Modern Algebra

Chapter IX. The Structure of Rings

IX.1. Simple and Primitive Rings—Proofs of Theorems

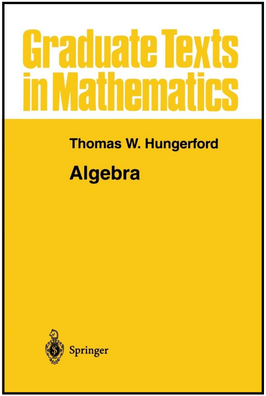

Table of contents

1. Lemma IX.1.A
2. Lemma IX.1.B
3. Theorem IX.1.3
4. Theorem IX.1.4
5. Proposition IX.1.6
6. Proposition IX.1.7
7. Lemma IX.1.C
8. Theorem IX.1.9
9. Lemma IX.1.10 (Schur)
10. Lemma IX.1.11
11. Theorem IX.1.12. Jacobson Density Theorem
12. Corollary IX.1.13
13. Theorem IX.1.14. Wedderburn-Artin Theorem for Simple Artinian Rings
14. Lemma IX.1.15
15. Lemma IX.1.16
16. Proposition IX.1.17

Lemma IX.1.A

Lemma IX.1.A. Every simple module A is cyclic. In fact, $A = Ra$ for every nonzero $a \in A$.

Proof. First, Ra is a submodule of A by Theorem IV.1.5(i). Consider $B = \{c \in A \mid Rc = \{0\}\}$. Notice that $c_1, c_2 \in B$ implies $R(c_1 - c_2) = Rc_1 - Rc_2 = \{0\} - \{0\} = \{0\}$, so $c_1 - c_2 \in B$ and B is a subgroup of A (by Theorem I.2.5). By Definition IV.1.3, "submodule," B is a submodule of A (i.e., a sub-R-module of A).

Lemma IX.1.A

Lemma IX.1.A. Every simple module A is cyclic. In fact, $A = Ra$ for every nonzero $a \in A$.

Proof. First, Ra is a submodule of A by Theorem IV.1.5(i). Consider $B = \{c \in A \mid Rc = \{0\}\}$. Notice that $c_1, c_2 \in B$ implies $R(c_1 - c_2) = Rc_1 - Rc_2 = \{0\} - \{0\} = \{0\}$, so $c_1 - c_2 \in B$ and B is a subgroup of A (by Theorem I.2.5). By Definition IV.1.3, "submodule," B is a submodule of A (i.e., a sub-R-module of A). Since A is simple, then Ra is either $\{0\}$ of A and similarly for B. Also, since A is simple, then by Definition IX.1.1, $RA \neq \{0\}$; but $RB = \{0\}$ and we must have $B \neq A$. This implies that $B = \{0\}$ and so $Ra = \{0\}$ only when $a = 0$. So for all $a \in A$ where $a \neq 0$ we must have $Ra = A$, as claimed.

Lemma IX.1.A

Lemma IX.1.A. Every simple module A is cyclic. In fact, $A = Ra$ for every nonzero $a \in A$.

Proof. First, Ra is a submodule of A by Theorem IV.1.5(i). Consider $B = \{c \in A \mid Rc = \{0\}\}$. Notice that $c_1, c_2 \in B$ implies $R(c_1 - c_2) = Rc_1 - Rc_2 = \{0\} - \{0\} = \{0\}$, so $c_1 - c_2 \in B$ and B is a subgroup of A (by Theorem I.2.5). By Definition IV.1.3, "submodule," B is a submodule of A (i.e., a sub-R-module of A). Since A is simple, then Ra is either $\{0\}$ of A and similarly for B. Also, since A is simple, then by Definition IX.1.1, $RA \neq \{0\}$; but $RB = \{0\}$ and we must have $B \neq A$. This implies that $B = \{0\}$ and so $Ra = \{0\}$ only when $a = 0$. So for all $a \in A$ where $a \neq 0$ we must have $Ra = A$, as claimed. Now the cyclic submodule of A generated by a consists of $\{ra + na \mid r \in Rmb \in \mathbb{Z}\}$ by Theorem IV.1.5(ii). But $Ra = A$ and so Ra includes all of $\{ra + na \mid r \in Rmb \in \mathbb{Z}\}$ and hence R-module A is cyclic and generated by a. □

Lemma IX.1.A

Lemma IX.1.A. Every simple module A is cyclic. In fact, $A = Ra$ for every nonzero $a \in A$.

Proof. First, Ra is a submodule of A by Theorem IV.1.5(i). Consider $B = \{c \in A \mid Rc = \{0\}\}$. Notice that $c_1, c_2 \in B$ implies $R(c_1 - c_2) = Rc_1 - Rc_2 = \{0\} - \{0\} = \{0\}$, so $c_1 - c_2 \in B$ and B is a subgroup of A (by Theorem I.2.5). By Definition IV.1.3, "submodule," B is a submodule of A (i.e., a sub-R-module of A). Since A is simple, then Ra is either $\{0\}$ of A and similarly for B. Also, since A is simple, then by Definition IX.1.1, $RA \neq \{0\}$; but $RB = \{0\}$ and we must have $B \neq A$. This implies that $B = \{0\}$ and so $Ra = \{0\}$ only when $a = 0$. So for all $a \in A$ where $a \neq 0$ we must have $Ra = A$, as claimed. Now the cyclic submodule of A generated by a consists of $\{ra + na \mid r \in Rmb \in \mathbb{Z}\}$ by Theorem IV.1.5(ii). But $Ra = A$ and so Ra includes all of $\{ra + na \mid r \in Rmb \in \mathbb{Z}\}$ and hence R-module A is cyclic and generated by a. □

Lemma IX.1.B

Lemma IX.1.B. Let $A = Ra$ be a cyclic R-module. Define $\theta : R \to A$ as $\theta(r) = ra$. Then $R/\text{Ker}(\theta)$ (and hence A) has no proper submodules if and only if $\text{Ker}(\theta)$ is a maximal left ideal of R.

Proof. Define $\theta : R \to A$ as $\theta(r) = ra$. By Theorem IV.1.5(i), θ is an R-module epimorphism (onto homomorphism). The kernel of θ is its kernel as a homomorphism of abelian groups (by definition, see Section IV.1) and so the kernel of θ determines a subgroup of the additive abelian group of R by Exercise I.2.9(a).

Lemma IX.1.B

Lemma IX.1.B. Let $A = Ra$ be a cyclic R-module. Define $\theta : R \to A$ as $\theta(r) = ra$. Then $R/\mathrm{Ker}(\theta)$ (and hence A) has no proper submodules if and only if $\mathrm{Ker}(\theta)$ is a maximal left ideal of R.

Proof. Define $\theta : R \to A$ as $\theta(r) = ra$. By Theorem IV.1.5(i), θ is an R-module epimorphism (onto homomorphism). The kernel of θ is its kernel as a homomorphism of abelian groups (by definition, see Section IV.1) and so the kernel of θ determines a subgroup of the additive abelian group of R by Exercise I.2.9(a). For $b \in \mathrm{Ker}(\theta)$ and $r \in R$ we have $rb \in \mathrm{Ker}(\theta)$ since $\theta(rb) = (rb)a = r(ba) = r\theta(b) = r0 = 0$. So by Definition IV.1.3, $I = \mathrm{Ker}(\theta)$ is a submodule of A. By the First Isomorphism Theorem (Theorem IV.1.7), $R/I = R/\mathrm{Ker}(\theta) \cong A$.

Lemma IX.1.B

Lemma IX.1.B. Let $A = Ra$ be a cyclic R-module. Define $\theta : R \to A$ as $\theta(r) = ra$. Then $R/\text{Ker}(\theta)$ (and hence A) has no proper submodules if and only if $\text{Ker}(\theta)$ is a maximal left ideal of R.

Proof. Define $\theta : R \to A$ as $\theta(r) = ra$. By Theorem IV.1.5(i), θ is an R-module epimorphism (onto homomorphism). The kernel of θ is its kernel as a homomorphism of abelian groups (by definition, see Section IV.1) and so the kernel of θ determines a subgroup of the additive abelian group of R by Exercise I.2.9(a). For $b \in \text{Ker}(\theta)$ and $r \in R$ we have $rb \in \text{Ker}(\theta)$ since $\theta(rb) = (rb)a = r(ba) = r\theta(b) = r0 = 0$. So by Definition IV.1.3, $I = \text{Ker}(\theta)$ is a submodule of A. By the First Isomorphism Theorem (Theorem IV.1.7), $R/I = R/\text{Ker}(\theta) \cong A$. By Theorem IV.1.10, every submodule of R/I is of the form J/I, where J is a left ideal of R that contains $I = \text{Ker}(\theta)$. So module $R/\text{Ker}(\theta) = R/I$ (and hence A since $R/I \cong A$) has no proper submodules if and only if $I = \text{Ker}$ is a maximal left ideal of R. □

Lemma IX.1.B

Lemma IX.1.B. Let $A = Ra$ be a cyclic R-module. Define $\theta : R \to A$ as $\theta(r) = ra$. Then $R/\text{Ker}(\theta)$ (and hence A) has no proper submodules if and only if $\text{Ker}(\theta)$ is a maximal left ideal of R.

Proof. Define $\theta : R \to A$ as $\theta(r) = ra$. By Theorem IV.1.5(i), θ is an R-module epimorphism (onto homomorphism). The kernel of θ is its kernel as a homomorphism of abelian groups (by definition, see Section IV.1) and so the kernel of θ determines a subgroup of the additive abelian group of R by Exercise I.2.9(a). For $b \in \text{Ker}(\theta)$ and $r \in R$ we have $rb \in \text{Ker}(\theta)$ since $\theta(rb) = (rb)a = r(ba) = r\theta(b) = r0 = 0$. So by Definition IV.1.3, $I = \text{Ker}(\theta)$ is a submodule of A. By the First Isomorphism Theorem (Theorem IV.1.7), $R/I = R/\text{Ker}(\theta) \cong A$. By Theorem IV.1.10, every submodule of R/I is of the form J/I, where J is a left ideal of R that contains $I = \text{Ker}(\theta)$. So module $R/\text{Ker}(\theta) = R/I$ (and hence A since $R/I \cong A$) has no proper submodules if and only if $I = \text{Ker}$ is a maximal left ideal of R. □

Theorem IX.1.3

Theorem IX.1.3. A left module A over ring R is simple if and only if A is isomorphic to R/I for some regular maximal left ideal I. This holds also if we replace "left" with "right."

Proof. Suppose A is simple. Then by Note IX.1.A, $A = Ra \cong R/I$ where U is some maximal left ideal. Since $A = Ra$ then $a = ea$ for some $e \in R$. So for any $r \in R$, $ra = req$ or $(r - re)a = 0$, whence $r - re \in \text{Ker}(\theta) = I$ where $\theta : R \to A$ is the epimorphism of Lemma IX.1.B defined as $\theta(r) = ra$. Therefore I is regular.

Theorem IX.1.3

Theorem IX.1.3. A left module A over ring R is simple if and only if A is isomorphic to R/I for some regular maximal left ideal I. This holds also if we replace "left" with "right."

Proof. Suppose A is simple. Then by Note IX.1.A, $A = Ra \cong R/I$ where U is some maximal left ideal. Since $A = Ra$ then $a = ea$ for some $e \in R$. So for any $r \in R$, $ra = req$ or $(r - re)a = 0$, whence $r - re \in \text{Ker}(\theta) = I$ where $\theta : R \to A$ is the epimorphism of Lemma IX.1.B defined as $\theta(r) = ra$. Therefore I is regular.

Suppose I is a regular maximal left ideal of R such that $A \cong R/I$ is of the form J/I where J is a left ideal of R that contains I. So module $R/I \cong A$ has no proper submodules since I is a maximal left ideal. So to show that $A \cong R/I$ is simple we need to show that $RA = R(R/I) \neq \{0\}$.

Theorem IX.1.3

Theorem IX.1.3. A left module A over ring R is simple if and only if A is isomorphic to R/I for some regular maximal left ideal I. This holds also if we replace "left" with "right."

Proof. Suppose A is simple. Then by Note IX.1.A, $A = Ra \cong R/I$ where U is some maximal left ideal. Since $A = Ra$ then $a = ea$ for some $e \in R$. So for any $r \in R$, $ra = req$ or $(r - re)a = 0$, whence $r - re \in \mathrm{Ker}(\theta) = I$ where $\theta : R \to A$ is the epimorphism of Lemma IX.1.B defined as $\theta(r) = ra$. Therefore I is regular.

