Central Simple Algebras

Daniel Krashen

January 22, 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 $m \in P \setminus \{0\}$, $mR = P$,*
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 $m \in P \setminus \{0\}$. Then mR is a nonzero submodule of P and hence we must have $mR = P$.
(2 $\implies$ 3) Choose some $m \in P \setminus \{0\}$. 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 $\text{ann}_R(M)$ 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 $f \in D \setminus \{0\}$. 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 warm up, let's examine what certain commutators look like in matrix algebras.

Lemma 1.3.4. *Suppose that $R \subset S$ are rings. We may consider the inclusions*

$$R \subset S \subset M_n(S)$$

where the latter is induced by mapping the element s to the diagonal matrix sI_n. Then

1. $C_{M_n(S)}(R) = M_n(C_S(R))$,
2. $C_{M_n(S)}(M_n(R)) = C_S(R)I_n$.

Proof. It is easy to check that for a matrix $a = \sum a_{i,j}e_{i,j}$ and a matrix $b = \sum \beta e_{i,i} = \beta I_n$, that a and b commute exactly when β commutes with each $a_{i,j}$. In particular, it follows that $C_S(R)I_n \subset C_{M_n(S)}(M_n(R))$ and $M_n(C_S(R)) \subset C_{M_n(S)}(R)$.

To check that $C_{M_n(S)(R)} \subset M_n(C_S(R))$, choose $a = \sum_{i,j} a_{i,j}e_{i,j} \in C_{M_n(S)}(R)$. For $r \in R$, we have

$$0 = ar - ra = \sum (a_{i,j}r - ra_{i,j})e_{i,j}$$

which tells us that $a_{i,j} \in C_S(R)$, as desired.

Finally, if we let $a = \sum_{i,j} a_{i,j}e_{i,j} \in C_{M_n(S)}(M_n(R))$, 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 the coefficient of a general $e_{p,q}$ 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 sI_n. for some $s \in S$. Since a must also commute with $R = RI_n$, we therefore find $s \in C_S(R)I_n$ as claimed. □

Theorem 1.3.5 (Double Centralizer, 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 1.3.4(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 1.3.4(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

The Structure of Central Simple Algebras

2.1 Characterizing central simple algebras

Definition 2.1.1. *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 2.1.2. *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 2.1.3. *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 1.3.4(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 1.3.4(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 2.1.4. *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 $I \triangleleft A$, 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, Version 1 (Theorem 1.3.5), 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. □

invariants of csa's: index, degree

2.2 The Brauer Group

brauer equivalence, identification with isomorphism classes of division algebras. period. state period index problem.

2.3 Noether-Skolem and Double Centralizers

2.4 Maximal Subfields

open questions on the existence of nonmaximal subfields

2.5 Quaternions, Cyclics and Crossed Products

2.6 The Second Galois Cohomology Group

period divides index

primary decomposition in the Brauer group

decomposibility - open problems and examples

2.7 Cyclicity of Division Algebras

2.7.1 Degree 3 algebras

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.

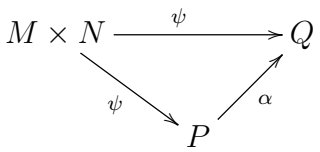
2. *for all $m \in M$, the map*

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

   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