CHAPTER XVII

SIMPLE RINGS

1. Tensor Products of Algebras

Let k be a commutative ring and let A and B be k-algebras. Then we may form the k-module $A \otimes_k B$, and we may define a binary operation on it by

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2, \qquad a_1, a_2 \in A, b_1, b_2 \in B.$$

(Of course, you should check that this definition makes sense on the tensor product in the usual way by defining appropriate bilinear maps.) It is not hard to check that this operation endows $A \otimes_k B$ with a product which makes it a ring. $A \otimes_k B$ is already a k-module, and it is easy to see that it becomes a k-algebra. Also, the maps $A \to A \otimes_k B$ defined by $a \mapsto a \otimes 1$ and $B \to A \otimes_k B$ defined by $b \to 1 \otimes b$ are k-algebra homomorphisms.

In what follows, we shall often omit the subscript k is '$\otimes_k$' since all tensor products in this section will be over k.

Proposition. *Suppose A is a k-algebra, and M is a free k-module with basis $\{x_i \,|\, i \in I\}$. Then $A \otimes M$ is a free A-module with basis $\{1 \otimes x_i \,|\, i \in I\}$. If k is a field, then the ring homomorphisms $A \to A \otimes B$ and $B \to A \otimes B$ are monomorphisms.*

Proof. The first statement is a consequence of the fact that tensor products commute with direct sums. The second statement follows from the first statement and the fact that B (or A) has a basis starting with $x_1 = 1$. Alternately, we may argue as follows. Let $i : k \to B$ be the ring hmomorphism giving B its k-algebra structure. (It is a monomorphism since k is a field.) Since everything splits over a fields, there is a k-linear map $j : B \to k$ such that $ji = \mathrm{Id}_k$. By functorality, $(A \otimes j)(A \otimes i) = A \otimes \mathrm{Id}_k = \mathrm{Id}_{A\otimes B}$. Hence, $A \otimes i$ (which is in fact the map $A \to A \otimes B$ defined above) is a monomorphism. Reversing the roles of A and B gives the result for B.

Let k be a field and let A be a k-algebra. Then we may view k as imbedded in the center of A in a natural way (as the image of the map defining the algebra or also as the set of all $c1, c \in k$.) We say that A is a *central* k-algebra if the center of A is k. We say that A is *central simple* over k if it is central and simple.

Proposition. *Let k be a field.*
(i) If A and B are central k-algebras, then $A \otimes B$ is a central k-algebra.
(ii) If A is central simple over k and B is a k-algebra which is simple, then $A \otimes B$ is simple.
(iii) If A and B are both central simple, then so is $A \otimes B$.

Proof. (i) Suppose that $z = \sum a_i \otimes b_i \in A \otimes B$ is in the center of $A \otimes B$, and suppose the b_i are chosen as part of a k-basis for B. Then by the above proposition, the $a_i \in A$ are unique. Since $z \in Z(A \otimes B)$, we have

$$\sum aa_i \otimes b_i = (a \otimes 1)(\sum a_i \otimes b_i) = (\sum a_i \otimes b_i)(a \otimes 1) = \sum a_ia \otimes b_i$$

so $aa_i = a_ia$ for each i and each $a \in A$. It follows that each $a_i \in Z(A) = k$. Hence, $z = \sum 1 \otimes a_ib_i = 1 \otimes \sum a_ib_i = 1 \otimes b$. Since $1 \otimes b$ commutes with every $1 \otimes b'$, and since $B \to 1 \otimes B$ is an isomorphism, it follows that $b \in Z(B) = k$. Hence, $z \in k \otimes k = k$.

