{m,1} & f_{m,2} & \cdots & f_{m,n} \end{bmatrix}$$

and one may check that composition of functions fg precisely corresponds to matrix multiplication and composition of endomorphisms within each entry of the product. Consequently, we have:

Lemma 1.2.21. *Let R be a ring, $M = \oplus_{j=1}^{m} M_j$. Then $End_R(M)$ is isomorphic to the ring of matrices of the form*

$$\begin{bmatrix} Hom_R(M_1, M_1) & Hom_R(M_1, M_2) & \cdots & Hom_R(M_1, M_n) \\ Hom_R(M_2, M_1) & Hom_R(M_2, M_2) & \cdots & Hom_R(M_2, M_n) \\ \vdots & \vdots & & \vdots \\ Hom_R(M_m, M_1) & Hom_R(M_m, M_2) & \cdots & Hom_R(M_m, M_n) \end{bmatrix}$$

with the natural ring structure inhereted by matrix addition and multiplication.

Theorem 1.2.22 (Wedderburn-Artin)**.** *Let A be a finite dimensional algebra over a field F, and suppose that $J(A) = 0$. Then we may write $A = \oplus (P_i)^{d_j}$ as a direct sum of minimal right ideals, and $A \cong \oplus_{i=1}^{n} M_{d_i}(D_i)$, where each $D_i = End_A(P_i)$ is a division algebra.*

Proof. Since $J(A) = 0$, A_A is a semisimple right A-module, and we can write $A_A = \oplus_{i=1}^{n} (P_i)^{d_i}$, where the P_i's are distinct, and mutually nonisomorphic simple right R-modules (and hence minimal right ideals). Since the P_i's are nonisomorphic and simple, it follows that $Hom_{P_i, P_j} = 0$ if $i \neq j$ and is isomorphic to a division algebra D_i if $i = j$. It therefore follows that $End_A(A_A)$ consists of block diagonal matrices with the algebras of the form $M_{d_i}(D_i)$ along the diagonal. The result follows. $\square$

Corollary 1.2.23 (Wedderburn Structure Theorem)**.** *Let A be a simple finite dimensional algebra over a field F. Then $A_A = P^d$ for some minimal right ideal $P <_r A$ and some positive integer d. Further, $A \cong M_d(D)$ where $D = End_A(P)$ is a division algebra.*

Proof. Since A is simple, we have $J(A) = 0$. By the Wedderburn-Artin Theorem, it follows that $A \cong \oplus_i M_{d_i}(D_i)$, where each D_i has the form $End_A(P_i^{d_i})$. But since each of these factors would be an ideal of A, and A is simple, it follows that there is only one index i, and so $A = P^d$, with $A \cong M_d(D)$ as claimed. □

Corollary 1.2.24. *Suppose that A is a simple, finite dimensional algebra over a field F. Then all simple right A modules are isomorphic. In particular, all the minimal right ideals of A are isomorphic as right A-modules.*

Proof. Suppose that P, Q are minimal right ideals which are nonisomorphic right A-modules. Since A is simple, $J(A) = 0$ and A_A is semisimple. Write $A_A = \oplus P_i$. Since we have nontrivial homomorphisms $P, Q \to A_A$, it follows that we must have nontrivial homomorphisms $P \to P_i$, $Q \to P_j$ some i, j. But since all these are simple modules, we therefore have $P \cong P_i$ and $Q \cong P_j$. By the Wedderburn-Artin Theorem, it follows that we have at least two distinct factors in the representation $A \cong \oplus_i M_{d_i}(D_i)$, contradicting the simplicity of A. □

1.3 Tensors and commutators

1.3.1 Tensor products of algebras

Definition and universal property

Let F be a field, and A, B F-algebras. Then the vector space tensor product $A \otimes_F B$ can be given the structure of an F-algebra via, defining for simple tensors:

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

Under this definition, we find that A, B are naturally isomorphic to subalgebras of $A \otimes_F B$, as $A \otimes 1$ and $B \otimes 1$ respectively, and furthermore, these images of the algebras commute inside $A \otimes_F B$. In fact, this characterizes the tensor product of algebras:

Proposition 1.3.1. *Suppose that A, B are F-algebras. Then for any F-algebra C, the set of homomorphisms $A \otimes B \to C$ are in bijection with pairs of homomorphisms $A \to C$, $B \to C$ such that the images of A and B in C commute (via restriction to the subalgebras defined above).*

Proof. Clearly, if we are given a homomorphism $\phi : A \otimes B \to C$, we obtain by restriction to the subalgebras $A \otimes 1$ and $1 \otimes B$, corresponding homomoprhisms from A and B. Since $A \otimes B$ is generated by these subalgebras, it follows that the homomorphism ϕ is determined by these restrictions. Since $a \otimes 1$ and $1 \otimes b$ commute in $A \otimes B$, it follows that the images of A and B commute in C.

It remains simply to show that every pair of maps $\alpha : A \to C$, $\beta : B \to C$ with αA commuting with βB is induced by a map $A \otimes B \to C$. To see this, consider the map

$$\phi : A \times B \to C$$

defined by $\phi(a,b) = ab$. This is a bilinear map and therefore induces a map $\widetilde{\phi} : A \otimes B \to C$ such that $\widetilde{\phi}(a \otimes b) = (\alpha a)(\beta b)$. To see that this is a homomorphisms, we check

$$\begin{aligned}
\phi\left((\sum a_i \otimes b_i)(\sum a'_j \otimes b'_j)\right) &= \phi\left(\sum_{i,j} a_i a'_j \otimes b_i b'_j\right) \\
&= \sum_{i,j} \phi(a_i a'_j \otimes b_i b'_j) \\
&= \sum_{i,j} \alpha(a_i a'_j)\beta(b_i b'_j) \\
&= \sum_{i,j} \alpha(a_i)\alpha(a'_j)\beta(b_i)\beta(b'_j) \\
&= \sum_{i,j} \alpha(a_i)\beta(b_i)\alpha(a'_j)\beta(b'_j) \\
&= \left(\sum \alpha(a_i)\beta(b_i)\right)\left(\sum \alpha(a'_j)\beta(b'_j)\right) \\
&= \phi\left(\sum a_i \otimes b_i\right)\phi\left(\sum a'_j \otimes b'_j\right)
\end{aligned}$$

□

Description via structure constants

Suppose that A is a finite dimensional F-algebra. if $\{e_i\}$ is a basis for A, ...

1.3.2 Tensors and bimodules

Let F be a field, A and B F-algebras. If M is an $A - B$ bimodule then we have algebra homomorphisms $A \to \mathrm{End}_F(M)$ and $B^{op} \to \mathrm{End}_F(M)$. The statement that these give a bimodule structure is exactly the statement the the images of these maps commute in the endomorphism ring.

Proposition 1.3.2. *Let A, B be F-algebras. Then we have natural equivalences between the following categories*

1. *$A - B$ bimodules,*
2. *F-algebra homomorphisms $A \otimes B^{op} \to \mathrm{End}_F(M)$,*
3. *$A \otimes B^{op}$-modules.*

1.3.3 Commutators and endomorphisms

Recall that if R is a ring, $L \subset R$ any subset, the centralizer of L in R, $C_R(L)$ is defined to be the set of $r \in R$ which commute with every element of L.

Let F be a field, A an F-algebra, and M a right A-module. The right A-module structure of M gives rise to a homomorphism of F-algebras

$$f : A^{op} \to \mathrm{End}_F(M).$$

We can then characterize the endomorphisms of M as a right A-module as those linear transformations $b : M \to M$ such that

$$b(ma) = (b(m))a,$$

or in other words, $\mathrm{End}_A(M) = C_{\mathrm{End}_F(M)}(f(A))$.

Notation 1.3.3. *If A is an F-algebra, M a right A-module, we regard elements of $\mathrm{End}_A(M)$ as acting on the left of M, using the standard convention of functions (in $\mathrm{End}_F(M)$) acting on the left. On the other hand, if N is a left A-module, we will instead choose to regard A-module endomorphisms of N as acting on the right, and therefore will consider N as a right $\mathrm{End}_A(N)^{op}$-module, following therefore the convention of functions composing left to right instead of right to left.*

That is to say, if $f, g \in \mathrm{End}_A(N)$, we will write nf for $f(n)$, and nfg to represent $g(f(n)) = gf(n)$.

1.3.4 A double commutator theorem

To begin, let's set up a few basic facts about computing commutators in tensor products.