Suppose I is a regular maximal left ideal of R such that $A \cong R/I$ is of the form J/I where J is a left ideal of R that contains I. So module $R/I \cong A$ has no proper submodules since I is a maximal left ideal. So to show that $A \cong R/I$ is simple we need to show that $RA = R(R/I) \neq \{0\}$.

Theorem IX.1.3 (continued)

Theorem IX.1.3. A left module A over ring R is simple if and only if A is isomorphic to R/I for some regular maximal left ideal I. This holds also if we replace "left" with "right."

Proof (continued). ASSUME $R(R/I) = \{0\}$. Then for all $r \in R$, $r(e + I) \in R(R/I)$, where $r - re \in I$ by the regularity of I, and so $r(e + 1) = I$ (the identity in R/I), or $re + I = I$ or $re \in I$. Since $r - re \in I$, then $r \in I$ and so $R = I$. But this CONTRADICTS the definition maximal ideal (we need $I \neq R$; see Definition III.2.7 of maximal ideal).

Theorem IX.1.3 (continued)

Theorem IX.1.3. A left module A over ring R is simple if and only if A is isomorphic to R/I for some regular maximal left ideal I. This holds also if we replace "left" with "right."

Proof (continued). ASSUME $R(R/I) = \{0\}$. Then for all $r \in R$, $r(e + I) \in R(R/I)$, where $r - re \in I$ by the regularity of I, and so $r(e + 1) = I$ (the identity in R/I), or $re + I = I$ or $re \in I$. Since $r - re \in I$, then $r \in I$ and so $R = I$. But this CONTRADICTS the definition maximal ideal (we need $I \neq R$; see Definition III.2.7 of maximal ideal). So the assumption that $R(R/I) = \{0\}$ is false and we must have $RA = R(R/I) \neq \{0\}$. Therefore by Definition IX.1.1, A is simple. □

Theorem IX.1.3 (continued)

Theorem IX.1.3. A left module A over ring R is simple if and only if A is isomorphic to R/I for some regular maximal left ideal I. This holds also if we replace "left" with "right."

Proof (continued). ASSUME $R(R/I) = \{0\}$. Then for all $r \in R$, $r(e + I) \in R(R/I)$, where $r - re \in I$ by the regularity of I, and so $r(e + 1) = I$ (the identity in R/I), or $re + I = I$ or $re \in I$. Since $r - re \in I$, then $r \in I$ and so $R = I$. But this CONTRADICTS the definition maximal ideal (we need $I \neq R$; see Definition III.2.7 of maximal ideal). So the assumption that $R(R/I) = \{0\}$ is false and we must have $RA = R(R/I) \neq \{0\}$. Therefore by Definition IX.1.1, A is simple. □

Theorem IX.1.4

Theorem IX.1.4. Let B be a subset of a left module A over a ring R. Then $\mathcal{A}(B) = \{r \in R \mid rb = 0 \text{ for all } b \in B\}$ is a left ideal of R. If B is a submodule of A, then $\mathcal{A}(B)$ is an (two sided) ideal.

Proof. Let $r \in R$ and $s \in \mathcal{A}(B)$. Then $sb = 0$ for all $b \in B$ and so $(rs)b = r(sb) = r0 = 0$ for all $b \in B$; i.e., $rs \in \mathcal{A}(B)$. So $\mathcal{A}(B)$ is a left ideal of R.

Theorem IX.1.4

Theorem IX.1.4. Let B be a subset of a left module A over a ring R. Then $\mathcal{A}(B) = \{r \in R \mid rb = 0 \text{ for all } b \in B\}$ is a left ideal of R. If B is a submodule of A, then $\mathcal{A}(B)$ is an (two sided) ideal.

Proof. Let $r \in R$ and $s \in \mathcal{A}(B)$. Then $sb = 0$ for all $b \in B$ and so $(rs)b = r(sb) = r0 = 0$ for all $b \in B$; i.e., $rs \in \mathcal{A}(B)$. So $\mathcal{A}(B)$ is a left ideal of R.

Suppose B is a submodule of A. If $r \in R$ and $s \in \mathcal{A}(B)$, then for every $b \in B$ we have $(sr)b = s(rb) = s0 = 0$ since $rb \in B$ because B is a submodule of A (see Definition IV.1.3). Consequently $sr \in \mathcal{A}(B)$ and so $\mathcal{A}(B)$ is also a right ideal and hence a (two sided) ideal. □

Theorem IX.1.4

Theorem IX.1.4. Let B be a subset of a left module A over a ring R. Then $\mathcal{A}(B) = \{r \in R \mid rb = 0 \text{ for all } b \in B\}$ is a left ideal of R. If B is a submodule of A, then $\mathcal{A}(B)$ is an (two sided) ideal.

Proof. Let $r \in R$ and $s \in \mathcal{A}(B)$. Then $sb = 0$ for all $b \in B$ and so $(rs)b = r(sb) = r0 = 0$ for all $b \in B$; i.e., $rs \in \mathcal{A}(B)$. So $\mathcal{A}(B)$ is a left ideal of R.

Suppose B is a submodule of A. If $r \in R$ and $s \in \mathcal{A}(B)$, then for every $b \in B$ we have $(sr)b = s(rb) = s0 = 0$ since $rb \in B$ because B is a submodule of A (see Definition IV.1.3). Consequently $sr \in \mathcal{A}(B)$ and so $\mathcal{A}(B)$ is also a right ideal and hence a (two sided) ideal. □

Proposition IX.1.6

Proposition IX.1.6. A simple ring R with identity is primitive.

Proof. By Theorem III.2.18, R contains a maximal left ideal I. Since R has an identity then ideal I is regular (use $e = 1_R$ in Definition IX.1.2, "regular ideal"). Whence left R-module R/I is (isomorphic to) a simple R-module by Theorem IX.1.3.

Proposition IX.1.6

Proposition IX.1.6. A simple ring R with identity is primitive.

Proof. By Theorem III.2.18, R contains a maximal left ideal I. Since R has an identity then ideal I is regular (use $e = 1_R$ in Definition IX.1.2, "regular ideal"). Whence left R-module R/I is (isomorphic to) a simple R-module by Theorem IX.1.3. Now the annihilator $\mathcal{A}(R/I)$ is a (left) ideal of R by Theorem IX.1.4. Since R is simple by hypothesis, then $\mathcal{A}(R/I)$ must be either $\{0\}$ or R. Since I is a maximal ideal in R then $I \neq R$ (see Definition III.2.17 of maximal ideal) and so $R/I \neq \{0\}$. So 1_R cannot be in $\mathcal{A}(R/I)$; that is, $\mathcal{A}(R/I) \neq R$. Hence it must be that $\mathcal{A}(R/I) = \{0\}$. Therefore, left R-module R/I is faithful and ring R is primitive by Definition IX.1.5. □

Proposition IX.1.6

Proposition IX.1.6. A simple ring R with identity is primitive.

Proof. By Theorem III.2.18, R contains a maximal left ideal I. Since R has an identity then ideal I is regular (use $e = 1_R$ in Definition IX.1.2, "regular ideal"). Whence left R-module R/I is (isomorphic to) a simple R-module by Theorem IX.1.3. Now the annihilator $\mathcal{A}(R/I)$ is a (left) ideal of R by Theorem IX.1.4. Since R is simple by hypothesis, then $\mathcal{A}(R/I)$ must be either $\{0\}$ or R. Since I is a maximal ideal in R then $I \neq R$ (see Definition III.2.17 of maximal ideal) and so $R/I \neq \{0\}$. So 1_R cannot be in $\mathcal{A}(R/I)$; that is, $\mathcal{A}(R/I) \neq R$. Hence it must be that $\mathcal{A}(R/I) = \{0\}$. Therefore, left R-module R/I is faithful and ring R is primitive by Definition IX.1.5. □

Proposition IX.1.7

Proposition IX.1.7. A commutative ring R is primitive if and only if R is a field.

Proof. Suppose R is a field. Then R is a division ring and by the first example in this section of class notes, R is simple. Since a field has an identity, then by Proposition IX.1.6, R is primitive.

Proposition IX.1.7

Proposition IX.1.7. A commutative ring R is primitive if and only if R is a field.

Proof. Suppose R is a field. Then R is a division ring and by the first example in this section of class notes, R is simple. Since a field has an identity, then by Proposition IX.1.6, R is primitive.

Suppose R is a commutative primitive ring. By Definition IX.1.5, this means there is a simple faithful (left) R-module A; that is, simple R-module A satisfies $\mathcal{A}(A) = \{0\}$. By Theorem IX.1.3, $A \cong R/I$ for some regular maximal left ideal I. Since R is commutative then I is a (two sided) ideal.

Proposition IX.1.7

Proposition IX.1.7. A commutative ring R is primitive if and only if R is a field.

Proof. Suppose R is a field. Then R is a division ring and by the first example in this section of class notes, R is simple. Since a field has an identity, then by Proposition IX.1.6, R is primitive.

Suppose R is a commutative primitive ring. By Definition IX.1.5, this means there is a simple faithful (left) R-module A; that is, simple R-module A satisfies $\mathcal{A}(A) = \{0\}$. By Theorem IX.1.3, $A \cong R/I$ for some regular maximal left ideal I. Since R is commutative then I is a (two sided) ideal. Also $I \subset \mathcal{A}(R/I) = \mathcal{A}(A) = \{0\}$, so we must have $I = \{0\}$. Since $I = \{0\}$ is regular, by Definition IX.1.2 there is $e \in R$ such that $r - re = r - er \in I$, or $r = re = er$ for all $r \in R$. That is, $e = 1_R$ is an identity for R. Since $I = \{0\}$ is maximal by Corollary III.2.21 (the (iii) implies (i) part), R is a field. □

Proposition IX.1.7

Proposition IX.1.7. A commutative ring R is primitive if and only if R is a field.

Proof. Suppose R is a field. Then R is a division ring and by the first example in this section of class notes, R is simple. Since a field has an identity, then by Proposition IX.1.6, R is primitive.

Suppose R is a commutative primitive ring. By Definition IX.1.5, this means there is a simple faithful (left) R-module A; that is, simple R-module A satisfies $\mathcal{A}(A) = \{0\}$. By Theorem IX.1.3, $A \cong R/I$ for some regular maximal left ideal I. Since R is commutative then I is a (two sided) ideal. Also $I \subset \mathcal{A}(R/I) = \mathcal{A}(A) = \{0\}$, so we must have $I = \{0\}$. Since $I = \{0\}$ is regular, by Definition IX.1.2 there is $e \in R$ such that $r - re = r - er \in I$, or $r = re = er$ for all $r \in R$. That is, $e = 1_R$ is an identity for R. Since $I = \{0\}$ is maximal by Corollary III.2.21 (the (iii) implies (i) part), R is a field. □

Lemma IX.1.C

Lemma IX.1.C/Example. For V a vector space over a division ring D, the endomorphism ring $\text{Hom}_D(V, V)$ is a dense subring of itself.

Proof. Let $n \in \mathbb{N}$, $\{u_1, u_2, \ldots, u_n\}$ be a linearly independent subset of V, and $\{v_1, v_2, \ldots, v_n\} \subset V$. By Theorem IV.2.4 there is a basis U of V that contains $u_1, u_2, \ldots, u_n$. Define the map $\theta : V \to V$ by $\theta(u_i) = v_i$ for $i = 1, 2, \ldots, n$ and $\theta(u) = 0$ for $u \in U \setminus \{u_1, u_2, \ldots, u_n\}$.

Lemma IX.1.C

Lemma IX.1.C/Example. For V a vector space over a division ring D, the endomorphism ring $\mathrm{Hom}_D(V, V)$ is a dense subring of itself.

Proof. Let $n \in \mathbb{N}$, $\{u_1, u_2, \ldots, u_n\}$ be a linearly independent subset of V, and $\{v_1, v_2, \ldots, v_n\} \subset V$. By Theorem IV.2.4 there is a basis U of V that contains $u_1, u_2, \ldots, u_n$. Define the map $\theta : V \to V$ by $\theta(u_i) = v_i$ for $i = 1, 2, \ldots, n$ and $\theta(u) = 0$ for $u \in U \setminus \{u_1, u_2, \ldots, u_n\}$. By Theorem IV.2.4, V is a free D-module. By Theorem IV.2.1(iv), θ is a homomorphism (see the proof of (i) implies (iv)). That is, $\theta \in \mathrm{Hom}_D(V, V)$ and so $\mathrm{Hom}_D(V, V)$ is a dense subring of itself by Definition IV.1.8. □

Lemma IX.1.C

Lemma IX.1.C/Example. For V a vector space over a division ring D, the endomorphism ring $\mathrm{Hom}_D(V, V)$ is a dense subring of itself.