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TEX

(ii) Let I be a nontrivial 2-sided ideal in $A \otimes B$. Let $u = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ be a nontrivial element of I where as above the b_i are linearly independent over k. Suppose moreover, that n is minimal for any nontrivial element of I. Clearly, $a_1 \neq 0$ so Aa_1A is a nontrivial ideal in A so by simplicity $Aa_1A = A$. It follows that if we multiply u on the left and on the right by suitable elements of $A \otimes 1$ and add, we may obtain an element of I of the form

$$1 \otimes b_1 + \cdots + a_n \otimes b_n$$

which we again call u. Consider the element

$$(a \otimes 1)u - u(a \otimes 1) = (aa_2 - a_2a) \otimes b_2 + \cdots + (aa_n - a_na) \otimes b_n.$$

Since this is also an element of I, the minimality of n tells us it is zero so $aa_i = a_ia$ for each i. Hence each $a_i \in Z(A) = k$ and as above $u = 1 \otimes b$ for an appropriate $b \neq 0 \in B$. On the other hand, we have

$$I \supseteq (1 \otimes B)(1 \otimes b)(1 \otimes B) = 1 \otimes BbB = 1 \otimes B$$

since B is simple, so $I \supseteq (A \otimes 1)(1 \otimes B) = A \otimes B$. Hence, $I = A \otimes B$.

(iii) follows from (i) and (ii).

If D is a division ring and an algebra over k, we call it a division algebra over k. Note that any division ring is an algebra over its center which is necessarily a field.

Proposition. *Let k be an algebraically closed field. There are no finite dimensional division algebras over k other than k itself.*

Proof. Let D be a finite dimensional division algebra over k, and let $x \in D$. Since k is in the center of D, $k[x]$ is a commutative subring of D, and it is finite dimensional over k. It follows exactly as in the discussion of algebraic field extensions that $k[x]$ is a field extension of k. Since k is algebraically closed, $k[x] = k$ and $x \in k$. Hence, $D = k$.

Theorem. *Let D be a division ring which is finite dimensional over its center k. Then $[D : k] = \dim_k D$ is a square.*

Proof. Let $\overline{k}$ be the algebraic closure of k, and let $\overline{D} = \overline{k} \otimes D$. By the propositions above, $\overline{D}$ is a simple algebra over $\overline{k}$, and in addition

$$[\overline{D} : \overline{k}] = [D : k].$$

It is not hard to see that it is central over $\overline{k}$. (Let $z = \sum x_i \otimes y_i$ where $x_i \in \overline{k}$, and reason as above.) $\overline{D}$ is a matrix algebra over a division algebra D' which is finite dimensional over $\overline{k}$, and by the above proposition $D' = \overline{k}$ since $\overline{k}$ is algebraically closed. Hence, $\overline{D} = M_n(\overline{k})$ so $[\overline{D} : \overline{k}] = n^2$.

Corollary. *Let A be a central simple algebra over k which is finite dimensional over k. Then $[A : k]$ is a square.*

Proof. $A = M_n(D)$ where D is a division algebra over k. By the theorem, $[D : k] = m^2$ for some m. It follows that $[A : k] = (mn)^2$.

Theorem. *Let A be a central simple algebra over k and suppose $[A : k] = n < \infty$. Then $A \otimes_k A^{op} \cong M_n(k)$.*

Proof. Define $A \otimes A^{op} \to \mathrm{Hom}_k(A, A)$ by $a \otimes b \mapsto \lambda_a \rho_b$ where $\lambda_a(x) = ax$ and $\rho_b(x) = xb$. (Of course, you must check that this yields a well defined map on the tensor product.) This is an algebra homomorphism since $(a \otimes b)(a' \otimes b') = aa' \otimes \mapsto \lambda_{aa'} \rho_{b'b}$ and

$$\lambda_{aa'}(\rho_{b'b}(x)) = aa'xb'b = \lambda_a \rho_b \lambda_{a'} \rho_{b'}(x).$$

Since A and A^{op} are central simple, $A \otimes A^{op}$ is simple. Hence, the above homomorphism is necessarily a monomorphism. On the other hand both domain and codomain have dimension n^2 over k, so the homomorphism is an isomorphism.

Exercises.

2. Central simple algebras

Let A be a simple artinian ring, i.e., a matrix ring over a division ring D. A is clearly an algebra over the center k of D, and it is not hard to see that the field k is the center of A.

