I

Semisimple modules

Simple modules and simple algebras give a great deal of information about arbitrary algebras and their modules and it is this point that we shall develop in this chapter. Semisimple modules are the key idea. They provide a quick proof of the celebrated Wedderburn theorem on simple algebras and they show how any module can be viewed as consisting of many layers of semisimple modules. Our main interest is group algebras and we shall see quickly how these general results lead to insights about group representations.

Let us establish some fixed notation. We let A be a finite-dimensional algebra with unit element over an algebraically closed field k whose characteristic is p. All A-modules are assumed to be left modules and finite-dimensional over k. We also fix a finite group G and let kG be the group algebra of G over k. When we refer to p-groups or p-subgroups of G we shall be implicitly assuming that p is a prime.

1 Simple modules

There is a close connection between the structure of A and the structure of A-modules. Certainly the most important A-module is A itself with the module structure given by left multiplication. Moreover, if U is any A-module and $u_1, \ldots, u_n$ are generators for U (for example, a basis of U over k) then U is a homomorphic image of the A-module $A \oplus \cdots \oplus A$, the direct sum of n copies of A, via the map which sends the n-tuple $(a_1, \ldots, a_n)$ to $a_1u_1 + \cdots + a_nu_n$, as is easily verified. If U is a simple A-module then any non-zero element of U is a generator so that U is a homomorphic image of the A-module A. This implies that there are only finitely many simple A-modules, up to isomorphism, as the A-module A has a composition series

and we have just seen that any simple module is a composition factor.

We shall examine modules built up from simple modules by using direct sums. This will be the basis for all our important results.

Lemma 1 *If the A-module U is a direct sum of the simple submodules* $S_1, \ldots, S_n$ *and V is a submodule of U then there is a subset I of* $\{1, \ldots, n\}$ *such that U is the direct sum of V and the sum of all the* S_i, $i \in I$.

We shall use the usual notation S_I for the latter sum, where $S_\varnothing = 0$. In order to prove the result, simply choose a subset I maximal subject to the condition that S_I and V intersect in 0. We need only see that U is the sum of V and S_I. But, if this is not the case then there is j, $1 \leqslant j \leqslant n$ with S_j not contained in $S_I + V$. Thus, as S_j is simple, we have $S_j \cap (S_I + V) = 0$ and $S_j + S_I + V$ is also a direct sum, contradicting the maximality of I.

Proposition 2 *If U is an A-module then the following are equivalent:*

(1) *U is a direct sum of simple A-modules;*

(2) *Every submodule of U is a direct summand.*

We shall call such modules *semisimple*. Our results imply some natural properties of this class of modules. First, the lemma gives us that a submodule of a semisimple module is again semisimple. Indeed, with the notation of the lemma, V is isomorphic with U/S_I which is, in turn by our assumption, isomorphic with S_J where J is the complement to I in $\{1, \ldots, n\}$. Second, any quotient of a semisimple is also semisimple. In fact, again with the same notation, U/V is isomorphic with S_I. This fact is also a consequence of the proposition. Indeed, let us see that the quotient U/V has the second property of the proposition. Let W/V be a submodule of U/V, where W is a submodule of U containing V. By the lemma, U is the direct sum of W and a submodule X. It follows that U/V is the direct sum of W/V and $X + V/V$: their sum is U/V and $W \cap (X + V) = V$ as $V \subseteq W$ and $W \cap X = 0$. Finally, it is trivial that the direct sum of semisimple modules is again semisimple.

It remains now to prove the proposition. In view of the lemma, it suffices to demonstrate that the second assertion implies the first. However, this second property passes to quotient modules: if W/V is a submodule of U/V, where $W \supseteq V$ are submodules of U, then U is the direct sum of W and X so U/V is the direct sum of W/V and $X + V/V$. (Indeed, $W + (X + V) \supseteq W + X = U$ and $W \cap (X + V) = V$ as $W \supseteq V$ and $W \cap X = 0$). This allows us to proceed by induction on the composition length of U. In fact, if S is a simple

submodule of U then there is a direct sum $U = S + T$ so $T \cong U/S$ is a direct sum of simple modules, by induction, so certainly U has this property.