Lemma 1.3.4. *Suppose that A and B are F-algebras, and $A' \subset A$, $B' \subset B$ are subalgebras. Then $C_{A\otimes B}(A' \otimes B') = C_A(A') \otimes C_B(B')$.*

Proof. Suppose that $\sum a_i \otimes b_i \in C_{A\otimes B}(A' \otimes B')$. Without loss of generality, we may assume that the $\{b_i\}$ and $\{a_i\}$ are both linearly independent sets, respectively. If $a' \in A'$, then we have

$$0 = (a' \otimes 1)\sum a_i \otimes b_i - \left(\sum a_i \otimes b_i\right) a' \otimes 1 = \sum (a'a_i - a_i a') \otimes b_i$$

and since the b_i are independent, this implies $a_i \in C_A(A')$ for each i. Similarly, we find that $b_i \in C_B(B')$ and so $C_{A\otimes B}(A' \otimes B') \subset C_A(A') \otimes C_B(B')$. The reverse inclusion is immediate. □

Lemma 1.3.5. *Let F be a field. Then $Z(M_n(F)) = F$.*

Proof. Let $a = \sum_{i,j} a_{i,j} e_{i,j} \in Z(M_n(F))$, then a must commute with each matrix unit $e_{k,\ell}$. We therefore have

$$0 = e_{k,\ell}a - ae_{k,\ell} = \sum_{i,j} a_{i,j} e_{k,\ell} e_{i,j} - \sum_{i,j} a_{i,j} e_{i,j} e_{k,\ell} = \sum_j a_{\ell,j} e_{k,j} - \sum_i a_{i,k} e_{i,\ell}.$$

Consequently, we must have that each coefficient of the $e_{p,q}$s is 0. For $p \neq k$, this says that $a_{p,k} = 0$ and for $q \neq \ell$, this says that $a_{\ell,q} = 0$. It follows that such an a must be diagonal, of the form $a = \sum a_{i,i}e_{i,i}$. In this case, the commutator now looks like:

$$e_{k,\ell}a - ae_{k,\ell} = \sum_i a_{i,i}e_{k,\ell}e_{i,i} - \sum_i a_{i,i}e_{i,i}e_{k,\ell} = a_{\ell,\ell}e_{k,\ell} - a_{k,k}e_{k,\ell} = (a_{\ell,\ell} - a_{k,k}).$$

It then follows that for these to commute, a must be of the form λI_n, for some $\lambda \in F$. □

Lemma 1.3.6. *Suppose that $B \subset A$ are F-algebras. We may consider the inclusions*

$$B \subset A \subset M_n(A)$$

where the latter is induced by mapping the element a to the diagonal matrix aI_n. Then

1. $C_{M_n(A)}(B) = M_n(C_A(B))$,
2. $C_{M_n(A)}(M_n(B)) = C_A(B)I_n$.

Proof. Writing $M_n(A) = M_n(F) \otimes A$, we have by Lemma 1.3.4

$$C_{M_n(A)}(B) = C_{M_n(F)\otimes A}(1 \otimes B) = M_n(F) \otimes C_A(B) = M_n(C_A(F)).$$

Similarly, we have

$$\begin{aligned} C_{M_n(A)}(M_n(B)) = C_{M_n(F)\otimes A}(M_n(F) \otimes B) &= C_{M_n(F)}(M_n(F)) \otimes C_A(B) \\ &= Z(M_n(F)) \otimes C_A(B) = F \otimes C_A(B) = C_A(B). \end{aligned}$$

□

Theorem 1.3.7 (Double Centralizer, Warm-Up Version 1)**.** *Let B be an F-algebra, and M a faithful semisimple right B-module, finite dimensional as an F-vector space. Let $E = \mathrm{End}_F(M)$, regard B^{op} as a subalgebra of E via its right multiplication action. Then we have $B^{op} = C_E(C_E(B^{op}))$.*

Proof. Let $\phi \in C_E(C_E(B^{op}))$, and choose $m_1, \ldots, m_n$ a basis for M over F. As in the convention of Notation 1.3.3, E and $C_E(B^{op})$ act on the left on M, and $C_E(C_E(B^{op}))$ act on the right.

Set $N = \oplus^n M$, and let $w = (m_1, \ldots, m_n) \in N$. Since N is semisimple as a right B-module, we can write $N = wB \oplus N'$ as right B-modules, and let $\pi : N \to mB \to N$ be the projection. The map $\phi \in E$ acts naturally (diagonally) on N as $\phi I_n \in M_n(E) = \mathrm{End}_F(N)$, and since the m_i are a basis, it follows that the action of ϕ on M is determined by its action on $w \in N$. It therefore suffices to show that we can find $b \in B$ such that $w\phi = wb$.

To see this, we note that since π is a right B-module homomorphism, we have by Lemma 1.3.6(1),

$$\pi \in C_{M_n(E)}(B^{op}) = M_n(C_E(B^{op})).$$

Further, we see that the action of ϕ on N as ϕI_n satisfies

$$\phi \in C_E(C_E(B^{op}))I_n = C_{M_n(E)}(M_n(C_E(B^{op}))),$$

by Lemma 1.3.6(2). Consequently, the actions of π and ϕ on N commute, and we have, since $w = \pi w$,

$$w\phi = (\pi w)\phi = \pi(w\phi) \in wB.$$

This means we may write $w\phi = wb$ some $b \in B$, as desired. □

Chapter 2

Idempotents

2.1 Basic Notions

In a ring R, an **idempotent** element $e \in R$ is one with $e^2 = e$. Of course, the most obvious example of these are the elements 0 and 1, and in case R is, for example, a commutative domain, it is immediate that these are the only possible such elements. We call 0 and 1 trivial idempotents.

Another important source of examples are projection maps: if V is a vector space with $V = W \oplus U$, then the projection map $\pi_W : V \to V$ defined by $\pi_W(w, u) = (w, 0)$ is a nontrivial idempotent linear transformation in the ring $\mathrm{End}(V)$. We will see that, in some sense, idempotents can be thought of as "projections," and correspond to certain decompositions.

Definition 2.1.1. *We say that idempotent elements $e, f \in R$ are **complementary** if $e + f = 1$. We say that they are **orthogonal** if $ef = fe = 0$.*

Note that if e is an idempotent, then so is $1 - e$ since

$$(1 - e)^2 = 1 - 2e + e^2 = 1 - 2e + e == 1 - e.$$

It is also easy to see that the idempotents e and $1 - e$ are also complementary.

Definition 2.1.2. *Let $e \in R$ be an idempotent. We say that e is **primitive** if we cannot write $e = e_1 + e_2$ for nontrivial idempotents e_1, e_2.*

Definition 2.1.3. *Let $e_1, \ldots, e_n \in R$ be idempotents. We say that these are a **complete** set of idempotents if $\sum e_i = 1$.*

2.2 Ring decompositions

2.2.1 Central idempotents and product decompositions

Suppose that $e \in R$ is a central idempotent – that is, e is an idempotent and $e \in Z(R)$. In this case, if we set $f = 1 - e$ to be the complementary idempotent, we have

$$R = R \cdot 1 = Re + Rf.$$

Since e is central, it is easy to check that Re is both additively and multiplicatively closed, and hence is itself a ring, with identity element e. Similarly Rf is a ring with identify f. We also see that $Re \cap Rf = 0$ since if $r = ae = bf$ then $r = aee = bfe = b0 = 0$. Hence we have a product decomposition

$$R = Re \times Rf.$$

These observations naturally extend to give the following Proposition, the proof of which is left to the reader.

Proposition 2.2.1. *Let R be a ring. Then there is a bijective correspondence*

$$\left\{\begin{array}{c} e_1, \ldots, e_n \text{ a complete set of pairwise} \\ \text{orthogonal central idempotents} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} \text{decompositions of the form} \\ R = R_1 \times \cdots \times R_n \end{array}\right\}.$$

given by

$$(e_1, \ldots, e_n) \mapsto \big(R = Re_1 \times \cdots \times Re_n\big)$$

and where the reverse is given by setting e_i to be the element $(0, \ldots, 0, 1, 0, \ldots, 0)$ with a 1 in the ith place.

2.2.2 Pierce decomposition

In the case of a noncentral idempotent $e \in R$, although eR is no longer a ring, eRe does have the structure of a ring. Furthermore, eR has the structure of an $eRe - R$ bimodule. We will take advantage of this fact, together with the fact that we may identify

$$R = Hom_R(R_R).$$

Proposition 2.2.2. *Let $e_1, \ldots, e_n \in R$ be a complete set of orthogonal idempotents. Then we have $e_iRe_j = Hom_R(e_jR, e_iR)$, induced via left multiplication.*

Proof. Note that we have an injection $R \to \mathrm{End}_R(R_R) = \mathrm{End}_R(\oplus e_iR)$, and as in Lemma 1.2.21, we may therefore represent R as matrices of the form

$$\begin{bmatrix} Hom_R(e_1R, e_1R) & Hom_R(e_1R, e_2R) & \cdots & Hom_R(e_1R, e_nR) \\ Hom_R(e_2R, e_1R) & Hom_R(e_2R, e_2R) & \cdots & Hom_R(e_2R, e_nR) \\ \vdots & \vdots & & \vdots \\ Hom_R(e_nR, e_1R) & Hom_R(e_nR, e_2R) & \cdots & Hom_R(e_nR, e_nR) \end{bmatrix}$$

which is to say that we also obtain a decomposition of R in its left multiplication action on itself as $R = \oplus Hom_R(e_jR, e_iR)$. Said another way, this means that for each $r \in R$, we have a natural decomposition $r = \sum r_{i,j}$ where $r_{i,j}$ induces a map from e_jR to e_iR via left multiplication, and such that $r_{i,j}e_kR = 0$ for $k \neq j$. If we compare this to the decomposition given by the idempotents via

$$r = 1r1 = \left(\sum e_i\right) r \left(\sum e_j\right) = \sum_{i,j} e_i r e_j$$

that $e_i r e_j e_k R = 0$ for $k \neq j$ and lies in e_iR, that $r_{i,j} = e_i r e_j$. In particular, it follows that we have $e_iRe_j = Hom(e_jR, e_iR)$ via left multiplication as claimed. □

2.3 Galois extensions

The tensor product of a Galois field extension with itself provides a nice example of idempotent elements with interesting structure relating to the Galois action. This example will be useful later as well.

Let E/F be a Galois extension. That is, $E = F[t]/f(t)$ where f is a separable, irreducible polynomial, and where E/F is normal.

