CENTRAL SIMPLE ALGEBRAS

DANIEL KRASHEN

Contents

1. Preliminaries

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.

1.2. Modules and bimodules.

Definition 1.2.1. *Let R be a ring. A left R-module is a set M together with a binary operation*

$$R \times M \to M$$
$$(r, m) \to rm$$

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

$$M \times R \to M$$
$$(m, r) \to mr$$

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

Remark 1.2.4. *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 1.2.5. *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 1.2.6. *We note that just as every Abelian group naturally has the structure of a $\mathcal{Z}$-module, every left (resp. right) R-module has the structure of a $R - \mathcal{Z}$ (resp. $\mathcal{Z} - R$) bimodule.*

Notation 1.2.7. *We will write ${}_RM_S$ to denote the fact that M is an $R - S$ bimodule.*

2. Some Structure Theory

2.1. **Simple and Semisimple Modules.**

Definition 2.1.1. *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 2.1.2. *Let R be a ring, P a left R-module. For a subset $X \subset P$, we define $\operatorname{ann}_R(X)$, the annihilator of P in R, to be the set*

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

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

Definition 2.1.3. *An ideal $I < R$ is called left primitive if I is of the form $I = \operatorname{ann}_R(P)$ for some simple left R module P.*

Proposition 2.1.4. *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

$$R \to P$$
$$r \mapsto mr,$$

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 2.1.5. *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 2.1.6. *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. □

2.2. **Semiprimitive Algebras.**

Definition 2.2.1. *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 2.2.2. *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. $\square$

Lemma 2.2.3. *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 2.1.6, it follows that A_A is semisimple as desired. $\square$

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 2.3.1. *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 2.3.2. *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 2.3.3. *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 2.3.4. *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 2.3.5. *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 2.3.6. *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 2.3.7. *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 2.3.8. *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 2.3.9. *We say that a ring R is* ***semiprimitive*** *if $J(R) = 0$.*

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 2.4.1 (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. □

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 2.4.2. *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 2.4.3 (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 2.4.4 (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. $\square$

Corollary 2.4.5. *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. $\square$