Proof. Let $n \in \mathbb{N}$, $\{u_1, u_2, \ldots, u_n\}$ be a linearly independent subset of V, and $\{v_1, v_2, \ldots, v_n\} \subset V$. By Theorem IV.2.4 there is a basis U of V that contains $u_1, u_2, \ldots, u_n$. Define the map $\theta : V \to V$ by $\theta(u_i) = v_i$ for $i = 1, 2, \ldots, n$ and $\theta(u) = 0$ for $u \in U \setminus \{u_1, u_2, \ldots, u_n\}$. By Theorem IV.2.4, V is a free D-module. By Theorem IV.2.1(iv), θ is a homomorphism (see the proof of (i) implies (iv)). That is, $\theta \in \mathrm{Hom}_D(V, V)$ and so $\mathrm{Hom}_D(V, V)$ is a dense subring of itself by Definition IV.1.8. □

Theorem IX.1.9

Theorem IX.1.9. Let R be a dense ring of endomorphisms of a vector space V over a division ring D. Then R is left (respectively, right) Artinian if and only if $\dim_D(V)$ is finite, in which case $R = \mathrm{Hom}_D(V, V)$.

Proof. Let R be Artinian. ASSUME $\dim_D(V)$ is infinite. Then there exists an infinite linearly independent subset $\{u_1, u_2, \ldots\}$ of V. By Exercise IV.1.7(c), V is a left $\mathrm{Hom}_D(V, V)$-module; since R is a subring of $\mathrm{Hom}_D(V, V)$ (by Definition IX.1.8, "dense ring of endomorphisms") then V is also a left R-module (see Definition IV.1., "R-module").

Theorem IX.1.9

Theorem IX.1.9. Let R be a dense ring of endomorphisms of a vector space V over a division ring D. Then R is left (respectively, right) Artinian if and only if $\dim_D(V)$ is finite, in which case $R = \mathrm{Hom}_D(V, V)$.

Proof. Let R be Artinian. ASSUME $\dim_D(V)$ is infinite. Then there exists an infinite linearly independent subset $\{u_1, u_2, \ldots\}$ of V. By Exercise IV.1.7(c), V is a left $\mathrm{Hom}_D(V, V)$-module; since R is a subring of $\mathrm{Hom}_D(V, V)$ (by Definition IX.1.8, "dense ring of endomorphisms") then V is also a left R-module (see Definition IV.1., "R-module"). For each $n \in \mathbb{N}$ let I_n be the left annihilator in R of the set $\{u_1, u_2, \ldots, u_n\}$. Then $I_1 \supset I_2 \supset \cdots$ is a descending chain of left ideal.

Theorem IX.1.9

Theorem IX.1.9. Let R be a dense ring of endomorphisms of a vector space V over a division ring D. Then R is left (respectively, right) Artinian if and only if $\dim_D(V)$ is finite, in which case $R = \mathrm{Hom}_D(V, V)$.

Proof. Let R be Artinian. ASSUME $\dim_D(V)$ is infinite. Then there exists an infinite linearly independent subset $\{u_1, u_2, \ldots\}$ of V. By Exercise IV.1.7(c), V is a left $\mathrm{Hom}_D(V, V)$-module; since R is a subring of $\mathrm{Hom}_D(V, V)$ (by Definition IX.1.8, "dense ring of endomorphisms") then V is also a left R-module (see Definition IV.1., "R-module"). For each $n \in \mathbb{N}$ let I_n be the left annihilator in R of the set $\{u_1, u_2, \ldots, u_n\}$. Then $I_1 \supset I_2 \supset \cdots$ is a descending chain of left ideal. Let w be any nonzero element of V. Since $\{u_1, u_2, \ldots, u_{n+1}\}$ is linearly independent for each $n \in \mathbb{N}$ and R is dense, then (by Definition IX.1.8, "sense ring of endomorphisms") there is $\theta \in R$ such that $\theta(u_i) = 0$ for $i = 1, 2, \ldots, n$ and $\theta(u_{n+1}) = w \neq 0$. Then $\theta \in I_n$ (since θ annihilates $\{u_1, u_2, \ldots, u_n\}$) but $\theta \notin I_{n+1}$. So $I_n \supset I_{n+1}$ and $I_n \neq I_{n+1}$.

Theorem IX.1.9

Theorem IX.1.9. Let R be a dense ring of endomorphisms of a vector space V over a division ring D. Then R is left (respectively, right) Artinian if and only if $\dim_D(V)$ is finite, in which case $R = \text{Hom}_D(V, V)$.

Proof. Let R be Artinian. ASSUME $\dim_D(V)$ is infinite. Then there exists an infinite linearly independent subset $\{u_1, u_2, \ldots\}$ of V. By Exercise IV.1.7(c), V is a left $\text{Hom}_D(V, V)$-module; since R is a subring of $\text{Hom}_D(V, V)$ (by Definition IX.1.8, "dense ring of endomorphisms") then V is also a left R-module (see Definition IV.1., "R-module"). For each $n \in \mathbb{N}$ let I_n be the left annihilator in R of the set $\{u_1, u_2, \ldots, u_n\}$. Then $I_1 \supset I_2 \supset \cdots$ is a descending chain of left ideal. Let w be any nonzero element of V. Since $\{u_1, u_2, \ldots, u_{n+1}\}$ is linearly independent for each $n \in \mathbb{N}$ and R is dense, then (by Definition IX.1.8, "sense ring of endomorphisms") there is $\theta \in R$ such that $\theta(u_i) = 0$ for $i = 1, 2, \ldots, n$ and $\theta(u_{n+1}) = w \neq 0$. Then $\theta \in I_n$ (since θ annihilates $\{u_1, u_2, \ldots, u_n\}$) but $\theta \notin I_{n+1}$. So $I_n \supset I_{n+1}$ and $I_n \neq I_{n+1}$.

Theorem IX.1.9 (continued)

Proof (continued). But then $I_1 \supset I_2 \supset \cdots$ is a "properly descending" chain and so R cannot be left Artinian, a CONTRADICTION. So the assumption that $\dim_D(V)$ is finite is false. Hence if R is Artinian then $\dim_D(V)$ is finite.

Suppose $\dim_D(V)$ is finite. Then V has a finite basis $\{v_1, v_2, \ldots, v_m\}$. If f is any element of $\hom_D(V, V)$ then f is completely determines by its action on $v_1, v_2, \ldots, v_m$. Since R is dense then, by Definition IX.1.8, there exists $\theta \in R$ such that $\theta(v_i) = f(v_i)$ for $i = 1, 2, \ldots, m$. Whence $f = \theta \in R$ and so $\mathrm{Hom}_D(V, V) \in R$.

Theorem IX.1.9 (continued)

Proof (continued). But then $I_1 \supset I_2 \supset \cdots$ is a "properly descending" chain and so R cannot be left Artinian, a CONTRADICTION. So the assumption that $\dim_D(V)$ is finite is false. Hence if R is Artinian then $\dim_D(V)$ is finite.

Suppose $\dim_D(V)$ is finite. Then V has a finite basis $\{v_1, v_2, \ldots, v_m\}$. If f is any element of $\hom_D(V, V)$ then f is completely determines by its action on $v_1, v_2, \ldots, v_m$. Since R is dense then, by Definition IX.1.8, there exists $\theta \in R$ such that $\theta(v_i) = f(v_i)$ for $i = 1, 2, \ldots, m$. Whence $f = \theta \in R$ and so $\mathrm{Hom}_D(V, V) \in R$. But dense ring of endomorphisms R is a subring of $\mathrm{Hom}_D(V, V)$ (see Definition IX.1.8 again), so $\mathrm{Hom}_D(V, V)$ is isomorphic to the ring of all $n \times n$ matrices with entries from D. By Corollary VIII.1.12, $\mathrm{Mat}_n(D)$ is Artinian. Therefore, since R is a subring of $\mathrm{Hom}_D(V, V)$ then R is Artinian. □

Theorem IX.1.9 (continued)

Proof (continued). But then $I_1 \supset I_2 \supset \cdots$ is a "properly descending" chain and so R cannot be left Artinian, a CONTRADICTION. So the assumption that $\dim_D(V)$ is finite is false. Hence if R is Artinian then $\dim_D(V)$ is finite.

Suppose $\dim_D(V)$ is finite. Then V has a finite basis $\{v_1, v_2, \ldots, v_m\}$. If f is any element of $\hom_D(V, V)$ then f is completely determines by its action on $v_1, v_2, \ldots, v_m$. Since R is dense then, by Definition IX.1.8, there exists $\theta \in R$ such that $\theta(v_i) = f(v_i)$ for $i = 1, 2, \ldots, m$. Whence $f = \theta \in R$ and so $\mathrm{Hom}_D(V, V) \in R$. But dense ring of endomorphisms R is a subring of $\mathrm{Hom}_D(V, V)$ (see Definition IX.1.8 again), so $\mathrm{Hom}_D(V, V)$ is isomorphic to the ring of all $n \times n$ matrices with entries from D. By Corollary VIII.1.12, $\mathrm{Mat}_n(D)$ is Artinian. Therefore, since R is a subring of $\mathrm{Hom}_D(V, V)$ then R is Artinian. □

Lemma IX.1.10 (Schur)

Lemma IX.1.10. (Schur) Let A be a simple module over a ring R and let B be any R-module.

(i) Every nonzero R-module homomorphism $f : A \to B$ is a monomorphism (one to one);

(ii) every nonzero R-module homomorphism $f : B \to A$ is an epimorphism (onto);

(iii) the endomorphism ring $D = \mathrm{Hom}_R(A, A)$ is a division ring.

Proof. (i) The kernel of f is its kernel as a homomorphism of abelian groups (by definition, see Section IV.1) and so the kernel of f determines a subgroup of the additive abelian group of R by Exercise I.2.9(a). For $c \in \mathrm{Ker}(f)$ and $r \in R$ we have $rc \in \mathrm{Ker}(f)$ since $f(rc) = rf(c) = r0 = 0$ (see Definition IV.1.2, "R-module homomorphism"). So by Definition IV.1.3, $\mathrm{Ker}(f)$ is a submodule of A. Since f is nonzero then $\mathrm{Ker}(f) \neq A$.

Lemma IX.1.10 (Schur)

Lemma IX.1.10. (Schur) Let A be a simple module over a ring R and let B be any R-module.

(i) Every nonzero R-module homomorphism $f : A \to B$ is a monomorphism (one to one);

(ii) every nonzero R-module homomorphism $f : B \to A$ is an epimorphism (onto);

(iii) the endomorphism ring $D = \mathrm{Hom}_R(A, A)$ is a division ring.

Proof. (i) The kernel of f is its kernel as a homomorphism of abelian groups (by definition, see Section IV.1) and so the kernel of f determines a subgroup of the additive abelian group of R by Exercise I.2.9(a). For $c \in \mathrm{Ker}(f)$ and $r \in R$ we have $rc \in \mathrm{Ker}(f)$ since $f(rc) = rf(c) = r0 = 0$ (see Definition IV.1.2, "R-module homomorphism"). So by Definition IV.1.3, $\mathrm{Ker}(f)$ is a submodule of A. Since f is nonzero then $\mathrm{Ker}(f) \neq A$.

Lemma IX.1.10 (Schur) continued

Proof (continued). Since A is simple then it must be that $\text{Ker}(f) = \{0\}$ and so f is a monomorphism (one to one) by Theorem I.2.3 (see also page 170 of Hungerford and the example in the class notes after Definition IV.1.3), as claimed.

(ii) $\text{Im}(g)$ is a submodule of A by Exercise I.2.9(b) (see also the example in the class notes after Definition IV.1.3). Since g is nonzero, $\text{Im}(g) \neq \{0\}$. So $\text{Im}(g)$ is a nonzero submodule of A and since A is simple it must be that $\text{Im}(f) = A$. That is, g is an epimorphism (onto), as claimed.

Lemma IX.1.10 (Schur) continued

Proof (continued). Since A is simple then it must be that $\mathrm{Ker}(f) = \{0\}$ and so f is a monomorphism (one to one) by Theorem I.2.3 (see also page 170 of Hungerford and the example in the class notes after Definition IV.1.3), as claimed.