If we write

$$E \otimes E = E \otimes F[t]/f(t) = E[t]/f(t),$$

then we find, by the assumption of normality, that since $f(t)$ has a root in E, it must completely split in E, and we have:

$$E \otimes E = E[t]/\prod\prod(t - \alpha_i) = \bigtimes E[t]/(t - \alpha_i) \cong \bigtimes^{n} Ee_i,$$

where e_i is the idempotent element of $E \otimes E$ corresponding the the factor in the product. Of course, since the Galois group G acts simply and transitively on the roots α_i, choosing $\alpha = \alpha_1$, we may also write this as:

$$E \otimes E = \bigtimes_{\sigma \in G} E[t]/(t - \sigma(\alpha)) \cong \bigtimes_{\sigma \in G} Ee_\sigma.$$

Consider the projection onto the σ factor $\pi_\sigma : E \otimes E \to Ee_\sigma$. Since $x \otimes 1$ maps to the constant polynomial x in $E[t]/(t - \sigma(\alpha))$, and $1 \otimes \alpha$ maps to $\sigma(\alpha)$, we find that $\pi_\sigma(x \otimes y) = x\sigma(y)$ for $x, y, \in E$. Since this projection is defined also by multiplication by the idempotent e_σ, we therefore have

$$(x \otimes y)e_\sigma = x\sigma(y)e_\sigma,$$

and therefore

$$(1 \otimes y)e_\sigma = \sigma(y)e_\sigma = (\sigma(y) \otimes 1)e_\sigma.$$

In particular, we have $(x \otimes y)e_1 = (y \otimes x)e_1$.

Chapter 3

The Structure of Central Simple Algebras

3.1 Definition and invariants

3.1.1 Characterizing central simple algebras

Definition 3.1.1. *Let F be a field, and A an F-algebra. We say that A is F-central if $Z(A) = F$ and $\dim_F(A)$ is finite.*

Definition 3.1.2. *Let F be a field and A an F-algebra. We say that A is a central simple algebra over F (a csa/F for short), if*

1. *A is simple as a ring (no 2-sided ideals) and*
2. *A is F-central.*

A particularly important case of this is if D is a finite dimensional division algebra over F with $Z(D) = F$. In this case, D is called a central division algebra over F (a *cda*/F for short).

Proposition 3.1.3. *Let F be a field. The following are equivalent:*

1. *A is a csa/F,*
2. *$A \cong M_n(D)$ for some D, a cda/F.*

Further, in part (2), D is uniquely defined up to isomorphism by A.

Proof. Assuming that A is a *csa*/F, it follows from the Wedderburn structure Theorem (Corollary 1.2.23), that we have $A \cong M_n(D)$ for some division algebra D over F, where D may be identified as $\mathrm{End}_A(P)$ for a simple right module P, and P is uniquely determined

up to isomorphism by Corollary 1.2.24. Consequently, D is uniquely determined up to isomorphism by A. To see that D is a cda/F, we note that by Lemma 1.3.6(2),

$$F = Z(A) = Z(M_n(D)) = C_{M_n(D)}(M_n(D)) = Z(D)I_n = Z(D).$$

On the other hand, assuming that D is a cda/F, if $A = M_n(D)$ it follows from computation with matrix units $e_{i,j}$ that A is a simple algebra. Again by Lemma 1.3.6(2), we have $Z(A) = Z(M_n(D)) = Z(D)$. Since $Z(D) = F$, this shows that A is central. □

Given any F-algebra A, we may regard A has having the structure of an $A-A$ bimodule. This induces an F-algebra homomorphism

$$\begin{aligned} A \otimes A^{op} &\to \mathrm{End}_F(A) \\ a \otimes b &\mapsto \big(x \mapsto axb\big) \end{aligned}$$

often referred to as the sandwich map.

Theorem 3.1.4. *Let F be a field and A a finite dimensional F-algebra. Then A is a csa/F if and only if the sandwich map $A \otimes A^{op} \to \mathrm{End}_F(A)$ is an isomorphism.*

Proof. On the one hand, suppose that the sandwich map is an isomorphism. We can see that A is simple since if it did have a proper ideal $I \lhd A$, then $I \otimes A^{op}$ would be a proper ideal (one may verify properness by considering its dimension as an F-vector space). However, tihs would contradict the fact that $\mathrm{End}_F(A) = M_{\dim A}(F)$ is a simple algebra. To see that A is central, we note that if $a \in Z(A)$, then

$$a \otimes 1 \in Z(A \otimes A^{op}) = Z(\mathrm{End}_F(A)) = Z(M_{\dim A}(F)) = F.$$

If a is not in the F-span of $1 \in A$, then it would follow that $a \otimes 1$ and $1 \otimes 1$ would be linearly independent and hence $a \otimes 1$ would not be in the F-span of $1 \otimes 1 = 1_{A \otimes A^{op}}$, contradicting the fact that $a \otimes 1 \in Z(A \otimes A^{op}) = F$. It therefore follows that $a \in F \cdot 1$, and so $Z(A) = F$ as claimed.

Next suppose that A is a csa/F. To see that the sandwich map is an isomorphism, we note that since both sides are vector spaces over F of dimension $(\dim_F(A))^2$, it suffices to check that the map is surjective. Let $B \subset \mathrm{End}_F(A)$ be the image of $A \otimes A^{op}$. Since A is a simple algebra, it is a simple left $A \otimes A^{op}$ module, and hence a simple left B-module.

Consider the centralizer $C_{\mathrm{End}_F(A)}(B)$. If $f : A \to A \in \mathrm{End}_F(A)$ is an element of this centralizer, then setting $x = f(1) \in A$, we find that for $a \in A$, we have $f(a) = f((a \otimes 1)1) = a \otimes 1 f(1) = a \cdot x \cdot 1 = ax$, and so f is determined by its value on 1. On the other hand, since f also must commute with the right action of A (i.e. the left module action of A^{op} from the bimodule structure), we have

$$ax = f(a) = f((1 \otimes a)1) = (1 \otimes a)f(1) = xa$$

for every $x \in A$, which tells us that $a \in Z(A) = F$. Consequently, we find $C_{\mathrm{End}_F(A)}(B) = F$.

Since A is a simple algebra, it is a simple left $A \otimes A^{op}$ module, and it is a simple left B module, and therefore also a semisimple B-module. By the Double Centralizer Theorem, Warm-Up Version 1 (Theorem 1.3.7), we therefore have have

$$B = C_{\mathrm{End}(A)}(C_{\mathrm{End}(A)}(B)) = C_{\mathrm{End}(A)}(F) = \mathrm{End}(A),$$

and so the sandwich map is surjective. □

Theorem 3.1.5. *Suppose that A/F is an algebra. Then the following are equivalent:*

1. *A is a csa/F,*
2. *the sandwich map $A \otimes A^{op} \to \mathrm{End}_F(A)$ is an isomorphism,*
3. *$A \otimes_F B \cong M_m(F)$ for some F-algebra B and some positive integer m,*
4. *$A \otimes_F \overline{F} \cong M_n(\overline{F})$ for some positive integer n,*
5. *$A \otimes_F L \cong M_n(L)$ for some field extension L/F and some positive integer n.*

Proof. The equivalence of (1) and (2) follows from Theorem 3.1.4, and the implication (2) $\implies$ (3) is immediate.

To check (3) $\implies$ (4), we note that the isomorphism $A \otimes B \cong M_n(F)$ yields an isomorphism $(A \otimes_F \overline{F}) \otimes_{\overline{F}} (B \otimes_F \overline{F})$, and so it follows that $A \otimes_F \overline{F}$ is a central simple $\overline{F}$-algebra. By the Wedderburn Structure Theorem (Corollary 1.2.23), we have $A \otimes \overline{F} \cong M_n(D)$ for some finite dimensional division algebra D over $\overline{F}$. But note that for every $d \in D$, $\overline{F}(d) \subset D$ is a commutative finite dimensional domain, and hence a field. Since this means that $\overline{F}(d)/\overline{F}$ is a finite field extension, and $\overline{F}$ is algebraically closed, it follows that $D = \overline{F}$ and so $A \otimes_F \overline{F} \cong M_n(\overline{F})$ as claimed.

Clearly (4) $\implies$ (5), and so to complete the proof, we need only show that (5) $\implies$ (1). So, suppose that $A \otimes_F L \cong M_n(L)$ for some field extension L/F. If $I \lhd A$ is a two-sided ideal, then $I \otimes L$ is a two-sided ideal of $A \otimes L = M_n(L)$ of dimension $(\dim I)(\dim L)$. In particular, I is proper if and only if $I \otimes L$ is proper. Since $A \otimes L \cong M_n(L)$ is simple, it follows that A has no proper ideals and is therefore also simple. Similarly, we note that if $a \in Z(A)$, then $a \otimes 1 \in Z(A \otimes L) = 1 \otimes L$. By Proposition A.3.1, if $a \notin F$, then $a \otimes 1$ would be independent from the F-subspace $1 \otimes L$ in $A \otimes L$, and it would follow that $a \notin Z(A)$ contradicting our assumption. Therefore, we must have $a \in F$ and so $Z(A) = F$ as claimed.

□

Lemma 3.1.6. *Suppose A is an F-algebra. Then the following are equivalent:*

1. *A is a csa/F,*
2. *for every field extension L/F, $A \otimes_F L$ is a csa/L.*
3. *for some field extension L/F, $A \otimes_F L$ is a csa/L,*

Proof. If A is a csa/F, let L/F be a field extension, and $\overline{L}$ the algebraic closure of L. Since $F \subset L \subset \overline{L}$ and $\overline{L}$ is algebraically closed, we may choose an algebraic closure $\overline{F}$ inside of $\overline{L}$. Since $A \otimes \overline{F} \cong M_n(\overline{F})$, it follows that

$$(A \otimes_F L) \otimes_L \overline{L} = A \otimes_F \overline{L} = A \otimes_F \overline{F} \otimes_{\overline{F}} \overline{L} \cong M_n(\overline{F}) \otimes_{\overline{F}} \overline{L} = M_n(\overline{L})$$

and so $A \otimes_F L$ is a csa/L by Theorem 3.1.5.