We are now going to apply these ideas to the algebra A. This is done by means of the *radical* of A, written rad A, which consists of the elements of A which annihilate every simple A-module, that is annihilate each semisimple A-module. (Recall that an element a of A annihilates the module M if $aM = 0$.) The radical of A is an ideal: it is closed under addition and if $a, b \in A$, $r \in \text{rad } A$ and S is a simple module, then

$$(arb)S = ar(bS) \subseteq arS = 0.$$

There are some remarkable and important characterizations of the radical.

Theorem 3 *The radical of A is equal to each of the following:*

(1) *the smallest submodule of A whose corresponding quotient is semisimple;*
(2) *the intersection of all the maximal submodules of A;*
(3) *the largest nilpotent ideal of A.*

These statements require some explanation. The submodules of the A-module A are, of course, just the left ideals of A. It is part of the theorem that the submodule described in the first part actually exists. An ideal N of A is nilpotent if there is a positive integer n such that $x_1 x_2 \cdots x_n = 0$ whenever $x_1, \ldots, x_n \in N$. We are claiming also that there is a largest such ideal.

Before proving the theorem, let us see how it enables us to define a vitally important class of algebras. We say that the algebra A is *semisimple* if rad $A = 0$. The first part of the theorem shows that A is semisimple if, and only if, the A-module A is semisimple. Since every A-module is a homomorphic image of a direct sum of copies of A, it is immediate that A is semisimple exactly when all A-modules are semisimple. One reason this type of algebra is useful is that if A is any algebra then $A/\text{rad } A$ is a semisimple algebra. Indeed, $A/\text{rad } A$ is a semisimple A-module, by the theorem, so it is certainly still semisimple as an $A/\text{rad } A$-module. In fact, an A-module is semisimple if, and only if, it is an $A/\text{rad } A$-module regarded as an A-module, since each semisimple A-module is annihilated by rad A while all $A/\text{rad } A$-modules are semisimple. In particular, $A/\text{rad } A$ has zero radical.

Let us now turn to the proof of this important result. Suppose that I and J are nilpotent ideals of A so that $I^m = J^n = 0$ for suitable positive integers m and n. Certainly $I + J$ is also an ideal and it is nilpotent: $(I + J)^{m+n} = 0$.

Indeed, if $x_i \in I$, $y_i \in J$, $1 \leqslant i \leqslant m+n$, then

$$(x_1 + y_1) \cdots (x_{m+n} + y_{m+n})$$

is a sum of 2^{m+n} terms each of which has at least m factors from I or at least n factors from J. However, I and J are ideals, so each term is a product of m elements from I or n elements from J. Thus, $(I+J)^{m+n}=0$, the sum of nilpotent ideals is again the same, and there is a largest nilpotent ideal N of A.

If S is a simple A-module then NS is a submodule of S. Hence NS is S or 0. If $NS=S$ then $N^nS=S$ for any positive integer n, contradicting the nilpotence of N, so we deduce that $NS=0$ and so $N \subseteq \text{rad } A$. To see that rad $A=N$ it now suffices to show that rad A is nilpotent as then rad $A \subseteq N$. Let

$$A = A_0 \supset A_1 \supset \cdots \supset A_r = 0$$

be a composition series for the A-module so each quotient $A_i/A_{i+1}, 0 \leqslant i < r$, is simple. Hence, (rad $A)A_i \subseteq A_{i+1}$ so (rad $A)^r A_0 = 0$ and (rad $A)^r = 0$, as required.

Suppose that $M_1, \ldots, M_r$ are maximal submodules of the A-module A so each quotient A/M_i is a simple module and $A/M_1 \oplus \cdots \oplus A/M_r$ is semisimple. It follows that $A/M_1 \cap \cdots \cap M_r$ is also semisimple since it is isomorphic with a submodule of the preceding direct sum (via the map sending the coset containing $a \in A$ to the r-tuple $(M_1 + a, \ldots, M_r + a)$). Hence, if I is the intersection of all the maximal submodules of A then A/I is semisimple because I is the intersection of a finite number of maximal submodules. On the other hand, suppose M is a submodule of A with A/M semisimple, in fact, say $A/M = L_1/M + \cdots + L_s/M$ is a direct sum when each L_i is a submodule containing M with L_i/M simple. Thus, if we let M_i be the sum of all the L_j, $j \neq i$, then $A/M_i \cong L_i/M$ is simple so M_i is maximal and we also have $M = M_1 \cap \cdots \cap M_s$. Thus, $M \supseteq I$ and so I is the smallest submodule of A with semisimple quotient. We have established that the submodule described in (1) exists and coincides with the submodule I. Hence, it remains only to prove that $I = \text{rad } A$.