(ii) $\mathrm{Im}(g)$ is a submodule of A by Exercise I.2.9(b) (see also the example in the class notes after Definition IV.1.3). Since g is nonzero, $\mathrm{Im}(g) \neq \{0\}$. So $\mathrm{Im}(g)$ is a nonzero submodule of A and since A is simple it must be that $\mathrm{Im}(f) = A$. That is, g is an epimorphism (onto), as claimed.

(iii) We use parts (i) and (ii). Let $j \in D = \mathrm{Hom}_R(A, A)$ with $h \neq 0$. By (i), h is onto to ne (injective) and by (ii) f is onto (surjective), so h is an isomorphism. By Theorem I.2.3(ii) (see also page 170 of Hungerford) h has a two-sided inverse $h^{-1} \in \mathrm{Hom}_R(A, A) = D$. Since h is an arbitrary nonzero element of D, then D is a division ring. □

Lemma IX.1.10 (Schur) continued

Proof (continued). Since A is simple then it must be that $\text{Ker}(f) = \{0\}$ and so f is a monomorphism (one to one) by Theorem I.2.3 (see also page 170 of Hungerford and the example in the class notes after Definition IV.1.3), as claimed.

(ii) $\text{Im}(g)$ is a submodule of A by Exercise I.2.9(b) (see also the example in the class notes after Definition IV.1.3). Since g is nonzero, $\text{Im}(g) \neq \{0\}$. So $\text{Im}(g)$ is a nonzero submodule of A and since A is simple it must be that $\text{Im}(f) = A$. That is, g is an epimorphism (onto), as claimed.

(iii) We use parts (i) and (ii). Let $j \in D = \text{Hom}_R(A, A)$ with $h \neq 0$. By (i), h is onto to ne (injective) and by (ii) f is onto (surjective), so h is an isomorphism. By Theorem I.2.3(ii) (see also page 170 of Hungerford) h has a two-sided inverse $h^{-1} \in \text{Hom}_R(A, A) = D$. Since h is an arbitrary nonzero element of D, then D is a division ring. □

Lemma IX.1.11

Lemma IX.1.11. Let A be a simple module over a ring R. Consider A as a vector space over the division ring $D = \mathrm{Hom}_R(A, A)$. If V is a finite dimensional D-subspace of the D-vector space A and $a \in A \setminus V$, then there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$.

Proof. We give an induction proof on $n = \dim_D(V)$.

Lemma IX.1.11

Lemma IX.1.11. Let A be a simple module over a ring R. Consider A as a vector space over the division ring $D = \text{Hom}_R(A, A)$. If V is a finite dimensional D-subspace of the D-vector space A and $a \in A \setminus V$, then there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$.

Proof. We give an induction proof on $n = \dim_D(V)$.

Let $n = 0$. Then $V = \{0\}$ and so $a \in A \setminus V$ implies $a \neq 0$. Since A is simple, then by Lemma IX.1.A, $A = Ra$. So there is some $r \in R$ such that $ra = a \neq 0$ and $rV = v\{0\} = \{0\}$, and the claim holds for $n = \dim_D(V) = 0$.

Lemma IX.1.11

Lemma IX.1.11. Let A be a simple module over a ring R. Consider A as a vector space over the division ring $D = \mathrm{Hom}_R(A, A)$. If V is a finite dimensional D-subspace of the D-vector space A and $a \in A \setminus V$, then there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$.

Proof. We give an induction proof on $n = \dim_D(V)$.

Let $n = 0$. Then $V = \{0\}$ and so $a \in A \setminus V$ implies $a \neq 0$. Since A is simple, then by Lemma IX.1.A, $A = Ra$. So there is some $r \in R$ such that $ra = a \neq 0$ and $rV = v\{0\} = \{0\}$, and the claim holds for $n = \dim_D(V) = 0$.

Now suppose $\dim_D(V) = n \in \mathbb{N}$ and that the theorem holds for dimensions $0, 1, \ldots, n-1$. Let $\{u_1, u_2, \ldots, u_{n-1}, u\}$ be a D-basis of V (which exists by Theorem IV.2.4) and let W be the $(n-1)$-dimensional D-subspace $W = \mathrm{span}\{u_1, u_2, \ldots, u_{n-1}\}$ (with $W = \{0\}$ if $n = 1$).

Lemma IX.1.11

Lemma IX.1.11. Let A be a simple module over a ring R. Consider A as a vector space over the division ring $D = \mathrm{Hom}_R(A, A)$. If V is a finite dimensional D-subspace of the D-vector space A and $a \in A \setminus V$, then there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$.

Proof. We give an induction proof on $n = \dim_D(V)$.

Let $n = 0$. Then $V = \{0\}$ and so $a \in A \setminus V$ implies $a \neq 0$. Since A is simple, then by Lemma IX.1.A, $A = Ra$. So there is some $r \in R$ such that $ra = a \neq 0$ and $rV = v\{0\} = \{0\}$, and the claim holds for $n = \dim_D(V) = 0$.

Now suppose $\dim_D(V) = n \in \mathbb{N}$ and that the theorem holds for dimensions $0, 1, \ldots, n-1$. Let $\{u_1, u_2, \ldots, u_{n-1}, u\}$ be a D-basis of V (which exists by Theorem IV.2.4) and let W be the $(n-1)$-dimensional D-subspace $W = \mathrm{span}\{u_1, u_2, \ldots, u_{n-1}\}$ (with $W = \{0\}$ if $n = 1$).

Lemma IX.1.11 (continued 1)

Proof (continued). Since $\{u_1, u_2, \ldots, u_{n-1}, u\}$ is a basis then it is linearly independent and so $W \cap Du = \{0\}$ (notice that Du itself is a vector space; it is the span of $\{u\}$). So $V = W \oplus Du$ by Theorem IV.1.5. The left annihilator $I = \mathcal{A}(W)$ in R of W is a left ideal o fR by Theorem IX.1.4. By Exercise IV.1.3(a), Iu is an R-submodule of A. Since $u \in A \setminus W$ and $\dim_D(W) = n - 1$ then by the *induction hypothesis* there is $r \in R$ such that $ru \neq 0$ and $rW = \{0\}$ (that is, $r \in I = \mathcal{A}(W)$). This implies $0 \neq ru \in Iu$ is a nonzero R-submodule of A then $A = Iu$. Notice that the induction hypothesis has given us that: for $u \in A$ we have that $u \notin W$ (where $\dim_D(W) = n - 1$) implies there is $r \in I = \mathcal{A}(W)$ such that $ru \neq 0$.

Lemma IX.1.11 (continued 1)

Proof (continued). Since $\{u_1, u_2, \ldots, u_{n-1}, u\}$ is a basis then it is linearly independent and so $W \cap Du = \{0\}$ (notice that Du itself is a vector space; it is the span of $\{u\}$). So $V = W \oplus Du$ by Theorem IV.1.5. The left annihilator $I = \mathcal{A}(W)$ in R of W is a left ideal o fR by Theorem IX.1.4. By Exercise IV.1.3(a), Iu is an R-submodule of A. Since $u \in A \setminus W$ and $\dim_D(W) = n - 1$ then by the *induction hypothesis* there is $r \in R$ such that $ru \neq 0$ and $rW = \{0\}$ (that is, $r \in I = \mathcal{A}(W)$). This implies $0 \neq ru \in Iu$ is a nonzero R-submodule of A then $A = Iu$. Notice that the induction hypothesis has given us that: for $u \in A$ we have that $u \notin W$ (where $\dim_D(W) = n - 1$) implies there is $r \in I = \mathcal{A}(W)$ such that $ru \neq 0$. The contrapositive of this is that:

For $v \in A$, if for all $r \in I = \mathcal{A}(W)$ we have $rv = 0$ then $v \in W$. (*)

Lemma IX.1.11 (continued 1)

Proof (continued). Since $\{u_1, u_2, \ldots, u_{n-1}, u\}$ is a basis then it is linearly independent and so $W \cap Du = \{0\}$ (notice that Du itself is a vector space; it is the span of $\{u\}$). So $V = W \oplus Du$ by Theorem IV.1.5. The left annihilator $I = \mathcal{A}(W)$ in R of W is a left ideal o fR by Theorem IX.1.4. By Exercise IV.1.3(a), Iu is an R-submodule of A. Since $u \in A \setminus W$ and $\dim_D(W) = n - 1$ then by the *induction hypothesis* there is $r \in R$ such that $ru \neq 0$ and $rW = \{0\}$ (that is, $r \in I = \mathcal{A}(W)$). This implies $0 \neq ru \in Iu$ is a nonzero R-submodule of A then $A = Iu$. Notice that the induction hypothesis has given us that: for $u \in A$ we have that $u \notin W$ (where $\dim_D(W) = n - 1$) implies there is $r \in I = \mathcal{A}(W)$ such that $ru \neq 0$. The contrapositive of this is that:

For $v \in A$, if for all $r \in I = \mathcal{A}(W)$ we have $rv = 0$ then $v \in W$. (*)

We must find $r \in R$ such that $ra \neq 0$ and $rV = \{0\}$. ASSUME no such r exists. Then define $\theta : A \to A$ as follows. For $ru \in Iu = A$ let $\theta(ru) = ra \in A$.

Lemma IX.1.11 (continued 1)

Proof (continued). Since $\{u_1, u_2, \ldots, u_{n-1}, u\}$ is a basis then it is linearly independent and so $W \cap Du = \{0\}$ (notice that Du itself is a vector space; it is the span of $\{u\}$). So $V = W \oplus Du$ by Theorem IV.1.5. The left annihilator $I = \mathcal{A}(W)$ in R of W is a left ideal o fR by Theorem IX.1.4. By Exercise IV.1.3(a), Iu is an R-submodule of A. Since $u \in A \setminus W$ and $\dim_D(W) = n - 1$ then by the *induction hypothesis* there is $r \in R$ such that $ru \neq 0$ and $rW = \{0\}$ (that is, $r \in I = \mathcal{A}(W)$). This implies $0 \neq ru \in Iu$ is a nonzero R-submodule of A then $A = Iu$. Notice that the induction hypothesis has given us that: for $u \in A$ we have that $u \notin W$ (where $\dim_D(W) = n - 1$) implies there is $r \in I = \mathcal{A}(W)$ such that $ru \neq 0$. The contrapositive of this is that:

$$\text{For } v \in A, \text{ if for all } r \in I = \mathcal{A}(W) \text{ we have } rv = 0 \text{ then } v \in W. \qquad (*)$$

We must find $r \in R$ such that $ra \neq 0$ and $rV = \{0\}$. ASSUME no such r exists. Then define $\theta : A \to A$ as follows. For $ru \in Iu = A$ let $\theta(ru) = ra \in A$.

Lemma IX.1.11 (continued 2)

Proof (continued). We claim that θ is well-defined (that is, if $r_1 u = r_2 u$ for $r_1, r_2 \in I = \mathcal{A}(W)$, then $(r_1 - r_2)u = 0$, whence $(r_1 - r_2)V = (r_1 - r_2)(W \oplus Du) = \{0\}$ (since elements of $W \oplus Du$ are sums of elements of W, which $r_1 - r_2$ annihilates, and multiples of u of the form $du = d(u)$ for $d \in D = \mathrm{Hom}_R(A, A)$ so that $(r_1 - r_2)du = (r_1 - r_2)d(u) = d((r_1 - r_2)u) = d(0) = 0$). By the assumption (that no r exists such that $ra \neq 0$ and $rV = \{0\}$; but here we have $(r_1 - r_2)V = \{0\}$) we must have $(r_1 - r_2)a = 0$. Therefore $r_1 a = r_2 a$ or $r_1 a = \theta(r_1 u) = \theta(r_2 u) = r_2 a$, and θ is well-defined. Let $a_1, a_2 \in A$. Since $A = Iu$ then there is $r_1, r_2 \in I$ such that $a_1 = r_1 u$ and $a_2 = r_2 u$.