On the other hand, Supposing that $A \otimes L$ is a csa/L for some field extension L/F, we find that, by identifying the sandwich map

$$\sigma_{A \otimes L} : (A \otimes L) \otimes_L (A \otimes L)^{op} \to \mathrm{End}_L(A \otimes L),$$

with the sandwich map for A tensored with L

$$\sigma_A \otimes_F L : A \otimes A^{op} \otimes L \to \mathrm{End}_F(A) \otimes_F L,$$

that since $\sigma_{A \otimes L}$ is an isomorphism by Theorem 3.1.5, so is σ by Lemma A.4.4. Therefore again by Theorem 3.1.5, it follows that A is a csa/F. □

Lemma 3.1.6 is useful as it helps us to understand the effect of taking tensor products of simple algebras.

Lemma 3.1.7. *Suppose that A, B are central simple algebras over F. Then so is $A \otimes_F B$.*

Proof. By Lemma 3.1.6, we may assume that $F = \overline{F}$. But now from Theorem 3.1.5 this follows from the fact that $M_n(M_m(F)) \cong M_{nm}(F)$. □

Lemma 3.1.8. *Suppose that A is a csa/F and B is a simple, finite dimensional F-algebra. Then $A \otimes_F B$ is a central simple $Z(B)$-algebra.*

Proof. We may identify

$$A \otimes B = A \otimes_F (L \otimes_L B) = (A \otimes_F L) \otimes_L B.$$

By Lemma 3.1.6, $A \otimes L$ is a csa/L and so by Lemma 3.1.7, $A \otimes B \cong (A \otimes_F L) \otimes_L B$ is as well. □

3.1.2 The degree and the index

It follows from the results of the last section that the dimension of a central simple algebra A over F is always a square, since dimension is preserved by scalar extensions, and since $A \otimes_F \overline{F} \cong M_n(\overline{F})$.

Definition 3.1.9. *Let A be a csa/F. We define the degree of A,* $\deg(A) = \sqrt{\dim_F(A)}$.

Definition 3.1.10. *Let A be a csa/F with $A \cong M_m(D)$ for D the underlying division algebra of A. We define the index of A,* $\mathrm{ind}(A) = \deg(D)$.

It follows immediately that if D is the underlying division algebra of A, that writing $A = M_m(D)$ we have

$$A \otimes \overline{F} \cong M_m(D \otimes \overline{F}) \cong M_m(M_{\operatorname{ind} A}(\overline{F})) \cong M_{m \operatorname{ind}(A)}(\overline{F}),$$

and since also $A \otimes \overline{F} \cong M_{\deg(A)}(\overline{F})$, it follows $\deg(A) = m \operatorname{ind}(A)$ and so we have:

Lemma 3.1.11. *Let A be a csa/F. Then* $\operatorname{ind}(A) | \deg(A)$.

In general, given a algebra A, the underlying division algebra of A contains the most important structural information about A, and in particular, the computation of the index of A is a central question in the field. A great deal of research to date has been concerned with the development of techniques to compute the index of algebras in particular cases. This includes, of course, the question of whether or not a given algebra A is a division algebra, as this may also be interpreted as the question of whether or not the equality $\deg(A) = \operatorname{ind}(A)$ holds.

3.2 More structure theory

3.2.1 Noether-Skolem and Double Centralizers

Lemma 3.2.1 (Double Centralizer, Warm-Up Version 2)**.** *Suppose $A = B \otimes C$ are cenral simple F-algebras. Then $C = C_A(B)$.*

Proof. Note that $C = C \otimes 1 \subset C_A(B)$, and so it suffices to show that $\dim C_A(B) = \dim C$. Since dimension is preserved under scalar extension, it suffices to assume that $F = \overline{F}$. By Theorem 3.1.5, we then have $B \cong M_n(F), C = M_m(F)$ and $B \otimes C \cong M_m(M_n(F))$, with the embedding $B = B \otimes 1 \subset A$ as the inclusion of $m \times m$ "scalar" matrices with (equal) entries in $M_n(F)$. By Lemma 1.3.6(1), we then have $C_{M_m(M_n(F))}(M_n(F)) = M_m(Z(M_n(F)) = M_m(F) = C$, and so the centralizer has the desired dimension. □

Theorem 3.2.2 (Noether-Skolem)**.** *Let A be a csa/F, $B, B' \subset A$ simple F-subalgebras. Given an isomorphism of F-algebras $\psi : B \to B'$, there exists an element $\alpha \in A^*$ such that $\psi(b) = \alpha b \alpha^{-1}$ for every $b \in B$.*

Proof. Consider the inclusions

$$B \subset A \subset A \otimes A^{op} \to \operatorname{End}_F(A).$$

This gives the vector space A the structure of a $B \otimes A^{op}$-module in two different ways:

$$b \otimes a \cdot_1 (x) = bxa, \quad b \otimes a \cdot_2 (x) \psi(b) x a.$$

We write these two different $B \otimes A^{op}$ modules as A_1 and A_2. Note that these of course have the same underlying set (A), but different module structures.

Since $B \otimes A^{op}$ is a simple F-algebra by Lemma 3.1.8, it follows from Corollary 1.2.24 that there is a unique simple left $B \otimes A^{op}$ module. Since A_1 and A_2 are finite dimensional $B \otimes A^{op}$-modules, they are both semisimple modules, and hence uniquely characterized by their dimension, since they are both a sum of the same simple module, repeated some number of times. Consequently, we may find an isomorphism $\phi : A_1 \to A_2$ of left $B \otimes A^{op}$ modules. That is, ϕ is a map from A to itself such that $\phi(bxa) = \psi(b)\phi(x)a$ for every $b \in B$, $a, x \in A$.

Using the sandwich map, we may regard ϕ as arising from the natural action of an element $\alpha \in A \otimes A^{op}$, acting on A using the standard left module structure defined by the sandwich map. Since this is an isomorphism, it follows that $\alpha \in (A \otimes A^{op})^*$. Since α is a $1 \otimes A^{op}$ module map (this part of the $B \otimes A^{op}$ module structures A_1 and A_2 on A coincide), it follows that $\alpha \in C_{A \otimes A^{op}}(A^{op})$ by Section **??**, and hence by Lemma 3.2.1, we have $\alpha \in A \otimes 1 \subset A \otimes A^{op}$. Since α is also in $(A \otimes A^{op})^*$, it follows that $\alpha \in A^*$. By the properties of ϕ, we then have, for $b \in B$, $\phi(b) = \psi(b)\phi(1)$, and so $\alpha b = \psi(b)\alpha$, or in other words

$$\alpha b \alpha^{-1} = \psi(b),$$

as desired. □

To prove the full double centralizer Theorem, let us begin with a quick lemma concerning subrings of matrix algebras.

Lemma 3.2.3. *Let $R, T \subset S$ be rings, and consider $S \subset M_n(S)$ via the diagonal embedding. We then have*

$$RM_n(T) = \{\sum r_i t_i | r_i \in R, t_i \in M_n(T)\} = M_n(RT).$$

Lemma 3.2.4. *By definition, it is enough to show that for every matrix unit $e_{i,j}$ and every $r \in R, t \in T$, we have $rte_{i,j} \in RM_n(T)$. But this is clear since $te_{i,j} \in M_n(T)$.*

Lemma 3.2.5 (Double Centralizer, Warm-Up Version 3)**.** *Suppose $B \subset A$ are central simple F-algebras. Then $A = BC_A(B) \cong B \otimes C_A(B)$.*

Proof. We wish to check that the natural map $B \otimes C_A(B) \to A$ via multiplication is an isomorphism. It suffices, by Lemma A.4.4, to check that this holds after scalar extension from F to $\overline{F}$. In particular, we may assume that the field F is algebraically closed.

By Theorem 3.1.5, we then have $B \cong M_n(F)$. Since F^n is a simple B-module, it is the unique one by Lemma 1.2.24, and if we write $A = End_F(V)$, it then follows that V is a semisimple B module, and hence isomorphic to $(F^n)^m$ for some m. In particular, we have $A = M_{nm}(F)$. Note that since we may embed $M_n(F)$ into A as "block scalar matrices," it follows from Noether-Skolem that after a change of basis of $V = F^{nm}$, we may assume that B is embedded in this way in A. But evidently, we now have $A = M_{nm}(F) = M_m(M_n(F)) = M_n(F) \otimes M_m(F) = B \otimes C_A(B)$ as claimed. □

Theorem 3.2.6 (The Double Centralizer Theorem)**.** *Let B be a simple F algebra, A a csa/F, and $B \subset A$. Then*

1. *$C_A(B)$ is a simple algebra,*

2. $(\dim_F B)(\dim_F C_A(B)) = dim_F A$,

3. $C_A(C_A(B)) = B$,

4. *If B is a csa/F, then $A \cong B \otimes C_A(B)$.*

Proof. Part (4) is exactly Lemma 3.2.5. Part (1) will follow from (4) and the fact that if $B \otimes C_A(B)$ is simple, then $C_A(B)$ must be simple as well.