However, if $a \in \text{rad } A$ and M is a maximal submodule then a annihilates the simple module A/M so $aA \subseteq M$ and, in particular, $a = a \cdot 1 \in M$. Hence, rad $A \subseteq M$ for each such submodule M and rad $A \subseteq I$, their intersection. Suppose that this inclusion is proper so I is not contained in rad A. Hence, there must be a simple A-module S with $IS \neq 0$. Choose $0 \neq s \in S$ with $Is \neq 0$ so $Is = S$ as Is is a submodule of S. Hence, there is $x \in I$ with $xs = -s$ so $(x+1)s = 0$. Therefore, $x+1$ lies in a proper left ideal of A, the annihilator of s, so $x+1$ lies in a maximal submodule M which contains this annihilator.

But $x \in I \subseteq M$, by definition of I, so $1 = (x+1) - x \in M$, a contradiction. Hence, rad A is not properly contained in I and the theorem is completely proved.

We shall now pause and examine a good example, namely $T_n(k)$, the algebra of $n \times n$ lower triangular matrices. Let N be the subset consisting of matrices with all diagonal entries zero. It is easy to verify that N is an ideal and that it is nilpotent; in fact, $N^n = 0$. Let M_i, $1 \leqslant i \leqslant n$, consist of the elements of $T_n(k)$ which have a zero in the ith diagonal position. It is also easy to see that M_i is an ideal. In particular, M_i is a submodule and, since it is of codimension one, it follows that $S_i = T_n(k)/M_i$ is a simple module. The way that an element t of $T_n(k)$ acts on S_i is by multiplication by that scalar which is the ith diagonal entry of t: this is immediate from matrix multiplication. Hence, $S_1, \ldots, S_n$ are n non-isomorphic simple $T_n(k)$-modules. We also have that $N = M_1 \cap \cdots \cap M_n$ so $T_n(k)/N \cong S_1 \oplus \cdots \oplus S_n$ since there is an embedding of the left-hand side in the right and both sides are n-dimensional. Thus, $T_n(k)/N$ is a semisimple module so $N \subseteq$ rad $T_n(k)$. But N is nilpotent so $N \supseteq$ rad $T_n(k)$ and therefore $N =$ rad $T_n(k)$. Finally, if S is any simple $T_n(k)$-module then S is isomorphic with one of $S_1, \ldots, S_n$. Indeed, S is isomorphic with a quotient of the $T_n(k)$-module $T_n(k)$ so S is a composition factor of $T_n(k)/\text{rad } T_n(k)$.

The remainder of this first section is devoted to using our results to study modules which are not semisimple by showing how they are made up of 'layers' of semisimple modules.

Proposition 4 *If U is an A-module then the following are equal:*

(1) (rad A)U;

(2) *the smallest submodule of U with semisimple quotient;*

(3) *the intersection of all maximal submodules of U.*

Part of the proof of Theorem 3 showed that, for the case $U = A$, the submodule described in the second statement exists and is equal to the intersection described in (3). The argument works equally well for an arbitrary A-module. It suffices therefore to prove that the modules given in (1) and (2) are the same.

However, rad A annihilates $U/(\text{rad } A)U$ so the quotient is a module for $A/\text{rad } A$. But $A/\text{rad } A$ is semisimple so each of its modules is semisimple, as we have seen above, and so $U/(\text{rad } A)U$ is certainly semisimple as an $A/\text{rad } A$-module and so as an A-module. Thus, to prove the proposition, we need only show that if U/V is semisimple then (rad A)$U \subseteq V$. However, the

semisimplicity of U/V means that rad A annihilates U/V, which is just what we want.