Lemma IX.1.11 (continued 2)

Proof (continued). We claim that θ is well-defined (that is, if $r_1u = r_2u$ for $r_1, r_2 \in I = \mathcal{A}(W)$, then $(r_1 - r_2)u = 0$, whence $(r_1 - r_2)V = (r_1 - r_2)(W \oplus Du) = \{0\}$ (since elements of $W \oplus Du$ are sums of elements of W, which $r_1 - r_2$ annihilates, and multiples of u of the form $du = d(u)$ for $d \in D = \mathrm{Hom}_R(A, A)$ so that $(r_1 - r_2)du = (r_1 - r_2)d(u) = d((r_1 - r_2)u) = d(0) = 0$). By the assumption (that no r exists such that $ra \neq 0$ and $rV = \{0\}$; but here we have $(r_1 - r_2)V = \{0\}$) we must have $(r_1 - r_2)a = 0$. Therefore $r_1a = r_2a$ or $r_1a = \theta(r_1u) = \theta(r_2u) = r_2a$, and θ is well-defined. Let $a_1, a_2 \in A$. Since $A = Iu$ then there is $r_1, r_2 \in I$ such that $a_1 = r_1u$ and $a_2 = r_2u$. So

$$\theta(a_1+a_2) = \theta(r_1u+r_2u) = \theta((r_1+r_2)u) = (r_1+r_2)a = r_1a+r_2a = \theta(r_1u)+\theta(r_2$$

Also, for $r' \in R$ and $a \in A = Iu$ (so that $a = ru$ for some $r \in I$) we have

$$\theta(r'a) = \theta(r'(ru)) = \theta((r'r)u) = (r'r)a = r'(ra) = r'\theta(ru) = r'\theta(a).$$

Lemma IX.1.11 (continued 2)

Proof (continued). We claim that θ is well-defined (that is, if $r_1 u = r_2 u$ for $r_1, r_2 \in I = \mathcal{A}(W)$, then $(r_1 - r_2)u = 0$, whence $(r_1 - r_2)V = (r_1 - r_2)(W \oplus Du) = \{0\}$ (since elements of $W \oplus Du$ are sums of elements of W, which $r_1 - r_2$ annihilates, and multiples of u of the form $du = d(u)$ for $d \in D = \mathrm{Hom}_R(A, A)$ so that $(r_1 - r_2)du = (r_1 - r_2)d(u) = d((r_1 - r_2)u) = d(0) = 0$). By the assumption (that no r exists such that $ra \neq 0$ and $rV = \{0\}$; but here we have $(r_1 - r_2)V = \{0\}$) we must have $(r_1 - r_2)a = 0$. Therefore $r_1 a = r_2 a$ or $r_1 a = \theta(r_1 u) = \theta(r_2 u) = r_2 a$, and θ is well-defined. Let $a_1, a_2 \in A$. Since $A = Iu$ then there is $r_1, r_2 \in I$ such that $a_1 = r_1 u$ and $a_2 = r_2 u$. So

$$\theta(a_1+a_2) = \theta(r_1 u+r_2 u) = \theta((r_1+r_2)u) = (r_1+r_2)a = r_1 a+r_2 a = \theta(r_1 u)+\theta(r_2$$

Also, for $r' \in R$ and $a \in A = Iu$ (so that $a = ru$ for some $r \in I$) we have

$$\theta(r'a) = \theta(r'(ru)) = \theta((r'r)u) = (r'r)a = r'(ra) = r'\theta(ru) = r'\theta(a).$$

Lemma IX.1.11 (continued 3)

Proof (continued). Therefore θ is an R-module homomorphism mapping $A \to A$ (by Definition IV.1.2); that is, $\theta \in \mathrm{Hom}_R(A, A) = D$. Then for every $r \in I$,

$$0 = ra - ra = \theta(ru) - ra = r\theta(u) - ra = r(\theta(u) - a).$$

So by $(*)$, $\theta(u) - a = \theta u - a \in W$ and $a - \theta u \in W$. Notice that $\theta u = \theta(u) \in Du$ since $\theta \in D = \mathrm{Hom}_R(A, A)$. Consequently $a = (a - \theta u) + \theta u \in W \oplus Du = V$. But this is a CONTRADICTION to the fact that $a \in A \setminus V$. So the assumption that no such r exists is false, and hence there exists $r \in R$ such that $ra \neq 0$ and $rV = \{0\}$. That is, the result holds for $\dim_D(V) = n$ and so holds for all $n \in \mathbb{N} \cup \{0\}$ by induction. $\square$

Lemma IX.1.11 (continued 3)

Proof (continued). Therefore θ is an R-module homomorphism mapping $A \to A$ (by Definition IV.1.2); that is, $\theta \in \mathrm{Hom}_R(A, A) = D$. Then for every $r \in I$,

$$0 = ra - ra = \theta(ru) - ra = r\theta(u) - ra = r(\theta(u) - a).$$

So by $(*)$, $\theta(u) - a = \theta u - a \in W$ and $a - \theta u \in W$. Notice that $\theta u = \theta(u) \in Du$ since $\theta \in D = \mathrm{Hom}_R(A, A)$. Consequently $a = (a - \theta u) + \theta u \in W \oplus Du = V$. But this is a CONTRADICTION to the fact that $a \in A \setminus V$. So the assumption that no such r exists is false, and hence there exists $r \in R$ such that $ra \neq 0$ and $rV = \{0\}$. That is, the result holds for $\dim_D(V) = n$ and so holds for all $n \in \mathbb{N} \cup \{0\}$ by induction. □

Theorem IX.1.12. Jacobson Density Theorem

Theorem IX.1.12. Jacobson Density Theorem.
Let R be a primitive ring and A a faithful simple R-module. consider A as a vector space over the division ring $\hom_R(A, A) = D$. Then R is isomorphic to a dense ring of endomorphisms of the D-vector space A.

Proof. For each $r \in R$ the map $\alpha_r : A \to A$ given by $\alpha_r(A) = ra$ is a D-endomorphism of A (for $a_1, a_2 \in A$ we have $\alpha_r(a_1 + a_2) = r(a_1 + a_2) = ra_1 + ra_2 = \alpha_r(a_1) + \alpha_r(a_2)$ and for $a \in A$ and $\theta \in D = \mathrm{Hom}_R(A, A)$ we have

$$\begin{aligned} \alpha_r(\theta a) &= \alpha_r(\theta(a)) = r\theta(a) \\ &= \theta(ra) \text{ since } \theta \in \mathrm{Hom}_R(A, A) \\ &= \theta(\alpha_r(a)), \end{aligned}$$

so by Definition IV.1.2 α_r is a homomorphism). That is, $\alpha_r \in \mathrm{Hom}_D(A, A)$. Furthermore, for all $r, s \in R$ we have $\alpha_{r+s} = \alpha_r + \alpha_s$ and $\alpha_{rs} = \alpha_r \alpha_s$.

Theorem IX.1.12. Jacobson Density Theorem

Theorem IX.1.12. Jacobson Density Theorem.
Let R be a primitive ring and A a faithful simple R-module. consider A as a vector space over the division ring $\hom_R(A, A) = D$. Then R is isomorphic to a dense ring of endomorphisms of the D-vector space A.

Proof. For each $r \in R$ the map $\alpha_r : A \to A$ given by $\alpha_r(A) = ra$ is a D-endomorphism of A (for $a_1, a_2 \in A$ we have $\alpha_r(a_1 + a_2) = r(a_1 + a_2) = ra_1 + ra_2 = \alpha_r(a_1) + \alpha_r(a_2)$ and for $a \in A$ and $\theta \in D = \mathrm{Hom}_R(A, A)$ we have

$$\begin{aligned}\alpha_r(\theta a) &= \alpha_r(\theta(a)) = r\theta(a)\\ &= \theta(ra) \text{ since } \theta \in \mathrm{Hom}_R(A, A)\\ &= \theta(\alpha_r(a)),\end{aligned}$$

so by Definition IV.1.2 α_r is a homomorphism). That is, $\alpha_r \in \mathrm{Hom}_D(A, A)$. Furthermore, for all $r, s \in R$ we have $\alpha_{r+s} = \alpha_r + \alpha_s$ and $\alpha_{rs} = \alpha_r\alpha_s$.

Theorem IX.1.12. Jacobson Density Theorem (continued 1)

Proof (continued). Consequently, the map $\alpha : R \to \text{Hom}_D(A, A)$ defined by $\alpha(r) = \alpha_r$ is a homomorphism of rings. Since A is a faithful R-module (that is, $\mathcal{A}(A) = \{0\}$), $\alpha_r = 0 \in \text{Hom}_D(A, A)$ if an only if $r \in \mathcal{A}(A) = \{0\}$. So $\text{Ker}(\alpha) = \{0\}$ and α is a monomorphism (one to one; by Theorem I.2.3(i)). Whence R is isomorphic to the subring $\text{Im}(\alpha)$ of $\text{Hom}_D(A, A)$.

Now we show that $\text{Im}(\alpha)$ is a dense subring of $\text{Hom}_D(A, A)$. So given any D-linearly independent subset $U = \{u_1, U_2, \ldots, u_n\}$ of A and any subset $\{v_1, v_2, \ldots, v_n\}$ of A, we must find $\alpha_r \in \text{Im}(\alpha)$ such that $\alpha_r(u_i) = v_i$ for $i = 1, 2, \ldots, n$. Here we go.

Theorem IX.1.12. Jacobson Density Theorem (continued 1)

Proof (continued). Consequently, the map $\alpha : R \to \mathrm{Hom}_D(A, A)$ defined by $\alpha(r) = \alpha_r$ is a homomorphism of rings. Since A is a faithful R-module (that is, $\mathcal{A}(A) = \{0\}$), $\alpha_r = 0 \in \mathrm{Hom}_D(A, A)$ if an only if $r \in \mathcal{A}(A) = \{0\}$. So $\mathrm{Ker}(\alpha) = \{0\}$ and α is a monomorphism (one to one; by Theorem I.2.3(i)). Whence R is isomorphic to the subring $\mathrm{Im}(\alpha)$ of $\mathrm{Hom}_D(A, A)$.

Now we show that $\mathrm{Im}(\alpha)$ is a dense subring of $\mathrm{Hom}_D(A, A)$. So given any D-linearly independent subset $U = \{u_1, U_2, \ldots, u_n\}$ of A and any subset $\{v_1, v_2, \ldots, v_n\}$ of A, we must find $\alpha_r \in \mathrm{Im}(\alpha)$ such that $\alpha_r(u_i) = v_i$ for $i = 1, 2, \ldots, n$. Here we go. For each $i = 1, 2, \ldots, n$, let V_i be the D-subspace of A spanned by $\{u_1, u_2, \ldots, u_{i-1}, u_{i+1}, \ldots u_n\}$. Since U is D-linearly independent then $u_i \in V_i$. Consequently (since A is simple by Definition IX.1.5 of "primitive ring"), by Lemma IX.1.11 there exists $r_i \in R$ such that $r_i u_i \neq 0$ and $r_i V_i = \{0\}$.

Theorem IX.1.12. Jacobson Density Theorem (continued 1)

Proof (continued). Consequently, the map $\alpha : R \to \text{Hom}_D(A, A)$ defined by $\alpha(r) = \alpha_r$ is a homomorphism of rings. Since A is a faithful R-module (that is, $\mathcal{A}(A) = \{0\}$), $\alpha_r = 0 \in \text{Hom}_D(A, A)$ if an only if $r \in \mathcal{A}(A) = \{0\}$. So $\text{Ker}(\alpha) = \{0\}$ and α is a monomorphism (one to one; by Theorem I.2.3(i)). Whence R is isomorphic to the subring $\text{Im}(\alpha)$ of $\text{Hom}_D(A, A)$.

Now we show that $\text{Im}(\alpha)$ is a dense subring of $\text{Hom}_D(A, A)$. So given any D-linearly independent subset $U = \{u_1, U_2, \ldots, u_n\}$ of A and any subset $\{v_1, v_2, \ldots, v_n\}$ of A, we must find $\alpha_r \in \text{Im}(\alpha)$ such that $\alpha_r(u_i) = v_i$ for $i = 1, 2, \ldots, n$. Here we go. For each $i = 1, 2, \ldots, n$, let V_i be the D-subspace of A spanned by $\{u_1, u_2, \ldots, u_{i-1}, u_{i+1}, \ldots u_n\}$. Since U is D-linearly independent then $u_i \in V_i$. Consequently (since A is simple by Definition IX.1.5 of "primitive ring"), by Lemma IX.1.11 there exists $r_i \in R$ such that $r_i u_i \neq 0$ and $r_i V_i = \{0\}$.