For part (3), consider the inclusions $B \subset A \subset A \otimes A^{op}$. We note that $C_{A\otimes A^{op}}(B \otimes 1) = C_A(B) \otimes A^{op}$ since computing commutators, we find that for an arbitrary element $\sum a_i \otimes a_i' \in C_{A\otimes A^{op}}(B \otimes 1)$, chosen so that all the a_i' are independent, we have:

$$0 = b \otimes 1 \left(\sum a_i \otimes a_i'\right) - \left(\sum a_i \otimes a_i'\right) b \otimes 1 = \sum (ba_i - a_i b) \otimes a_i'$$

implies that b commutes with each a_i, or in other words $\sum a_i \otimes a_i' \in C_A(B) \otimes A^{op}$ as desired. It follows then that by Lemma 1.3.7,

$$B \otimes 1 = C_{A\otimes A^{op}}(C_{A\otimes A^{op}}(B)) = C_{A\otimes A^{op}}(C_A(B) \otimes A^{op}) = C_A(C_A(B)) \otimes 1.$$

Finally, we turn to part 2. The case where B is a central simple algebra over F follows from part 4. In general, since B is simple, we write $L = Z(B)$, and we have B is a csa/L. If we consider the inclusion $B \subset A \subset A \otimes A^{op} = End(A)$, then we see that the inclusion of L in B gives A the structure of an L-vector space under left multiplication, and since $L \subset Z(B)$, it also follows that B consists of L-linear endomorphisms of A. Further, we note that since $L \subset B$, the centralizer $C_{A\otimes A^{op}}(B)$, consists also of L-linear endomorphisms of A, and it follows that $C_{A\otimes A^{op}}(B) = C_{End_F(A)}(B) = C_{End_L(A)}(B)$. Since B and $End_L(A)$ are central simple L-algebras, it follows that $\dim_L(\mathrm{End}_L(A)) = \dim_L(B) \dim_L(C_{\mathrm{End}_F(A)}(B))$. We have

$$\dim_L(\mathrm{End}_L(A)) = \dim_L(A)^2 = (\dim_F(A)/[L : F])^2,$$

$$\dim_L(B) = \dim_F(B)/[L : F]$$

and

$$\begin{aligned}\dim_L(C_{\mathrm{End}_F(A)}(B)) &= \dim_F(C_{\mathrm{End}_F(A)}(B))/[L : F] = \dim_F(C_{A\otimes A^{op}}(B \otimes 1))/[L : F] \\ &= \dim_F(C_A(B) \otimes A^{op})/[L : F] = \dim_F(C_A(B)) \dim_F(A)/[L : F]\end{aligned}$$

and so

$$\dim_F(A)^2/[L : F]^2 = (\dim_F(B)/[L : F]) (\dim_F(C_A(B)) \dim_F(A)/[L : F])$$

giving us $\dim_F(A) = \dim_F(B) \dim_F(C_A(B))$ as desired.

□

stuff showing that centralizers of subfields are central simple and are equivalent to tensoring with the subfield

Corollary 3.2.7. *Suppose that A is a central simple algebra and $L \subset A$ is a subfield. Then* $\deg(A) = \deg(C_A(L))[L : F]$.

3.2.2 The Brauer Group

Definition 3.2.8. *We say that central simple F-algebras A and B are Brauer equivalent, and write $A \sim B$ if we have $M_n(A) \cong M_m(B)$ for some n, m. We write $[A]$ to denote the equivalence class of the algebra A.*

Lemma 3.2.9. *Let A and B be central simple algebras over F. Then $A \sim B$ if and only if A and B have isomorphic underlying division algebras.*

Proof. By Wedderburn-Artin, writing $A \cong M_a(D)$ and $B \cong M_b(D')$, it is clear that if $D \cong D'$ then $A \sim B$. Conversely, if $A \sim B$, this would imply that $M_{an}(D) \cong M_{bm}(D')$ for some n, m. Since both of these are central simple algebras, and since the underlying division algebra of a central simple algebra is uniquely determined up to isomorphism, we would then also have $D \cong D'$. □

Definition/Lemma 3.2.10. *Given Brauer equivalence classes $[A]$ and $[B]$, we define*

$$[A] + [B] = [A \otimes B].$$

*This endows the set of equivalence classes with the structure of an Abelian group, called the **Brauer group**. We denote this group by $\mathrm{Br}(F)$.*

Proof. We first need to show that this is a well defined operation. Note that by Lemma 3.1.7, $A \otimes B$ is again a csa/F. Since

$$M_a(A) \otimes M_b(B) \cong M_{ab}(A \otimes B) \sim A \otimes B$$

it is straightforward to check that the operation does not depend on the choice of representatives. This immediately shows that this gives the structure of a commutative monoid with identity $[F]$. To see that it is a group, we note that by Theorem 3.1.4, every class $[A]$ is invertible, with inverse $[A^{op}]$. □

Definition 3.2.11. *Let A be a central simple algebra. We define the **period** of A (also known as its **exponent**), denoted $\mathrm{per}(A)$ to be the order of $[A]$ in the group $\mathrm{Br}(F)$.*

We will show later that the period of any element of the Brauer group is in fact finite and must divide the index of the element.

A useful and important fact about the Brauer group is that field extensions induce homomorphisms on the Brauer groups.

Proposition 3.2.12. *Suppose that E/F is a field extension. Then the map*

$$\begin{aligned} \mathrm{Br}(F) &\to \mathrm{Br}(E) \\ [A] &\mapsto [A \otimes E] \end{aligned}$$

defines a homomorphism of groups.

Proof. It is easy to check that this map is well defined on Brauer equivalence classes. The fact that it is a homomorphism comes from the properties of the tensor product **??**:

$$(A \otimes B) \otimes E \cong (A \otimes E) \otimes_E (B \otimes E).$$

□

3.2.3 Idempotents and Brauer equivalence

Suppose that A is a csa/F and $e \in A$ is an idempotent element. By Pierce decomposition (Proposition 2.2.2), we find that eAe is an algebra which is isomorphic to the endomorphism ring $End_A(eA)$ of the right A module eA.

Lemma 3.2.13. *Let A be a central simple algebra, and $e \in A$ a nonzero idempotent element. Then eAe is Brauer equivalent to A.*

Proof. As in Lemma 3.2.9, it suffices to show that the eAe is a central simple algebra with the same underlying division algebra. Recall that by Wedderburn-Artin theory, A has a unique simple right module P, and we may write $A \cong P^n$ as a right A module. We then obtain

$$A \cong \mathrm{End}_A(A_A) \cong \mathrm{End}_A(P^n) = M_n(\mathrm{End}_A P) = M_n(D),$$

where $D = \mathrm{End}_A P$ is the underlying division algebra of A. But since the right module eA can also be written as P^m for some m, we have

$$eAe \cong \mathrm{End}_A(eA) \cong \mathrm{End}_A(P^m) = M_m(D)$$

has the same underlying division algebra, and is hence Brauer equivalent to A as claimed. □

3.3 Maximal Subfields

3.3.1 Splitting fields are maximal subfields

Proposition 3.3.1. *Suppose that E/F is a finite field extension and A/F is a central simple F algebra which is split by E, and such that $\deg A = [E : F]$. Then E is isomorphic to a maximal subfield of A.*

Proof. Let $n = [E : F] = \deg(A)$. The action of E on itself via left multiplication gives an injective homomorphism

$$E \to End_F(E) \cong M_n(F),$$

and in particular, an injection $E \to A \otimes M_n(F)$. Since $A \otimes E$ is a split algebra, so is $A \otimes M_n(F) \otimes E$, and therefore by Lemma **??**, it follows that $B = C_{A \otimes M_n(F)}(E)$ is a split algebra. By Corollary 3.2.7, we have $\deg(B) = n$, and consequently $B \cong M_n(E)$. Choose a subalgebra $M_n(F) \cong B' \subset B \subset A \otimes M_n(F)$. By definition $E \subset C_{A \otimes M_n(F)}(B) \subset C_{A \otimes M_n(F)}(B') = A'$. Since B' is a split algebra, by the double centralizer theorem **??**, we have A' is Brauer equivalent to A. By the double centralizer theorem **??**, we also have $\deg(A') = \deg(A)$, and so $A' \cong A$. But as we have noted $E \subset A'$, and so E is isomorphic to a maximal subfield of A as claimed. □

3.3.2 The index via splitting fields

Proposition 3.3.2. *Let A be a central simple algebra. Then*

$$\operatorname{ind}(A) = \gcd\{[E:F] \mid A \otimes E \text{ is split } \} = \min\{[E:F] \mid A \otimes E \text{ is split } \}.$$

Further, the equalities remain when taken in each case over finite ***separable*** *field extensions.*

Proof. To check these equalities, it suffices to assume that A is a division algebra, since splitting is actually a measure of the Brauer class, and not a particular representative algebra. By Proposition 3.3.1, we know that every such splitting field is isomorphic to a maximal subfield of some *csa* Brauer equivalent to A. Since A is division, this means such a splitting field E must be maximal in $M_m(A)$ for some m, and in particular, $[E:F] = m \operatorname{ind}(A)$. This tells us that every splitting field has degree a multiple of the index, and so is suffices to show that the minimal such degree is exactly $\operatorname{ind}(A)$, and not larger. But we know that since every division algebra has a maximal separable subfield by Proposition (in prior lecture, not yet entered), the desired minimum value is obtained, and is in fact obtained by a separable field extension. □

Chapter 4

Galois theory and crossed products

4.1 Quaternions, symbols and cyclics

4.1.1 Quaternion algebras

4.1.2 Symbol algebras

4.1.3 Cyclic algebras

4.2 Galois theory and crossed product algebras

4.2.1 Algebras with Galois maximal subfields

4.2.2 Galois ring extensions of fields

Let F be a field and suppose that E is a commutative F-algebra. We say that E/F is **separable** (or étale) if we can write

$$E \cong \bigtimes E_i$$

for some finite collection of separable field extensions E_i/F.

Definition 4.2.1. *Let E be a commutative separable F-algebra, and G a group of F-algebra automorphisms of E. We say that E is a G-Galois extension of F if $|G| = \dim_F E$ and $E^G = F$.*

Proposition 4.2.2. *Let E be a commutative separable F-algebra, $G \subset \mathrm{Aut}(E/F)$. The folowing are equivalent:*

1. *E is a G-Galois extension of F,*
2. *if we write $E = \times E_i$ for separable field extensions E_i/F, then G acts transitively on the E_i and E_i/F is $\mathrm{Stab}_G(E_i)$-Galois,*

Proof. Suppose that E/F is a G-Galois extension, and write $E = \times E_i e_i$, where e_i are the idempotents in E for this decomposition (as in Proposition 2.2.1).