The submodule of U given by the proposition is called the *radical* of U and is denoted rad(U). Of course, if $U = A$ then this definition coincides with the prior one. Since rad(U) is also an A-module, it too has a radical and

$$\text{rad}(\text{rad}(U)) = (\text{rad } A)((\text{rad } A)U) = (\text{rad } A)^2 U.$$

We denote this by $\text{rad}^2(U)$ and define $\text{rad}^n(U)$ recursively so $\text{rad}^n(U) = (\text{rad } A)^n U$ and is the radical of $\text{rad}^{n-1}(U)$. Since a power of rad A is zero we have that $\text{rad}^r(U) = 0$ with $\text{rad}^{r-1}(U) \neq 0$ (letting $\text{rad}^0(U) = U$ for convenience) for some positive integer r which is called the *radical length* of U. The sequence of modules

$$U = \text{rad}^0(U) \supseteq \text{rad}^1(U) \supseteq \text{rad}^2(U) \supseteq \cdots$$

is called the *radical series* of U. Each of the successive quotients is semisimple and we have a description of U in terms of semisimple modules.

This description of U starts with U and proceeds with a sequence of smaller and smaller modules. We now shall give another similar description that works the other way around, from small submodules to large. The first result is analogous to Proposition 4.

Proposition 5 *If U is an A-module then the following are equal:*

(1) *the set of u in U with* (rad A)$u = 0$;
(2) *the largest semisimple submodule of U;*
(3) *the sum of all the simple submodules of U.*

It is trivial that the set given by (1) is a submodule and, since it is annihilated by rad A, it is certainly semisimple. If V_1 and V_2 are semisimple submodules then so is $V_1 + V_2$, inasmuch as this sum is a homomorphic image of $V_1 \oplus V_2$, so the module described in (2) does exist and thus contains the module from (1). But rad A annihilates any semisimple submodule so the first two modules coincide. Finally, the sum of simple submodules is semisimple, by the above argument, and any semisimple module is the direct sum of simple modules so the result is proven.

The submodule just described is called the *socle* of U and is written soc(U). Now $U/\text{soc}(U)$ is a module so it, too, has a socle and we let $\text{soc}^2(U)$ be the submodule of U containing soc(U) such that $\text{soc}^2(U)/\text{soc}(U)$ is the socle of $U/\text{soc}(U)$. Hence, $(\text{rad } A)^2 \text{ soc}^2(U) = 0$, since $(\text{rad } A)\text{ soc}^2(U) \subseteq \text{soc}(U)$ and $(\text{rad } A)\text{ soc}(U) = 0$. In fact, this characterizes $\text{soc}^2 U$, since $(\text{rad } A)^2 u = 0$ means rad A annihilates (rad A)u so (rad A)$u \subseteq \text{soc}(U)$ and

thus rad A annihilates the coset of soc U containing u. This means that this coset is in $\text{soc}^2(U)$. Similarly, we can carry on and define, inductively, $\text{soc}^n(U)$ (letting $\text{soc}^0 U = 0$ for convenience) and this will consist of the elements of U annihilated by $(\text{rad } A)^n$. We have a *socle series*

$$0 = \text{soc}^0(U) \subseteq \text{soc}^1(U) \subseteq \text{soc}^2(U) \cdots$$

and the first positive integer r with $\text{soc}^r(U) = U$ is called the *socle length* of U. Again we have a description of U in terms of semisimple layers.

Exercises

1 Determine the radical and socle series of the $T_n(k)$-module $T_n(k)$.

2 Prove that

$$\text{rad}^i(T_n(k))/\text{rad}^{i+1}(T_n(k)) \cong S_{i+1} \oplus \cdots \oplus S_n,$$

$0 \leqslant i < n$, and that

$$\text{soc}^{i+1}(T_n(k))/\text{soc}^i(T_n(k)) \cong S_{n-i} \oplus \cdots \oplus S_{n-i}$$

where $0 \leqslant i < n$ and S_{n-i} appears $n-i$ times.

3 If U is an A-module then the radical length and socle length of U coincide (and this common length is the *Loewy length*).

4 If U is an A-module of Loewy length s then, for $0 \leqslant i \leqslant s$, $\text{rad}^i(U) \subseteq \text{soc}^{s-i}(U)$.

2 Simple algebras

We shall use our knowledge of modules to prove the basic structure theorems for simple and semisimple algebras. The idea is to pass from information on module structure to knowledge about endomorphisms and then algebras.

For any A-module U we let $\text{End}(U)$ be the algebra of all endomorphisms of U. We also let A° denote the opposite algebra to A, that is, the algebra with the same underlying set and linear structure as A but with new multiplication, $a \circ b = ba$.

Lemma 1 $\text{End}(A) \cong A^\circ$.