Theorem IX.1.12. Jacobson Density Theorem (continued 2)

Proof (continued). Applying Lemma IX.1.11 to D-subspace $V = \{0\}$ of A and nonzero $r_i u_i \in A \setminus V$, there exists $s_i \in R$ such that $s_i r_i u_i \neq 0$ and $s_i 0 = 0$. Since $s_i r_i u_i \neq 0$, the R-submodule $R r_i u_i$ of A is nonzero. But A is simple (by the definition of "primitive ring" R), so it must be that $R r_i u_i = A$. Therefore there exists $t_i \in R$ such that $t_i r_i u_i = v_i$. Define $r = t_1 r_1 + t_2 r_2 + \cdots + t_n r_n \in R$. By definition of V_j, we have for $i \neq j$ that $u_i \in V_j$ and so for $i \neq j$ we also have $t_j r_j u_i \in t_j(r_j V_j) = t_j\{0\} = \{0\}$ (since $r_j V_j = \{0\}$ by the choice of r_j above). Consequently for each $i = 1, 2, \ldots, n$ we have

$$\alpha_r(u_i) = r u_i = (t_1 r_1 + t_2 r_2 + \cdots + t_n r_n) u_i = t_i r_i u_i = v_i.$$

So, by Definition IX.1.8, "dense ring of endomorphisms," $\mathrm{Im}(\alpha)$ is a dense ring of endomorphisms of the D-vector space A. Since R is isomorphic to $\mathrm{Im}(\alpha)$ (under isomorphism α), the claim follows. □

Theorem IX.1.12. Jacobson Density Theorem (continued 2)

Proof (continued). Applying Lemma IX.1.11 to D-subspace $V = \{0\}$ of A and nonzero $r_i u_i \in A \setminus V$, there exists $s_i \in R$ such that $s_i r_i u_i \neq 0$ and $s_i 0 = 0$. Since $s_i r_i u_i \neq 0$, the R-submodule $R r_i u_i$ of A is nonzero. But A is simple (by the definition of "primitive ring" R), so it must be that $R r_i u_i = A$. Therefore there exists $t_i \in R$ such that $t_i r_i u_i = v_i$. Define $r = t_1 r_1 + t_2 r_2 + \cdots + t_n r_n \in R$. By definition of V_j, we have for $i \neq j$ that $u_i \in V_j$ and so for $i \neq j$ we also have $t_j r_j u_i \in t_j(r_j V_j) = t_j\{0\} = \{0\}$ (since $r_j V_j = \{0\}$ by the choice of r_j above). Consequently for each $i = 1, 2, \ldots, n$ we have

$$\alpha_r(u_i) = r u_i = (t_1 r_1 + t_2 r_2 + \cdots + t_n r_n) u_i = t_i r_i u_i = v_i.$$

So, by Definition IX.1.8, "dense ring of endomorphisms," $\mathrm{Im}(\alpha)$ is a dense ring of endomorphisms of the D-vector space A. Since R is isomorphic to $\mathrm{Im}(\alpha)$ (under isomorphism α), the claim follows. □

Corollary IX.1.13

Corollary IX.1.13. If R is a primitive ring, then for some division ring D either R is isomorphic to the endomorphism ring of a finite dimensional vector space over D or for every $m \in \mathbb{N}$ there is subring R_m of R and an epimorphism of rings mapping $R_m \to \text{Hom}_D(V_m, V_m)$ where V_m is an n-dimensional vector space over D.

Proof. In the notation of the Jacobson Density Theorem (Theorem IX.1.12) with A as the faithful simple R-module and $D = \text{Hom}_R(A, A)$, we have $\alpha : R \to \text{Hom}_D(A, A)$ is a monomorphism such that $R \cong \text{Im}(\alpha)$ and $\text{Im}(\alpha)$ is dense in $\text{Hom}_D(A, A)$. If $\dim_D(A) = n$ is finite, then $\text{Im}(\alpha) = \text{Hom}_D(A, A)$ by Theorem IX.1.9 (this also gives that $\text{Im}(\alpha)$ is left Artinian). So the first conclusion holds.

Corollary IX.1.13

Corollary IX.1.13. If R is a primitive ring, then for some division ring D either R is isomorphic to the endomorphism ring of a finite dimensional vector space over D or for every $m \in \mathbb{N}$ there is subring R_m of R and an epimorphism of rings mapping $R_m \to \text{Hom}_D(V_m, V_m)$ where V_m is an n-dimensional vector space over D.

Proof. In the notation of the Jacobson Density Theorem (Theorem IX.1.12) with A as the faithful simple R-module and $D = \text{Hom}_R(A, A)$, we have $\alpha : R \to \text{Hom}_D(A, A)$ is a monomorphism such that $R \cong \text{Im}(\alpha)$ and $\text{Im}(\alpha)$ is dense in $\text{Hom}_D(A, A)$. If $\dim_D(A) = n$ is finite, then $\text{Im}(\alpha) = \text{Hom}_D(A, A)$ by Theorem IX.1.9 (this also gives that $\text{Im}(\alpha)$ is left Artinian). So the first conclusion holds.

If $\dim_D(A)$ is infinite and $\{u_1, u_2, \ldots\}$ is an infinite linearly independent set, then let V_m be the m-dimensional D-subspace of A spanned by $\{u_1, u_2, \ldots, u_m\}$. Define $R_n = \{r \in R \mid rV_m \subset V_m\}$.

Corollary IX.1.13

Corollary IX.1.13. If R is a primitive ring, then for some division ring D either R is isomorphic to the endomorphism ring of a finite dimensional vector space over D or for every $m \in \mathbb{N}$ there is subring R_m of R and an epimorphism of rings mapping $R_m \to \text{Hom}_D(V_m, V_m)$ where V_m is an n-dimensional vector space over D.

Proof. In the notation of the Jacobson Density Theorem (Theorem IX.1.12) with A as the faithful simple R-module and $D = \text{Hom}_R(A, A)$, we have $\alpha : R \to \text{Hom}_D(A, A)$ is a monomorphism such that $R \cong \text{Im}(\alpha)$ and $\text{Im}(\alpha)$ is dense in $\text{Hom}_D(A, A)$. If $\dim_D(A) = n$ is finite, then $\text{Im}(\alpha) = \text{Hom}_D(A, A)$ by Theorem IX.1.9 (this also gives that $\text{Im}(\alpha)$ is left Artinian). So the first conclusion holds.

If $\dim_D(A)$ is infinite and $\{u_1, u_2, \ldots\}$ is an infinite linearly independent set, then let V_m be the m-dimensional D-subspace of A spanned by $\{u_1, u_2, \ldots, u_m\}$. Define $R_n = \{r \in R \mid rV_m \subset V_m\}$.

Corollary IX.1.13 (continued)

Corollary IX.1.13. If R is a primitive ring, then for some division ring D either R is isomorphic to the endomorphism ring of a finite dimensional vector space over D or for every $m \in \mathbb{N}$ there is subring R_m of R and an epimorphism of rings mapping $R_m \to \mathrm{Hom}_D(V_m, V_m)$ where V_m is an n-dimensional vector space over D.

Proof (continued). If $r_1, r_2 \in R_m$ then $(r_1 + r_2)V_m = r_1 V_m + r_2 V_m \subset V_m$ since $r_1 V_m$ and $r_2 V_m$ are subset of V_m (and V_m is closed under addition), and $(r_1 r_1)V_m = r_1(r_2 V_m) \subset V_m$ since $r_2 V_m \subset V_m$ and $r_1 V_m \subset V_m$. So R_m is a subring of R. Define $\beta : R_m \to \mathrm{Hom}_D(V_m, V_m)$ as the restriction of α_r to V_m: $\beta(r) = \alpha_r|_{V_m}$. By Exercise IX.1.A, β is a well-defined ring epimorphism and the second claim holds. □

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings.
The following conditions on a left Artinian ring R are equivalent:

(i) R is simple;

(ii) R is primitive;

(iii) R is isomorphic to the endomorphism ring of a nonzero finite dimensional space V over a division ring D;

(iv) for some $b \in \mathbb{N}$, R is isomorphic to the ring of all $n \times n$ matrices over a division ring.

Proof. (i)⇒(ii). Let $I = \{r \in R \mid Rr = \{0\}\}$. Then I is the right annihilator of R (treating ring R as an R-module) and since R is a submodule of itself then I is an ideal of R by Theorem IX.1.4. Since R is hypothesized to be simple then either $I = R$ or $I = \{0\}$.

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings.
The following conditions on a left Artinian ring R are equivalent:

(i) R is simple;

(ii) R is primitive;

(iii) R is isomorphic to the endomorphism ring of a nonzero finite dimensional space V over a division ring D;

(iv) for some $b \in \mathbb{N}$, R is isomorphic to the ring of all $n \times n$ matrices over a division ring.

Proof. (i)$\Rightarrow$(ii). Let $I = \{r \in R \mid Rr = \{0\}\}$. Then I is the right annihilator of R (treating ring R as an R-module) and since R is a submodule of itself then I is an ideal of R by Theorem IX.1.4. Since R is hypothesized to be simple then either $I = R$ or $I = \{0\}$.

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings (continued)

Proof (continued). Since R is a simple ring then (by Definition IX.1.1) $R^2 \neq \{0\}$ and we cannot have $I = R$ (or else $Rr = \{0\}$ for all $r \in R$; that is, $R^2 = \{0\}$). Hence $I = \{0\}$. Since R is left Artinian by hypothesis, the set of all nonzero left ideals of R contains a minimal left ideal J by Theorem VIII.1.4. Now J has no proper R-submodules (notice that an R-submodule of J would be a left ideal of R). We claim that annihilator $\mathcal{A}(J) = \{0\}$ in R.

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings (continued)

Proof (continued). Since R is a simple ring then (by Definition IX.1.1) $R^2 \neq \{0\}$ and we cannot have $I = R$ (or else $Rr = \{0\}$ for all $r \in R$; that is, $R^2 = \{0\}$). Hence $I = \{0\}$. Since R is left Artinian by hypothesis, the set of all nonzero left ideals of R contains a minimal left ideal J by Theorem VIII.1.4. Now J has no proper R-submodules (notice that an R-submodule of J would be a left ideal of R). We claim that annihilator $\mathcal{A}(J) = \{0\}$ in R. ASSUME $\mathcal{A}(J) \neq \{0\}$. By Theorem IX.1.4, the left annihilator $\mathcal{A}(J)$ is a left ideal of R. Since R is simple then we must have $\mathcal{A}(J) = R$. Then $Ru = 0$ for every nonzero $u \in J$. Consequently, each such nonzero u is in $I = \{0\}$, a CONTRADICTION. Therefore $\mathcal{A}(J) = \{0\}$. Also $RJ \neq \{0\}$ (or else $A(J) = R \neq \{0\}$). Thus J is a faithful simple R-module and so by Definition IX.1.5, "primitive ring," R is primitive.

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings (continued)

Proof (continued). Since R is a simple ring then (by Definition IX.1.1) $R^2 \neq \{0\}$ and we cannot have $I = R$ (or else $Rr = \{0\}$ for all $r \in R$; that is, $R^2 = \{0\}$). Hence $I = \{0\}$. Since R is left Artinian by hypothesis, the set of all nonzero left ideals of R contains a minimal left ideal J by Theorem VIII.1.4. Now J has no proper R-submodules (notice that an R-submodule of J would be a left ideal of R). We claim that annihilator $\mathcal{A}(J) = \{0\}$ in R. ASSUME $\mathcal{A}(J) \neq \{0\}$. By Theorem IX.1.4, the left annihilator $\mathcal{A}(J)$ is a left ideal of R. Since R is simple then we must have $\mathcal{A}(J) = R$. Then $Ru = 0$ for every nonzero $u \in J$. Consequently, each such nonzero u is in $I = \{0\}$, a CONTRADICTION. Therefore $\mathcal{A}(J) = \{0\}$. Also $RJ \neq \{0\}$ (or else $A(J) = R \neq \{0\}$). Thus J is a faithful simple R-module and so by Definition IX.1.5, "primitive ring," R is primitive.

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings (continued)

Proof (continued). (ii)⇒(iii). Since R is primitive by hypothesis, then by the Jacobson Density Theorem (Theorem IX.1.12) R is isomorphic to a dense ring T of endomorphisms of a vector space V over a division ring D. Since R is left Artinian by hypothesis then $R \cong T = \mathrm{Hom}_D(V, V)$ and $\dim_D(V)$ is finite, as claimed.

(iii)⇔(iv). By Theorem VII.1.4, $\mathrm{Hom}_D(V, V)$ is isomorphic to a ring of $n \times n$ matrices with entries from a division ring.

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings (continued)

Proof (continued). (ii)$\Rightarrow$(iii). Since R is primitive by hypothesis, then by the Jacobson Density Theorem (Theorem IX.1.12) R is isomorphic to a dense ring T of endomorphisms of a vector space V over a division ring D. Since R is left Artinian by hypothesis then $R \cong T = \text{Hom}_D(V, V)$ and $\dim_D(V)$ is finite, as claimed.

(iii)$\Leftrightarrow$(iv). By Theorem VII.1.4, $\text{Hom}_D(V, V)$ is isomorphic to a ring of $n \times n$ matrices with entries from a division ring.