To see that G acts transitively on these idempotents, consider, for example, the orbit of the idempotent e_1. Clearly for $\sigma \in G$, $\sigma(e_1)$ must also be an idempotent, and by the description of E, we can see that it must exactly be one of the other idempotents e_i, giving an isomorphism $E_1 \to E_i$. If we let e be the sum of all the idempotents in the orbit of G, we see that $e \in E^G$, and hence $e \in F$ by hypothesis. But therefore, since F is a field, and $e \neq 0$, we have $e = 1 = \sum e_i$, and hence the action is transitive.

Let $G_i = \mathrm{Stab}_G(E_i)$. To see that this is Galois, we note that by transitivity of the action, $E_i \cong E_j$ all i, j, and therefore, by the Orbit-Stabilizer Theorem, $|G_i| = [E_i : F]$ for each i. Let $H = \mathrm{Aut}(E_i/F)$. We have a homomorphism $G_i \to H$, and $|H| \leqslant [E_i : F]$ with equality of E_i/F is Galois. Suppose that $x \in E_i^{G_i}$. If $\sigma \in G$ with $\sigma(E_i) = E_j$, then we find that since $G_j = \sigma G_i \sigma^{-1}$, we have $\sigma(x) \in E_j^{G_j}$. Choose for each j, an element $\sigma_j \in G$ such that $\sigma_j(E_i) = E_j$, and set $y = \sum_j \sigma_j(x) \in \times E_j = E$. We then find that $y \in E^G = F$, and hence each component of y in each E_j lies in F. In particular, the ith component of y, namely x, is in F. Therefore $E_i^{G_i} = F$ as claimed.

Conversely, suppose that G acts transitively on the set of E_i's and that each E_i/F is G_i-Galois, where $G_i = \mathrm{Stab}_G(E_i)$ as before. Since G acts transitively on the E_i, they each have the same degree, and since each of the E_i are G_i-Galois, it follows that $|G| = \dim_F E$. To see that $E^G = F$, suppose that $x \in E^G$, and write $x_i = xe_i$ so that $x_i \in E_i$ and $\sum x_i = x$. Since $x \in E^G \subset E^{G_i}$ it follows that $x_i \in E_i^{G_i} = F$ for each i. Furthermore, if $\sigma(E_i) = E_j$, then we see that since σ is an F-algebra map, that $x_i = x_j$ since these elements are both in F. In other words, with respect to the product decomposition $E = \times E_i$, we have x is of the form $x = (x', x', \ldots, x')$ for $x' \in F$. Since this corresponds to an element in the image of F in E, we have $x \in F$ as claimed. □

It follows from this that we can also describe the Galois extension in a particularly explicit way.

Definition 4.2.3. *Suppose that G is a finite group with a subgroup H, and L/F is an algebra with an H-action. Let $\widetilde{{}^G L}$ denote the set of symbols ${}^\sigma x$ for $\sigma \in G$ and $x \in L$. We define an equivalence relation on these symbols by setting ${}^\sigma x \sim^\tau y$ if $\sigma^{-1}\tau \in H$ and $x = \sigma^{-1}\tau y$. Let ${}^G L$ denote the set of equivalence classes $[{}^\sigma x]$, and for a subset $S \subset G$, let ${}^S L$ denote that set of classes of the form $[{}^\sigma x]$ for $\sigma \in S$, $x \in L$.*

Note that we can think of this as "formally extending" the action of H on L to an action of G, where the symbol ${}^\sigma x$ is interpreted as $\sigma(x)$. To emphasize this, we will identify $[{}^\sigma x]$ with $\sigma(x)$ in the case that $\sigma \in H$. We may therefore regard L as a subset of ${}^G L$.

The following lemma is straightforward to check.

Lemma 4.2.4. *Let $\sigma H \in G/H$ be a left coset of H in G. Then the natural map ${}^\sigma L \to^{\sigma H} L$ is bijective, as is the map*

$$\begin{aligned} L &\to^\sigma L \\ x &\mapsto [{}^\sigma x]. \end{aligned}$$

In particular, we see that ${}^{\sigma H}L$ naturally admits the structure of an algebra.

Definition 4.2.5. *Suppose that G is a finite group with a subgroup H, and L/F is an algebra with an H-action. We set ${}^{G/H}L$ denote the algebra*

$$\bigtimes_{\sigma H \in G/H} {}^{\sigma H}L$$

where each factor ${}^{\sigma H}L$ is identified as an algebra by Lemma 4.2.4. We define a G action on ${}^{G/H}L$ via $\tau[{}^{\sigma}x] = [{}^{\tau\sigma}x]$.

One may check that the resulting object is an algebra with G action.

Proposition 4.2.6. *Suppose that E is a commutative separable F-algebra which is a G-Galois extension. Then we can find a subgroup $H \subset G$, and a H-Galois extension of fields L/F such that $E \cong {}^{G/H}L$.*

4.2.3 General crossed product algebras

Definition 4.2.7. *Suppose that A is an F-algebra containing a commutative subalgebra E, and $\sigma \in \mathrm{Aut}(E/F)$. We say that an element $u_\sigma \in A$ is a **Noether-Skolem element** for σ if $u_\sigma x u_\sigma^{-1} = \sigma(x)$ for each $x \in E$.*

Note that if A is a csa/F, and E is a field (and hence a simple algebra) Noether-Skolem element must always exist for each $\sigma \in \mathrm{Aut}(E/F)$. In fact, the same is true for Galois extensions E/F for commutative F-algebras E which are not necessarily fields.

Lemma 4.2.8. *Let A be a csa/F, $E \subset A$ a commutative subalgebra, such that E/F be a G-Galois extension. Then Noether-Skolem elements exist for every $\sigma \in G$.*

Proof. need to fill this in later □

Proposition 4.2.9 (Independence of Noether-Skolem elements)**.** *Suppose that B is an associative algebra over a field F, $E \subset B$ is a commutative subalgebra which is G-Galois over F, and $u_\sigma \in B$ is a collection of Noether-Skolem elements for each $\sigma \in G$. Then the elements u_σ are E-independent. That is, we have*

$$\sum x_\sigma u_\sigma = 0$$

for $x_\sigma \in E$ if and only if $x_\sigma = 0$ for each σ.

Proof. this proof is not done, and needs work!

Write $E = {}^{G/H}L = \bigtimes {}^{\sigma H}Le_{\sigma H}$, for primitive idempotents $e_{\sigma H} \in E$.

Suppose that we have a dependence relation of the form $0 = \sum x_\sigma u_\sigma$. We may assume that this relation has a minimal number of nonzero elements. Since some of the elements are nonzero, we may suppose that not all the elements x_σ are annihilated by e_1. Multiplying

by e_1 on the left, we may therefore assume that $x_\sigma \in Ee_1 = L$ for all σ. Now, consider right multiplication by some general $y \in E$. We have

$$\left(\sum x_\sigma u_\sigma\right) y = \sum x_\sigma \sigma(y) u_\sigma = x_\sigma(y) e_1 u_\sigma,$$

since $x = xe_1$ by assumption. Therefore, since L is a field, we may conclude by minimality of our dependence relation, that the vectors $(x_\sigma)_\sigma$ and $(x_\sigma y e_1)_\sigma$ are proportional over L. In other words, this implies $\sigma(y)e_1 = \tau(y)e_1$ for every $y \in E$ and for every σ, τ appearing in the sum.

Let us assume that there are at least two distinct factors in the sum, for group elements $\sigma \neq \tau$. Writing $\sigma^{-1}e_1 = e_{\sigma^{-1}(1)}$, we have $\sigma(y)e_1 = \tau(y)e_1$ for all $y \in E$ implies $ye_{\sigma^{-1}(1)} = \sigma^{-1}\tau(y)e_{\sigma^{-1}(1)}$. If $\sigma^{-1}\tau \in H$, then choosing $y \in E_1 \backslash E_1^{\sigma^{-1}\tau}$ (which we can do since E_1 is H-Galois), we find that this gives a contradiction. On the other hand, if $\sigma^{-1}\tau \notin H$, then choosing $y \in E_1$ arbitrarily, we find that since □

Suppose we have a central simple algebra A, a maximal commutative separable subalgebra E which is a G-Galois extension of F, and

discussion of existence of Noether-Skolem elements in the case that we have a maximal Galois subfield

Definition 4.2.10 (crossed product algebra)**.**

Proposition 4.2.11. *Crossed product algebras are in bijection with csa's with maximal Galois subfields.*

4.2.4 The second Galois cohomology group

Definition 4.2.12. *2-cocycle, cohomologousness.*

Theorem 4.2.13. *$H^2(G, E^*)$ is isomorphic to the subgroup of $\mathrm{Br}(F)$ consisting of csa's equivalent to ones with E/F as a maximal subfield.*

4.3 Galois descent

4.3.1 Vector spaces with semilinear actions

1. definition of semilinear action
2. equivalence with $(E, G, 1)$-module
3. structure theorem
4. identification of V^G with $F^n \otimes_{M_n(F)} F^n \cong F$. via dot product of vectors/dimension count (surjective from F^n...).

5. mutually inverse equivalences between vector spaces with semilinear action and vector spaces over F. respects tensor products (note the structure of tensor in the semilinear category is nonstandard with diagonal action...) need to check holds for just $E \otimes E$ and higher powers....