This is a trivial but vital fact about the A-module A. It is easy to prove. For each $a \in A$, let ρ_a be the linear transformation of A given by $\rho_a(x) = xa$, for $x \in A$. It is easy to verify that $\rho_a \in \text{End}(A)$ and $\rho_a \circ \rho_b = \rho_{ba}$ whenever $a, b \in A$. Moreover, if $\rho \in \text{End}(A)$ let $c = \rho(1)$ so, for any $x \in A$,

$$\rho(x) = \rho(x \cdot 1) = x\rho(1) = xc = \rho_c(x)$$

and $\rho = \rho_c$. Hence, the map which sends $a \in A^\circ$ to ρ_a is an algebra homomorphism of A° onto $\mathrm{End}(A)$ and it is one-to-one since $\rho_a = \rho_b$ implies that $a = \rho_a(1) = \rho_b(1) = b$.

The other key fact is Schur's lemma, which says that only the scalar multiplications are endomorphisms of a simple module:

Lemma 2 *If S is a simple A-module then* $\mathrm{End}(S) = kI$.

Proof Let $\rho \in \mathrm{End}(S)$ so ρ is certainly a linear transformation of S. Let $\lambda \in k$ be an eigenvalue of ρ so $\rho - \lambda I$ is a singular linear transformation and also an endomorphism. Thus $(\rho - \lambda I)S$ is a submodule of S and properly contained in S. Hence, this image is zero, $\rho - \lambda I = 0$ and $\rho = \lambda I$ as asserted.

Now that we understand endomorphisms of simple modules, let us go on to direct sums of modules. Suppose that the A-module U is a direct sum $U = U_1 + \cdots + U_r$. If $\rho \in \mathrm{End}(U)$ and $u_j \in U_j$ then $\rho(u_j)$ has an expression given by the direct decomposition: let ρ_{ij} be the function from U_j to U_i which attaches the ith component of $\rho(u_j)$ to u_j. Now ρ_{ij} is then the composition of the natural injection of U_j into U, ρ and the projection of U onto U_i so $\rho_{ij} \in \mathrm{Hom}_A(U_j, U_i)$. Moreover, $\rho(u_j) = \sum_i \rho_{ij}(u_j)$. Hence, if $\rho(u_1 + \cdots + u_r) = v_1 + \cdots + v_r$, with the obvious notation, then we can express this in terms of matrix multiplication as follows:

$$\begin{pmatrix} \rho_{11} & \cdots & \rho_{1r} \\ \vdots & & \vdots \\ \rho_{r1} & \cdots & \rho_{rr} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix}.$$

Let E consist of all $r \times r$ matrices whose i, j entry comes from $\mathrm{Hom}_A(U_j, U_i)$ so it is clear that such matrices add and multiply to form an algebra. To each $\rho \in \mathrm{End}(U)$ we have attached $M(\rho) \in E$. Furthermore, it is easy to check that every element of E so arises and the mapping M is an isomorphism. Summarizing, we have

Lemma 3 *If the A-module U is a direct sum*

$$U = U_1 + \cdots + U_r$$

of submodules then $\mathrm{End}(U)$ *is isomorphic with the algebra of all $r \times r$ matrices whose i, j entries come from* $\mathrm{Hom}_A(U_j, U_i)$.

This is just a generalization of the usual way of attaching matrices to linear transformations: we have gone from k-modules, that is, vector spaces, to A-modules. We can now use these ideas to derive easily a deep consequence.

Theorem 4 *If A is simple then A is a matrix algebra.*

More specifically, there is a positive integer n and an isomorphism between A and the algebra $M_n(k)$ of all $n \times n$ matrices over k.

Proof Let S be a simple submodule of A and let U be the sum of all submodules isomorphic with S. In particular, U is semisimple and, furthermore, if we express U as a direct sum of n simple submodules, then each of these summands is isomorphic with S since U, and hence each homomorphic image of U, is a sum of modules isomorphic with S. Hence, Lemmas 2 and 3 imply that $\mathrm{End}(U) \cong M_n(k)$.

However, if $\rho \in \mathrm{End}(A)$ then $\rho(U) \subseteq U$ because if T is a submodule of A isomorphic with S then the homomorphic image $\rho(T)$ of T is either zero or also isomorphic with S. From the proof of Lemma 1, we know this means that U is a right ideal so it must now be an ideal. But A is simple so $A = U$ and

$$A^{\circ} \cong \mathrm{End}(A) = \mathrm{End}(U) \cong M_n(k).$$

Thus, any isomorphism of A° onto $M_n(k)$, composed with the taking of transposes, is the needed isomorphism.