Theorem. *Let A be a simple artinian ring with center k, and let B be a k-subalgebra of A which is simple and which is finite dimensional over k. Any k-algebra monomorphism $f : B \to A$ may be extended to an inner automorphism of A, i.e., $\exists x \in U(A)$ such that $f(b) = xbx^{-1}$ for all $b \in B$.*

Proof. $A \otimes_k B^{op}$ is simple because A is central simple over k and B is simple. It is also left artinian. For, since B^{op} is a finite dimensional vector space over k, $A \otimes B^{op}$ is a free A-module of finite rank, and since A is left artinian, so is $A \otimes B^{op}$. (Note in passing that since $A \otimes B^{op}$ is simple and left artinian, it is left semi-simple, hence by what we showed previously, it is also right semi-simple and hence right artinian.)

Let U be the $A \otimes B^{op}$-module which as a k-module is just A, and where

$$(a \otimes b)x = axb \qquad a \in A, b \in B, x \in U = A.$$

Similarly, let V be the $A \otimes B^{op}$-module which as a k-module is A, and where

$$(a \otimes b)y = ayf(b) \qquad a \in A, b \in B, y \in V = A.$$

Of course, there is lots to be checked. Note that having the elements of B act on the right necessitates using B^{op} instead of B. Since $A \otimes B^{op}$ is semi-simple, U and V are certainly semi-simple modules so ,

$$U = \sum U_i \qquad \text{and} \qquad V = \sum V_j$$

where each U_i and V_j is a simple $A \otimes B^{op}$-module. Since a simple artinian ring has up to isomorphism only one simple module, all the U_i and V_j are isomorphic. Hence, depending on whether the cardinality of the set of U_i is greater or less than the cardinality of the set of V_j, we can define either an $A \otimes B^{op}$ epimorphism or an $A \otimes B^{op}$ monomorphism $g : U \to V$. Explicitly,

$$\begin{aligned} &g((a \otimes b)x) = (a \otimes b)g(x) \\ \text{or} \quad &g(axb) = ag(x)f(b) \qquad \text{for } a \in A, b \in B, x \in A. \end{aligned}$$

Taking $b = x = 1$ yields

$$g(a) = ag(1)f(1) = ag(1) \qquad \text{for } a \in A.$$

Taking $a = x = 1$ yields

$$g(b) = g(1)f(b) \qquad \text{for } b \in B.$$

Hence, for $b \in B$, we have $bg(1) = g(1)f(b)$. Thus if $g(1)$ is invertible,

$$f(b) = g(1)^{-1}bg(1).$$

To see that $g(1)$ is invertible in A, use the fact that $a \mapsto g(a) = ag(1)$ is either a monomorphim or an epimorphism. Since $A \cong M_n(D)$ for some division ring D, if $g(1)$ were not invertible, we could find $s, t \in A$ such that $sg(1) = g(1)t = 0$. It would then follow that $a \mapsto ag(1)$ is neither a monomorphism nor an epimorphism.

Corollary (Skolem-Noether). *Let A be a central simple finite dimensional algebra over a field k. Every automorphism of A which fixes k is inner.*

Proof. Take $A = B$.

Proposition. *Let D be a central division algebra which is finite dimensional over its center k. If L is a maximal subfield of D, then $[D:k]=[L:k]^2$.*

Proof. Let $A=D\otimes_k L$. A is simple since D is central simple and L is simple. Make D into an A-module by