(iv)$\Rightarrow$(i). Exercise III.2.9(a) implies R has no proper ideals and so, by Definition IX.1.1, R is simple. □

Theorem IX.1.14. The Wedderburn-Artin Theorem for Simple Artinian Rings (continued)

Proof (continued). (ii)⇒(iii). Since R is primitive by hypothesis, then by the Jacobson Density Theorem (Theorem IX.1.12) R is isomorphic to a dense ring T of endomorphisms of a vector space V over a division ring D. Since R is left Artinian by hypothesis then $R \cong T = \mathrm{Hom}_D(V, V)$ and $\dim_D(V)$ is finite, as claimed.

(iii)⇔(iv). By Theorem VII.1.4, $\mathrm{Hom}_D(V, V)$ is isomorphic to a ring of $n \times n$ matrices with entries from a division ring.

(iv)⇒(i). Exercise III.2.9(a) implies R has no proper ideals and so, by Definition IX.1.1, R is simple. □

Lemma IX.1.15

Lemma IX.1.15. Let V be a finite dimensional vector space over a division ring D. If A and B are simple faithful modules over the endomorphism ring $R = \mathrm{Hom}_D(V, V)$, then A and B are isomorphic R-modules.

Proof. Since V is finite dimensional (say $\dim_D(V) = n$), by Theorem VII.1.4 $R = \mathrm{Hom}_D(V, V)$ is isomorphic to a ring of $n \times n$ matrices over a division ring. By Corollary VIII.1.12, R is Artinian (and so satisfies the descending chain condition). Then by Theorem VIII.1.4, R contains a (nonzero) minimal left ideal I.

Lemma IX.1.15

Lemma IX.1.15. Let V be a finite dimensional vector space over a division ring D. If A and B are simple faithful modules over the endomorphism ring $R = \mathrm{Hom}_D(V, V)$, then A and B are isomorphic R-modules.

Proof. Since V is finite dimensional (say $\dim_D(V) = n$), by Theorem VII.1.4 $R = \mathrm{Hom}_D(V, V)$ is isomorphic to a ring of $n \times n$ matrices over a division ring. By Corollary VIII.1.12, R is Artinian (and so satisfies the descending chain condition). Then by Theorem VIII.1.4, R contains a (nonzero) minimal left ideal I. Since A is faithful then (by Definition IX.1.5) the annihilator $\mathcal{A}(A) = \{0\}$. So there exists $a \in A$ such that $Ia \neq \{0\}$. By Exercise IV.1.3, Ia is a nonzero submodule of A. Since A is simple, then $Ia = A$.

Lemma IX.1.15

Lemma IX.1.15. Let V be a finite dimensional vector space over a division ring D. If A and B are simple faithful modules over the endomorphism ring $R = \mathrm{Hom}_D(V, V)$, then A and B are isomorphic R-modules.

Proof. Since V is finite dimensional (say $\dim_D(V) = n$), by Theorem VII.1.4 $R = \mathrm{Hom}_D(V, V)$ is isomorphic to a ring of $n \times n$ matrices over a division ring. By Corollary VIII.1.12, R is Artinian (and so satisfies the descending chain condition). Then by Theorem VIII.1.4, R contains a (nonzero) minimal left ideal I. Since A is faithful then (by Definition IX.1.5) the annihilator $\mathcal{A}(A) = \{0\}$. So there exists $a \in A$ such that $Ia \neq \{0\}$. By Exercise IV.1.3, Ia is a nonzero submodule of A. Since A is simple, then $Ia = A$. Define $\theta : I \to Ia = A$ as $\theta(i) = ia$. Then θ is a nonzero R-module epimorphism; that is, $\theta \in \mathrm{Hom}_R(A, A)$. By Lemma IX.1.10, θ is a monomorphism and epimorphism, and so is an isomorphism. That is, $A \cong I$. Similarly, $B \cong I$ and so $A \cong B$. □

Lemma IX.1.15

Lemma IX.1.15. Let V be a finite dimensional vector space over a division ring D. If A and B are simple faithful modules over the endomorphism ring $R = \text{Hom}_D(V, V)$, then A and B are isomorphic R-modules.

Proof. Since V is finite dimensional (say $\dim_D(V) = n$), by Theorem VII.1.4 $R = \text{Hom}_D(V, V)$ is isomorphic to a ring of $n \times n$ matrices over a division ring. By Corollary VIII.1.12, R is Artinian (and so satisfies the descending chain condition). Then by Theorem VIII.1.4, R contains a (nonzero) minimal left ideal I. Since A is faithful then (by Definition IX.1.5) the annihilator $\mathcal{A}(A) = \{0\}$. So there exists $a \in A$ such that $Ia \neq \{0\}$. By Exercise IV.1.3, Ia is a nonzero submodule of A. Since A is simple, then $Ia = A$. Define $\theta : I \to Ia = A$ as $\theta(i) = ia$. Then θ is a nonzero R-module epimorphism; that is, $\theta \in \text{Hom}_R(A, A)$. By Lemma IX.1.10, θ is a monomorphism and epimorphism, and so is an isomorphism. That is, $A \cong I$. Similarly, $B \cong I$ and so $A \cong B$. □

Lemma IX.1.16

Lemma IX.1.16. Let V be a nonzero vector space over a division ring D and let R be the endomorphism ring $\text{Hom}_D(V, V)$. If $g : V \to V$ is a homomorphism of additive groups such that $gr = rg$ for all $r \in R$, then there exists $d \in D$ such that $g(v) = dv$ for all $v \in V$.

Proof. Let u be a nonzero element of V. We claim that u and $g(u)$ are linearly independent over D. If $\dim_D(V) = 1$ then this is trivial, so we now consider the case $\dim_D(V) \geq 2$.

Lemma IX.1.16

Lemma IX.1.16. Let V be a nonzero vector space over a division ring D and let R be the endomorphism ring $\text{Hom}_D(V, V)$. If $g : V \to V$ is a homomorphism of additive groups such that $gr = rg$ for all $r \in R$, then there exists $d \in D$ such that $g(v) = dv$ for all $v \in V$.

Proof. Let u be a nonzero element of V. We claim that u and $g(u)$ are linearly independent over D. If $\dim_D(V) = 1$ then this is trivial, so we now consider the case $\dim_D(V) \geq 2$. ASSUME $\{i, g(u)\}$ is linearly independent. Since R is dense in itself by Lemma IX.1.C, then there is $r \in R$ such that $r(u) = ru = 0$ and $r(g(u)) = rg(u) \neq 0$. But by hypothesis $f(g(u)) = rg(u) = gr(u) = g(r(u)) = g(0) = 0$, a CONTRADICTION to the fact that $r(g(u)) \neq 0$. So the assumption is false and $\{u, g(u)\}$ is linearly independent.

Lemma IX.1.16

Lemma IX.1.16. Let V be a nonzero vector space over a division ring D and let R be the endomorphism ring $\mathrm{Hom}_D(V, V)$. If $g : V \to V$ is a homomorphism of additive groups such that $gr = rg$ for all $r \in R$, then there exists $d \in D$ such that $g(v) = dv$ for all $v \in V$.

Proof. Let u be a nonzero element of V. We claim that u and $g(u)$ are linearly independent over D. If $\dim_D(V) = 1$ then this is trivial, so we now consider the case $\dim_D(V) \geq 2$. ASSUME $\{i, g(u)\}$ is linearly independent. Since R is dense in itself by Lemma IX.1.C, then there is $r \in R$ such that $r(u) = ru = 0$ and $r(g(u)) = rg(u) \neq 0$. But by hypothesis $f(g(u)) = rg(u) = gr(u) = g(r(u)) = g(0) = 0$, a CONTRADICTION to the fact that $r(g(u)) \neq 0$. So the assumption is false and $\{u, g(u)\}$ is linearly independent.

Lemma IX.1.16 (continued)

Lemma IX.1.16. Let V be a nonzero vector space over a division ring D and let R be the endomorphism ring $\text{Hom}_D(V, V)$. If $g : V \to V$ is a homomorphism of additive groups such that $gr = rg$ for all $r \in R$, then there exists $d \in D$ such that $g(v) = dv$ for all $v \in V$.

Proof (continued). Therefore for some $d \in D$, $g(u) = du$. If $v \in V$ then there exists $s \in R$ such that $s(u) = su = v$ because R is dense in itself. Consequently, since $s \in R = \text{Hom}_D(V, V)$, then

$$g(v) = g(s(u)) = gs(u) = sg(u) = s(du) = ds(u) = dv,$$

and since v is arbitrary, the claim holds. □

Proposition IX.1.17

Proposition IX.1.17. Let V_1 and V_2 be vector spaces of finite dimension n over the division rings D_1 and D_2, respectively.

(i) If there is an isomorphism of rings $\mathrm{Hom}_{D_1}(V_1, V_2) \cong \mathrm{Hom}_{D_2}(V_2, V_2)$, then $\dim_{D_1}(V_1) = \dim_{D_2}(V_2)$ and D_1 is isomorphic to D_2.

(ii) If there is an isomorphism of rings $\mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2)$, then $n_1 = n_2$ and D_1 is isomorphic to D_2.

Proof. (i) It is argued in the example after Definition IX.1.5 that each V_i is a faithful $\mathrm{Hom}_{D_i}(V_i, V_i)$-module for $i = 1, 2$. Let $R = \mathrm{Hom}_{D_1}(V_1, V_1)$ and let σ be the hypothesized isomorphism, $\sigma : r = \mathrm{Hom}_{D_1}(V_1, V_1) \to \mathrm{Hom}_{D_2}(V_2, V_2)$. So V_2 is a faithful simple R-module (or $\mathrm{Hom}_{D_1}(V_1, V_1)$-module) by pullback along σ; that is,

$$rv - \sigma(r)v \text{ for } r \in R, v \in V_2. \qquad (*)$$

By Lemma IX.1.15 (with $A = V_1$ and $B = V_2$) there is an R-module isomorphism $\varphi : V_1 \to V_2$.

Proposition IX.1.17

Proposition IX.1.17. Let V_1 and V_2 be vector spaces of finite dimension n over the division rings D_1 and D_2, respectively.

(i) If there is an isomorphism of rings $\mathrm{Hom}_{D_1}(V_1, V_2) \cong \mathrm{Hom}_{D_2}(V_2, V_2)$, then $\dim_{D_1}(V_1) = \dim_{D_2}(V_2)$ and D_1 is isomorphic to D_2.

(ii) If there is an isomorphism of rings $\mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2)$, then $n_1 = n_2$ and D_1 is isomorphic to D_2.

Proof. **(i)** It is argued in the example after Definition IX.1.5 that each V_i is a faithful $\mathrm{Hom}_{D_i}(V_i, V_i)$-module for $i = 1, 2$. Let $R = \mathrm{Hom}_{D_1}(V_1, V_1)$ and let σ be the hypothesized isomorphism, $\sigma : r = \mathrm{Hom}_{D_1}(V_1, V_1) \to \mathrm{Hom}_{D_2}(V_2, V_2)$. So V_2 is a faithful simple R-module (or $\mathrm{Hom}_{D_1}(V_1, V_1)$-module) by pullback along σ; that is,

$$rv - \sigma(r)v \text{ for } r \in R, v \in V_2. \qquad (*)$$

By Lemma IX.1.15 (with $A = V_1$ and $B = V_2$) there is an R-module isomorphism $\varphi : V_1 \to V_2$.

Proposition IX.1.17 (continued 1)

Proof (continued). For each $v \in V_1$ and $f \in R$, $\varphi(f(v)) = f\varphi(v) = \sigma(f)[\varphi(v)]$ by $(*)$. With $x \in V_2$ and $v = \varphi^{-1}(w)$ we then have $\varphi(f(\varphi^{-1}(w))) = \sigma(f)v$ for each $w \in V_2$ and $f \in R$. That is, $\varphi f \varphi^{-1} = \sigma(f)$ and this is a homomorphism (not necessarily an isomorphism since $f \in \mathrm{Hom}_{D_1}(V_1, V_1)$ is a homomorphism) of additive groups $V_2 \to V_2$. For each $d \in D_i$, let $\alpha_d : V_i \to V_i$ be the homomorphism of additive groups defined by the mapping $x \mapsto dx$ (for $i = 1, 2$). Now $\alpha_d = 0$ if and only if $d = 0$ (since $dx = 0$ for $d \neq 0$ implies $d^{-1}dx = d^{-1}0$ or $x = 0$ since d is in a division ring). For $f \in R = \mathrm{Hom}_{D_1}(V_1, V_1)$ and $d \in D_1$, we have for $x \in V_1$ that $f\alpha_d(x) = fdx = f(dx) = df(x) = \alpha_d f(x)$, so $f\alpha_d = \alpha_d f$.