4.3.2 The first Galois cohomology group

definition of twisted forms/torsors of algebraic structures (algebras!)

example of matrix algebras and csas

since same over E/F, differs by semilinear actions. definition of the standard semilinear action.

if B is a form of A, then we have $\psi : B \otimes E \xrightarrow{\sim} A \otimes E$ moving the G-action on $B \otimes E$ through the isomorphism gives a

4.3.3 Finite torsors and Galois extensions

4.3.4 PGL_n-torsors and central simple algebras

4.4 A bit more Galois cohomology

4.4.1 The boundary map

4.4.2 Saltman's proof of period dividing index

Chapter 5

A second look at the Brauer group

5.1 Corestriction

Let L/F be a separable field extension and A a csa/L. The **corestriction**, also called the norm, gives a way to associate to A a new csa/F. This new algebra will be given naturally by descent – that is to say, in order to define an F-algebra B, it is equivalent to find a Galois extension E/F, say with group G, and define an algebra $\widetilde{B}$ over E with a semilinear action by G. These are then in bijection with F-algebras by associating to $\widetilde{B}$ the algebra $\widetilde{B}^G$.

5.1.1 Twisting algebras

A crucial tool in constructing the corestriction, is the notion of taking the Galois twist of an algebra.

Definition 5.1.1. *Let E/F be a field extension, A and E-algebra, and σ an automorphism of E/F. We define the σ-twist of A, denoted ${}^{\sigma}A$, to be the E-algebra, whose elements are given by*

$$ {}^{\sigma}A = \{ {}^{\sigma}a \mid a \in A \} $$

with the algebra structure given by requiring the map $a \to {}^{\sigma}a$ being an isomorhism of rings, and with

$$ {}^{\sigma}(\lambda a) = \sigma(\lambda)\ {}^{\sigma}a $$

for $\lambda \in E$, $a \in A$.

As the next example illustrates, we can think of this concretely as by using σ to act on the structure constants of the algebra.

Example 5.1.2. *Let F be a field of containing a primitive n'th root of unity ρ, let E/F be a field extension and σ an automorphism of E/F. Choose $a, b \in E^*$. Consider the symbol algebra $A = (a,b)_\rho$, and the twisted algebra ${}^{\sigma}A$. Then we have an isomorphism*

$$ {}^{\sigma}(a,b)_\rho \to (\sigma(a), \sigma(b))_\rho . $$

To see this, we suppose that u, v are in A with $vu = \rho uv$, $u^n = a, v^n = b$. We then have ${}^\sigma v\ {}^\sigma u = {}^\sigma(\rho uv) = {}^\sigma(\rho)\ {}^\sigma u\ {}^\sigma v = \rho\ {}^\sigma u\ {}^\sigma v$, and $({}^\sigma u)^n = {}^\sigma(u^n) = {}^\sigma a = \sigma(a)\ {}^\sigma 1 = \sigma(a)$, and similarly for v.

Lemma 5.1.3. *Suppose that σ, τ are automorphisms of L/F and A is an L-algebra. Then we have a canonical isomorphism*

$$ {}^\sigma({}^\tau A) \cong {}^{\sigma\tau} A $$

given by ${}^\sigma({}^\tau a) \mapsto {}^{\sigma\tau} a$.

Lemma 5.1.4. *Suppose that σ is an automorphism of L/F and A, B are L-algebras. Then we have a canonical isomorphism*

$$ {}^\sigma A \otimes {}^\sigma B \cong {}^\sigma(A \otimes B) $$

given by ${}^\sigma a \otimes {}^\sigma b \mapsto {}^\sigma (a \otimes b)$.

Lemma 5.1.5. *Suppose that L/F is a field extension, σ an automorphism of L/F, and A an F-algebra. Then we have an isomorphism of L-algebras*

$$ {}^\sigma(A \otimes L) \cong A \otimes L $$

given by ${}^\sigma(a \otimes x) \mapsto a \otimes \sigma(x)$.

5.1.2 The case of a Galois extension

Although not strictly necessary, it is perhaps more intuitive to begin with the case L/F is a Galois extension with group G, and A/L is a *csa*.

In this case, we let ^{G} be the algebra

$$ {}^G A = \otimes_{\sigma \in G}\ {}^\sigma A. $$

Note that since each ${}^\sigma A$ is isomorphic as a ring to A, it is easy to see that they are central simple algebras. In particular, it also follows that B is itself central simple.

Lemma 5.1.6. *The map $\mathrm{Br}(L) \to \mathrm{Br}(L)$ given by $A \mapsto {}^G A$ is a homomorphism of groups.*

Proof. It follows from Lemma **??** that the map $\mathrm{Br}(L) \to \mathrm{Br}(L)$ given by $[A] \mapsto [{}^\sigma A]$ is a homomorphism, and in particular the map

$$ \mathrm{Br}(L) \to \prod_{\sigma \in G} \mathrm{Br}(L) $$

defined by $[A] \mapsto ([{}^\sigma A])_{\sigma \in G}$ is also a homomorphism. But, for any Abelian group M, the sum map $M^r \to M$ via $(m_1, \ldots, m_r) \mapsto \sum m_i$ is a homomorphism, and so in particular the composition

$$ \mathrm{Br}(L) \to \prod_{\sigma \in G} \mathrm{Br}(L) \xrightarrow{\sigma} \mathrm{Br}(L) $$

is a homomorphism. But this composition is just the map $A \mapsto {}^G A$ as desired. □

This new algebra ${}^{G}A$ comes equipped with a semiliear action of the Galois group G. Perhaps the easiest way to see this is as follows. Let us abuse notation and consider the algebras ${}^{\sigma}A$ as subalgebras of ${}^{G}A$ via the inclusion $x \mapsto 1 \otimes \cdots \otimes 1 \otimes x \otimes 1 \otimes \cdots \otimes 1$, where the entry x occurs in the position defined by σ (recall that the factors are indexed by the elements of G). By construction of the algebra ${}^{G}A$, such elements generate, and the images of ${}^{\sigma}A$ and ${}^{\tau}A$ commute in ${}^{G}A$ whenever $\sigma \neq \tau$. We define

$$\sigma({}^{\tau}a) = {}^{\sigma\tau}a.$$

One may then check that this extends to define an action of G on ${}^{G}A$ which is semilinear.

Definition 5.1.7. *Let A be a central simple L-algebra, where L/F is G-Galois. We define the **corestriction** of A, denoted $\mathrm{cor}_{L/F} A$ to be given by*

$$\mathrm{cor}_{L/F} A = \left({}^{G}A\right)^{G}.$$

Lemma 5.1.8. *The map $\mathrm{cor}_{L/F}$ induces a homomorphism $\mathrm{Br}(L) \to \mathrm{Br}(F)$.*

Proof. This follows immediately from Lemma **??**, together with the fact that the correspondence of Galois descent is compatible with the tensor product of algebras. □

5.1.3 The non-Galois case

In general, we'd like to define $\mathrm{cor}_{L/F} A$ in case L/F is separable, but not necessarily Galois. In this case, we start by choosing a Galois closure E/F of L, so that $G = Gal(E/F)$ and $L = E^H$ for some subgroup $H < G$. Instead of considering a twist of the algebra A by an element $\sigma \in G$, we instead wish to consider a twist of the algebra $A \otimes_L E$ by a coset $\sigma H \subset G/H$. Note that there is a natural action of H on $A \otimes_L E$ via acting on the second coordinate, however this does not naturally extend to an action of G. To illustrate the problem, if $\sigma \in G \backslash H$, say $\sigma(x) \neq x$ for some $x \in L$, then one would find when trying to extend this definition:

$$a \otimes x = ax \otimes 1 = \sigma(ax \otimes 1) = \sigma(a \otimes x) = a \otimes \sigma(x)$$

which would give a contradiction.

Definition 5.1.9. *Let ${}^{\sigma H}A = \{{}^{\tau}a \mid a \in A \otimes_L E,\ \tau \in \sigma H\} / \sim$ where $\sim$ is the equivalence relation described by*

$${}^{\tau}a \sim {}^{\gamma}b \iff \gamma^{-1}\tau a = b$$

Definition 5.1.10. *For A as above, we define ${}^{G/H}A = \otimes_{\sigma H \in G/H} {}^{\sigma H}A$.*

This algebra comes with a semilinear action of G by $\sigma({}^{\tau}a) = {}^{\sigma\tau}a$, for $a \in A \otimes_L E$.

One way to think of this algebra is that we have "formally extended" the action of G to $A \otimes_L E$ by setting $\sigma a = {}^{\sigma}a$.

Definition 5.1.11. *Let L/F be a separable extension, and suppose that E is an extension of L with E/F being G-Galois. We define the corestriction of A as*

$$\mathrm{cor}_{L/F} A = ({}^{G/H}A)^G$$

etcetera...

Proposition 5.1.12. *Suppose that A is an F algebra and L/F is a separable field extension of degree n. Then $\mathrm{cor}_{L/F}(A \otimes L)$ is Brauer equivalent to $A^{\otimes n}$.*

Proof. This follows from the fact that we may identify ${}^{G/H}A$ with $(A \otimes_F E)^{\otimes n} \cong A^{\otimes n} \otimes_F E$ together with its natural semilinear Galois action. □

As a corollary, we have yet another proof of the fact that the period of A divides its index, if we consider the case that L/F is a maximal subfield of the underlying division algebra of A.

5.2 Primary decomposition

5.2.1 Abstract primary decomposition

Suppose that M is group and $m \in M$ is an element which is torsion. The primary decomposition of m is a canonical way of writing m as a product of elements of M, which commute with each other, and such that each element has prime power order. This works as follows: consider the homomorphism $\mathbb{Z}/n \to M$ given by $1 \mapsto m$, where n is the order of m. Write $n = q_1 \cdots q_r$ where $q_i = p_i^{r_i}$ for distinct prime integers p_i. By the Chinese Remainder Theorem, we can write $\mathbb{Z}/n \cong \prod \mathbb{Z}/q_i$, where the projections onto the various factors are simply the natural quotient maps. Write the image of 1 as $(a_1, a_2, \ldots, a_r)$, and suppose that $b_i \in \mathbb{Z}/n$ is chosen to have image of 1 in $\mathbb{Z}/q_i$ and 0 in the other components. It follows that $\sum a_i b_i \equiv_n 1$, by looking at its image in each component, and $a_i b_i$ has order exactly q_i in $\mathbb{Z}/n$. Consequently, if we write $m_i = a_i b_i m_i$, we have

$$m = m_1 m_2 \cdots m_r$$

where the m_i mutually commute since they all lie in the same cyclic subgroup, and where m_i has order exactly q_i.