$$(x\otimes u)y = ayu \qquad \text{for } x\in D, u\in L, y\in D.$$

It is certainly a simple A-module because any left submodule would be a $D=D\otimes 1$-subspace. It follows that D is isomorphic to a minimal left ideal of A, and $A\cong \operatorname{Hom}_{D'}(D,D)$ where $D'=\operatorname{Hom}_A(D,D)$ is the commuting algebra. (Use Rieffel's Theorem.) However, $h\in \operatorname{Hom}_A(D,D)$ if and only if $h((x\otimes u)y)=(x\otimes u)h(y)$ or $h(xyu)=xh(y)u$ for $x,y\in D, u\in L$. Taking $y=u=1$ yields $h(x)=xh(1)$ for $x\in D$. Taking $x=y=1$ yields $h(u)=h(1)u$ for $u\in L$. Hence, $uh(1)=h(1)u$ for $u\in L$, so $h(1)$ centralizes L. It follows that $L[h(1)]$ is a field containing L and by maximality it equals L; hence $h(1)\in L$. Thus, h is just multiplication by $h(1)\in L$. Conversely, it is easy to see that multiplication on the right by an element of L commutes with the action of A. Thus, $D'=L$ acting on the right of A. Hence, if we view D as a vector space over L, we have

$$A\cong \operatorname{Hom}_L(D,D)$$

and $[A:L]=[D:L]^2$. On the other hand, since $A=D\otimes_k L$, we have $[A:L]=[D:k]$, so $[D:L]^2=[D:k]=[D:L][L:k]$. Hence, $[D:L]=[L:k]$ and $[D:k]=[L:k]^2$.

Theorem (Frobenius). *The only finite dimensional division algebras over $\mathbf{R}$ are $\mathbf{R},\mathbf{C}$, and the algebra of quaternions $\mathbf{H}$.*

Proof. Let D be a finite demnsional $\mathbf{R}$-algebra. Its center is a finite extension of $\mathbf{R}$, hence is $\mathbf{R}$ or $\mathbf{C}$. In the second case, since $\mathbf{C}$ is algebraically closed, we know that $D=\mathbf{C}$. Suppose the center is $\mathbf{R}$ and $D\neq\mathbf{R}$. Let L be a maximal subalgebra of D. Then L is an algebraic extension of $\mathbf{R}$ so $L=\mathbf{C}=\mathbf{R}+\mathbf{R}i$ where $i^2=-1$. Since $[\mathbf{C}:\mathbf{R}]=2$, it follows from the previous result that $[D:\mathbf{R}]=4$. Complex conjugation followed by inclusion provides a monomorphism from $\mathbf{C}$ into D, so $\exists x\in D$ such that $xix^{-1}=-i$. Hence $x^2ix^{-2}=-(-i)=i$, so x^2 centralizes the maximal subfield $L=\mathbf{C}$, so $x^2\in\mathbf{C}$. On the other hand, x is not in $\mathbf{C}$ since x does not centralize $\mathbf{C}$. Hence $\mathbf{R}[x]\cap\mathbf{C}=\mathbf{R}$ and since x^2 is in both $\mathbf{R}[x]$ and $\mathbf{C}$, it follows that $x^2\in\mathbf{R}$. If $a=x^2>0$ then x is one of the two real square roots of a; hence $a<0$. Suppose $a=x^2=-b^2$ where $b\in\mathbf{R}$. Define $j=xb^{-1}$ so that $j^2=-1$, and $j\notin\mathbf{C}$. Inner autormorphism by j has the same effect as inner automorphism by x since $b\in\mathbf{R}=Z(D)$. Hence, $jij^{-1}=-i$. Let $k=ij$. Then some simple algebra shows that $k^2=-1$, $ki=-ik=j$. Similarly, $ij=-ji=k$ and $jk=-jk=i$. Finally, $\{1,i,j,k\}$ is a linearly independent set over $\mathbf{R}$. For suppose

$$\begin{aligned} &a+bi+cj+dk=0\\ \text{i.e.,}\qquad &a+bi+(c+di)j=0. \end{aligned}$$

If $c+di\neq 0$, then

$$j=-(c+di)^{-1}(a+bi)\in\mathbf{C}$$

which we know to be false. Hence, $c+di=0$, and consequently $a+bi=0$. It follows that $a=b=c=d=0$. Thus,

$$D=\mathbf{R}+\mathbf{R}i+\mathbf{R}j+\mathbf{R}k$$

where i,j, and k satisfy the above relations. Thus $D\cong\mathbf{H}$.