We have also proved that A is semisimple in the midst of this proof. It is conversely true that $M_n(k)$ is simple and semisimple. Indeed, $M_n(k)$ has a simple module S consisting of column vectors of length n over k; the simplicity of S is immediate from the fact that $M_n(k)s = S$ for any $s \in S$, $s \neq 0$. Moreover, $M_n(k)$, as a module over itself, has a direct decomposition

$$M_n(k) = C_1 + \cdots + C_n$$

where C_i consists of the matrices which have zero entries outside the ith column. Each C_i is isomorphic with S so $M_n(k)$ is semisimple. Moreover, $M_n(k)$ has just one simple module, as any simple module would be a composition factor of the module $M_n(k)$. Now suppose that $0 \neq I$ is an ideal of $M_n(k)$. Let L be a simple submodule of I so $L \cong S$ and L is a module summand of $M_n(k)$. In particular, there is a module endomorphism φ_i of $M_n(k)$ such that $\varphi_i(L) = C_i$. By Lemma 1, φ_i is given by a right multiplication, $L \subseteq I$, an ideal, so $C_i = \varphi_i(L) \subseteq I$. Hence $I = M_n(k)$ as desired.

In passing, note that the integer n of the matrix algebra $M_n(k)$ is characterized as the number of summands when $M_n(k)$ is expressed as a direct sum of simple submodules, all of which are then isomorphic. This fact is useful when we are working with non-semisimple modules later.

Our next goal is to generalize these results to semisimple algebras, again

using module decompositions and endomorphisms. To do this we need the concept of a direct sum of algebras, which is really two ideas, internal and external direct sums, in analogy with the similar ideas for modules.

If $A_1, A_2, \ldots, A_t$ are algebras, form

$$A_1 \oplus \cdots \oplus A_t$$

and make this into an algebra, by defining all operations in a componentwise fashion, the direct sum of $A_1, \ldots, A_t$. Let B_i consist of the t-tuples which are zero except perhaps in the ith component, so B_i is an algebra, $B_i \cong A_i$ and the direct sum is the vector space direct sum of its ideals $B_1, \ldots, B_t$. On the other hand, if the algebra A has ideals $A_1, \ldots, A_t$ and A is the vector space direct sum $A = A_1 + \cdots + A_t$ then

$$A \cong A_1 \oplus \cdots \oplus A_t$$

by the obvious map, as is quite easy to verify.

This idea arises in several ways, one of which follows.

Lemma 5 *If the A-module U is a direct sum of submodules*

$$U = U_1 \oplus \cdots \oplus U_t$$

and $\mathrm{Hom}_A(U_i, U_j) = 0$ *when* $i \neq j$, *then*

$$\mathrm{End}(U) \cong \mathrm{End}(U_1) \oplus \cdots \oplus \mathrm{End}(U_t).$$

Proof This is an immediate consequence of Lemma 3, which implies that $\mathrm{End}(U)$ is isomorphic with the algebra of $t \times t$ matrices with zero i, j entries if $i \neq j$ and i, i entries from $\mathrm{Hom}_A(U_i, U_i)$.

Theorem 6 *If A is a semisimple algebra then A is the direct sum of matrix algebras.*

Proof Suppose that A has exactly t simple modules $S_1, \ldots, S_t$, up to isomorphism of course. The semisimplicity of A implies that we can express the A-module A as a direct sum

$$A = U_1 + \cdots + U_t$$

where U_i is a direct sum of simple modules each isomorphic with S_i. If $\varphi \in \mathrm{Hom}_A(U_i, U_j)$ then $\varphi(U_i)$ is a submodule of U_j and isomorphic with a quotient module of U_i so if $i \neq j$ we must have $\varphi = 0$. Hence, Lemma 5 gives us that

$$\mathrm{End}(A) \cong \mathrm{End}(U_1) \oplus \cdots \oplus \mathrm{End}(U_t).$$

However, $A^\circ \cong \mathrm{End}(A)$ and each algebra $\mathrm{End}(U_i)$ is a matrix algebra, just as in the argument of Theorem 4, so we have the desired isomorphism here, too, in the same way.