5.2.2 Primary decomposition in the Brauer group

Let's apply the ideas of the previous section specifically to the Brauer group. Suppose that D is a central division algebra of degree n and suppose that $n = q_1 \cdots q_r$ with the q_i relatively prime prime powers. As before, we can write the class $[D] \in Br(F)$ as $[D] = [D_1] + \cdots + [D_r]$ where each D_i is a division algebra whose period is q_i.

It is immediate that the product of the indices of the D_i must be no smaller than the index of D. Indeed, since $D_1 \otimes \cdots D_r$ is Brauer equivalent to D, and D is a division algebra,

it follows that the index of the tensor product of the D_i's must have degree at least as large as the index of D. Conversely, we claim that the index of the tensor product is no larger than the index of D.

5.3 Cyclic Algebras

5.4 Albert's criterion for cyclicity

5.5 Algebras of degree 3 are cyclic

Chapter 6

Involutions

6.1 Bilinear forms and adjoint involutions

The notion of an involution on a central simple algebra is a generalization of the notion of a transpose of a matrix. As one learns in linear algebra, the transpose of a matrix is intimitely connected to the idea of the standard inner product of vectors, as is illustrated by the multiplication of a row and a column matrix. That is, when we define for a pair of column vectors x, y in F^n,

$$x \cdot y = x^t y,$$

we find that for any linear transformation T, we have

$$x \cdot Ty = x^t Ty = (T^t x)^t y = T^t x \cdot y.$$

In other words, the linear transformation "moves across" the inner product by taking its transpose. In fact, this equation completely determines the transpose operation as one may check.

In general, if $b : V \times V \to F$ is a symmetric or skew symmetric bilinear form, we say that b is nondegenerate if for every $v \in V \backslash \{0\}$, we have $v \mapsto b(\_, v)$ induces an isomorphism $V \to V^*$ between V and its dual. In this case, for a linear transformation T, we can consider the functional

$$v \mapsto b(v, T(\_)) \in F.$$

By nondegeneracy, this must also have the form $b(\_, w)$ for some $w \in V$. Generalizing the prior discussion with the transpose, we define $adj_b(T)$ by $adj_b(T)(v) = w$.

Appendix A

Tensors

A.1 Existence of Tensor products

Definition A.1.1. *Let R, S, T be rings, ${}_RM_S$, ${}_SN_T$, ${}_RP_T$ bimodules. We say that a map*

$$\phi : M \times N \to P$$

is $R-S-T$ linear if

1. *for all $n \in N$, the map*

$$\begin{aligned} M &\to P \\ m &\mapsto \phi(m,n) \end{aligned}$$

   is a left R-module map.

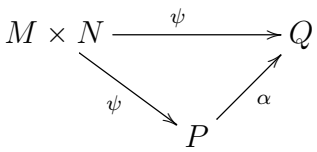
2. *for all $m \in M$, the map*

$$\begin{aligned} N &\to P \\ n &\mapsto \phi(m,n) \end{aligned}$$

   is a right T-module map.

3. *for all $n \in N, m \in M, s \in S$, we have $\phi(ns, m) = \phi(n, sm)$.*

Definition A.1.2. *Given bimodules ${}_RM_S$, ${}_SN_T$, we say that a bimodule ${}_RP_T$ together with an $R-S-T$ linear map $\phi : M \times N \to P$ is a tensor product for M and N if for every other bimodule ${}_RQ_T$ and $R-S-T$ linear map $\psi : M \times N \to Q$, there is a unique $R-T$ bimodule map $\alpha : P \to Q$ such that we have a commutative diagram:*



In fact, tensor products always exist and are unique up to unique isomorphism. The uniqueness follows from the standard arguments of universal objects, and the existence is a consequence of the following explicit construction.

Definition A.1.3. *Let Λ be a set. We define the free Abelian group generated by Λ, denoted $\langle\Lambda\rangle$ to be the set of formal finite linear combinations*

$$\sum_{i=1}^{n} a_i\lambda_i, \lambda_i \in \Lambda, a_i \in \mathbb{Z}$$

subject to the relation $a\lambda + b\lambda = (a+b)\lambda$.

Definition A.1.4. *Given bimodules ${}_RM_S$, ${}_SN_T$, we define $M \otimes_S N$ to be the quotient of $\langle M \times N\rangle$ by the submodule generated by the following types of expressions of the form $(ms, n) - (m, sn)$. We write $m \otimes n$ to denote the equivalence class of (m, n) in $M \otimes N$. This has a $R - T$ bimodule structure induced by $r(m \otimes n) = rm \otimes n$ and $(m \otimes n)t = m \otimes nt$.*

The map $M \times N \to M \otimes_S N$ sending (m, n) to $m \otimes n$ gives $M \otimes N$ the structure of a tensor product of M and N. We refer to this as *the* tensor product of M and N.

A.2 Scalar extension

A particularly useful instance of the tensor product is when one has an extension of rings $R \subset S$ (or more generally, a homomorphism of rings $\phi : R \to S$), and a left R-module M. In this case, the tensor product $S \otimes_R M$ naturally inherets the structure of a left S module (we are tensoring an $S - S$ bimodule with a $S - \mathbb{Z}$-bimodule).

We refer to $S \otimes_R M$ as the scalar extension (or base change) of M to S.

A.3 Tensor products of vector spaces

The tensor product of vector spaces is particularly easy to describe. Note first that if V is an F-vector space, then since F is commutative, we may either regard V as a right or as a left F-module. Doing both at once is also an option since F is commutative, and in this way V can be regarded as an $F - F$ bimodule. It follows then that the tensor product of vector spaces also inherets a natural vector space structure.

To simplify our language (and comply with convention), we will refer to a $F - F - F$ linear function as simply a bilinear function.

Proposition A.3.1. *Suppose that V and W are vector spaces over a field F with bases $\{v_i\}$ and $\{w_j\}$ respectively. Then $V \otimes_F W$ is a vector space with basis $\{v_i \otimes w_j\}$.*

Proof. It is clear that these elements span: by the definition of the tensor product, a typical element of $V \otimes_F W$ is of the form $\sum a_k \otimes b_k$ for some $a_k \in V, b_k \in W$. In particular, to see

that our elements span, it suffices to show that any vector of the form $a \otimes b$ lies in the span. By definition, we may write

$$a = \sum a_i v_i, \ b = \sum b_j w_j$$

and so

$$a \otimes b = (\sum a_i v_i) \otimes (\sum b_j w_j) = \sum_{i,j} a_i b_j v_i \otimes w_j$$

is in the span, as claimed.

To check independence, consider the function $f_{k,\ell} : V \times W \to F$ defined by

$$f_{k,\ell}(\sum a_i v_i, \sum b_j w_j) = a_k b_\ell.$$

It is easy to check that this is bilinear, and hence factors uniquely through the tensor product. Write $\widetilde{f}_{k,\ell} : V \otimes W \to F$ as the induced linear transformation. We then have $\widetilde{f}_{k,\ell}(v_i \otimes w_j) = \delta_{(k,\ell),(i,j)}$ and in particlar, $\widetilde{f}_{k,\ell}(\sum c_{i,j} v_i \otimes w_j) = c_{k,\ell}$.

It follows that, if

$$\alpha = \sum c_{i,j} v_i \otimes w_j = 0$$

then $\widetilde{f}_{i,j}(\alpha) = c_{i,j} = 0$ for all i, j, showing that these are indeed independent. □

A.4 Base extension of maps

Definition A.4.1. *Given a ring extension $R \subset S$ and a homomorphism of left R-modules $f : M \to N$, we define*

$$S \otimes f : S \otimes_R M \to S \otimes_R N$$

to be the map given by $S \otimes f(s \otimes m) = s \otimes f(m)$, and then extending by linearity to general elements of the tensor product.

Lemma A.4.2. *Suppose that L/F is a field extension, and V is a vector space over F with basis $\{v_i\}$. Then $\{1 \otimes v_i\}$ is a basis for $L \otimes V$.*

Proof. It is easy to see that the elements $1 \otimes v_i$ span $L \otimes V$ over L. To see that they are independent over L, consider an expression

$$\alpha = \sum x_i \otimes v_i,$$

with $x_i \in L$ for each i.

For any j, we may consider the function

$$\phi_j : L \times V \to L$$

via $\phi_j(x, \sum a_i v_i) = x a_j$. Note that this is a bilinear map of F-vector spaces, and hence defines an F-linear transformation $\widetilde{phi}_j : L \times V \to L$.

We compute that $\phi_i(\alpha) = x_i$, and therefore if $\alpha = 0$, each $\phi_i(\alpha) = x_i = 0$ as claimed. □

Lemma A.4.3. *Suppose that L/F is a field extension and $f : F^n \to F^m$ is a linear transformation represented by a matrix $(a_{i,j})$. Then $L \otimes f$ is represented by the matrix $(a_{i,j})$.*

Lemma A.4.4. *Suppose that L/F is a field extension, and $f : V \to W$ is a linear transormation of F-vector spaces. Then*

$$\ker L \otimes f = L \otimes_F \ker f, \quad \operatorname{coker} L \otimes f = L \otimes_F \operatorname{coker} f$$

Proof. This follows from the fact that bases for both of these can be computed through Gaussian elimination using the matrix in some basis. Since the matrix doesen't change under extension of scalars, the kernel and cokernel have the corresponding basis over F and L. □

Index