Proposition IX.1.17 (continued 1)

Proof (continued). For each $v \in V_1$ and $f \in R$, $\varphi(f(v)) = f\varphi(v) = \sigma(f)[\varphi(v)]$ by $(*)$. With $x \in V_2$ and $v = \varphi^{-1}(w)$ we then have $\varphi(f(\varphi^{-1}(w))) = \sigma(f)v$ for each $w \in V_2$ and $f \in R$. That is, $\varphi f \varphi^{-1} = \sigma(f)$ and this is a homomorphism (not necessarily an isomorphism since $f \in \mathrm{Hom}_{D_1}(V_1, V_1)$ is a homomorphism) of additive groups $V_2 \to V_2$. For each $d \in D_i$, let $\alpha_d : V_i \to V_i$ be the homomorphism of additive groups defined by the mapping $x \mapsto dx$ (for $i = 1, 2$). Now $\alpha_d = 0$ if and only if $d = 0$ (since $dx = 0$ for $d \neq 0$ implies $d^{-1}dx = d^{-1}0$ or $x = 0$ since d is in a division ring). For $f \in R = \mathrm{Hom}_{D_1}(V_1, V_1)$ and $d \in D_1$, we have for $x \in V_1$ that $f\alpha_d(x) = fdx = f(dx) = df(x) = \alpha_d f(x)$, so $f\alpha_d = \alpha_d f$. Consequently,

$$\begin{aligned}(\varphi\alpha_d\varphi^{-1})(\sigma f) &= \varphi\alpha_d\varphi^{-1}(\varphi f\varphi^{-1}) \text{ since } \varphi f\varphi^{-1} = \sigma(f) \\ &= \varphi\alpha_d f\varphi^{-1} = \varphi f\alpha_d\varphi^{-1} \text{ since } f\alpha_d = \alpha_d f \\ &= \varphi f\varphi^{-1}\varphi\alpha_d\varphi^{-1} = (\sigma f)(\varphi\alpha_d\varphi^{-1}) \text{ since } \varphi f\varphi^{-1} = \sigma f.\end{aligned}$$

Proposition IX.1.17 (continued 1)

Proof (continued). For each $v \in V_1$ and $f \in R$, $\varphi(f(v)) = f\varphi(v) = \sigma(f)[\varphi(v)]$ by $(*)$. With $x \in V_2$ and $v = \varphi^{-1}(w)$ we then have $\varphi(f(\varphi^{-1}(w))) = \sigma(f)v$ for each $w \in V_2$ and $f \in R$. That is, $\varphi f \varphi^{-1} = \sigma(f)$ and this is a homomorphism (not necessarily an isomorphism since $f \in \mathrm{Hom}_{D_1}(V_1, V_1)$ is a homomorphism) of additive groups $V_2 \to V_2$. For each $d \in D_i$, let $\alpha_d : V_i \to V_i$ be the homomorphism of additive groups defined by the mapping $x \mapsto dx$ (for $i = 1, 2$). Now $\alpha_d = 0$ if and only if $d = 0$ (since $dx = 0$ for $d \neq 0$ implies $d^{-1}dx = d^{-1}0$ or $x = 0$ since d is in a division ring). For $f \in R = \mathrm{Hom}_{D_1}(V_1, V_1)$ and $d \in D_1$, we have for $x \in V_1$ that $f\alpha_d(x) = fdx = f(dx) = df(x) = \alpha_d f(x)$, so $f\alpha_d = \alpha_d f$. Consequently,

$$\begin{aligned}(\varphi\alpha_d\varphi^{-1})(\sigma f) &= \varphi\alpha_d\varphi^{-1}(\varphi f \varphi^{-1}) \text{ since } \varphi f \varphi^{-1} = \sigma(f)\\ &= \varphi\alpha_d f \varphi^{-1} = \varphi f \alpha_d \varphi^{-1} \text{ since } f\alpha_d = \alpha_d f\\ &= \varphi f \varphi^{-1}\varphi\alpha_d\varphi^{-1} = (\sigma f)(\varphi\alpha_d\varphi^{-1}) \text{ since } \varphi f \varphi^{-1} = \sigma f.\end{aligned}$$

Proposition IX.1.17 (continued 2)

Proof (continued). Now $g = \varphi\alpha_d\varphi^{-1} : V_2 \to V_2$ is a homomorphism and this last equation shows that $g(\sigma f) = \sigma f)g$ for all φf for every $\sigma f \in \mathrm{Hom}_{D_2}(V_2, V_2)$ (since σ is surjective [onto; it is an isomorphism], σf for $f \in \mathrm{Hom}_{D_1}(V_1, V_1)$ includes all elements of $\mathrm{Hom}_{D_2}(V)2, V_2))$. So by Lemma IX.1.16 (with $V = V_2$) implies that there exists $d^* \in D_2$ such that $g = \varphi\alpha_d\varphi^{-1} = \alpha_{d^*}$. Let $\tau : D_1 \to D_2$ be the map given by $\tau(d) = d^*$. Then for every $d \in D_1$, $g = \varphi\alpha_d\varphi^{-1} = \alpha_{d^*} = \alpha_{\tau(d)}$. We now show that $\tau : D_1 \to D_2$ is an isomorphism. If $d, d' \in D_1$ then $\tau(d + d') = (d + d')^*$ where $\varphi\alpha_{d+d'}\varphi^{-1} = \alpha_{(d+d')^*}$.

Proposition IX.1.17 (continued 2)

Proof (continued). Now $g = \varphi\alpha_d\varphi^{-1} : V_2 \to V_2$ is a homomorphism and this last equation shows that $g(\sigma f) = \sigma f)g$ for all φf for every $\sigma f \in \mathrm{Hom}_{D_2}(V_2, V_2)$ (since σ is surjective [onto; it is an isomorphism], σf for $f \in \mathrm{Hom}_{D_1}(V_1, V_1)$ includes all elements of $\mathrm{Hom}_{D_2}(V)2, V_2))$. So by Lemma IX.1.16 (with $V = V_2$) implies that there exists $d^* \in D_2$ such that $g = \varphi\alpha_d\varphi^{-1} = \alpha_{d^*}$. Let $\tau : D_1 \to D_2$ be the map given by $\tau(d) = d^*$. Then for every $d \in D_1$, $g = \varphi\alpha_d\varphi^{-1} = \alpha_{d^*} = \alpha_{\tau(d)}$. We now show that $\tau : D_1 \to D_2$ is an isomorphism. If $d, d' \in D_1$ then $\tau(d + d') = (d + d')^*$ where $\varphi\alpha_{d+d'}\varphi^{-1} = \alpha_{(d+d')^*}$. As shown in the proof of Theorem IX.1.12, we have $\alpha_{d+d'} = \alpha_d + \alpha_{d'}$ and so

$$\varphi\alpha_{d+d'}\varphi^{-1} = \varphi(\alpha_d + \alpha_{d'})\varphi^{-1} = \varphi\alpha_d\varphi^{-1} + \varphi\alpha_{d'}\varphi^{-1}$$

$$= \alpha_{d^*} + \alpha_{(d')^*} = \alpha_{(d+d')^*},$$

so that $\tau(d + d') = (d + d')^* = d^* + (d')^*$.

Proposition IX.1.17 (continued 2)

Proof (continued). Now $g = \varphi\alpha_d\varphi^{-1} : V_2 \to V_2$ is a homomorphism and this last equation shows that $g(\sigma f) = \sigma f)g$ for all φf for every $\sigma f \in \mathrm{Hom}_{D_2}(V_2, V_2)$ (since σ is surjective [onto; it is an isomorphism], σf for $f \in \mathrm{Hom}_{D_1}(V_1, V_1)$ includes all elements of $\mathrm{Hom}_{D_2}(V)2, V_2)$). So by Lemma IX.1.16 (with $V = V_2$) implies that there exists $d^* \in D_2$ such that $g = \varphi\alpha_d\varphi^{-1} = \alpha_{d^*}$. Let $\tau : D_1 \to D_2$ be the map given by $\tau(d) = d^*$. Then for every $d \in D_1$, $g = \varphi\alpha_d\varphi^{-1} = \alpha_{d^*} = \alpha_{\tau(d)}$. We now show that $\tau : D_1 \to D_2$ is an isomorphism. If $d, d' \in D_1$ then $\tau(d + d') = (d + d')^*$ where $\varphi\alpha_{d+d'}\varphi^{-1} = \alpha_{(d+d')^*}$. As shown in the proof of Theorem IX.1.12, we have $\alpha_{d+d'} = \alpha_d + \alpha_{d'}$ and so

$$\varphi\alpha_{d+d'}\varphi^{-1} = \varphi(\alpha_d + \alpha_{d'})\varphi^{-1} = \varphi\alpha_d\varphi^{-1} + \varphi\alpha_{d'}\varphi^{-1}$$

$$= \alpha_{d^*} + \alpha_{(d')^*} = \alpha_{(d+d')^*},$$

so that $\tau(d + d') = (d + d')^* = d^* + (d')^*$.

Proposition IX.1.17 (continued 3)

Proof (continued). Similarly, as shown in the proof of Theorem IX.1.12, we have $\alpha_{dd'} = \alpha_d \alpha_{d'}$ and so

$$\alpha_{(dd')^*} = \varphi \alpha_{dd'} \varphi^{-1} = \varphi \alpha_d \alpha_{d'} \varphi^{-1} = (\varphi \alpha_d \varphi^{-1})(\varphi \alpha_{d'} \varphi^{-1}) = \alpha_{d^*} \alpha_{(d')^*}$$

so that $\tau(dd') = \tau(d)\tau(d')$. So τ is a ring homomorphism (by Definition III.1.7). Now suppose $d \neq d'$. then there is nonzero $v \in V_1$ such that $dv_1 \neq d'v_1$ (or else $dv_1 = d'v_1$ for all $v_1 \in V_1$ and so $(d-d')v_1 = 0$ for all $v_1 \in V_1$; if $d - d' \neq 0 \in D_2$ then $(d-d')^{-1}$ exists since D_2 is a division ring and so $(d-d')^{-1}(d-d')v_1 = (d-d')^{-1}0$ or $v_1 = 0$, a contradiction to the choice of v_1). So $\alpha_d \neq \alpha_{d'}$ because $\alpha_d v_1 = dv_1 \neq d'v_1 = \alpha_{d'} v_1$.

Proposition IX.1.17 (continued 3)

Proof (continued). Similarly, as shown in the proof of Theorem IX.1.12, we have $\alpha_{dd'} = \alpha_d \alpha_{d'}$ and so

$$\alpha_{(dd')^*} = \varphi \alpha_{dd'} \varphi^{-1} = \varphi \alpha_d \alpha_{d'} \varphi^{-1} = (\varphi \alpha_d \varphi^{-1})(\varphi \alpha_{d'} \varphi^{-1}) = \alpha_{d^*} \alpha_{(d')^*}$$

so that $\tau(dd') = \tau(d)\tau(d')$. So τ is a ring homomorphism (by Definition III.1.7). Now suppose $d \neq d'$. then there is nonzero $v \in V_1$ such that $dv_1 \neq d'v_1$ (or else $dv_1 = d'v_1$ for all $v_1 \in V_1$ and so $(d - d')v_1 = 0$ for all $v_1 \in V_1$; if $d - d' \neq 0 \in D_2$ then $(d - d')^{-1}$ exists since D_2 is a division ring and so $(d - d')^{-1}(d - d')v_1 = (d - d')^{-1}0$ or $v_1 = 0$, a contradiction to the choice of v_1). So $\alpha_d \neq \alpha_{d'}$ because $\alpha_d v_1 = dv_1 \neq d'v_1 = \alpha_{d'} v_1$.

Proposition IX.1.17 (continued 4)

Proof (continued). Now $\varphi : V_1 \to V_2$ and $\varphi^{-1} : V_2 \to V_1$ are isomorphisms (and so are surjective/onto and injective/one to one) so for some $v_2 \in V_2$ we have $\varphi^{-1} v_2 = v_1$ and

$$\begin{aligned} \alpha_{\tau(d)} v_2 &= \varphi \alpha_d \varphi^{-1} v_2 = \varphi \alpha_d v_1 \\ &\neq \varphi \alpha_{d'} v_1 \text{ since } \varphi \text{ is one to one} \\ &= \varphi \alpha_{d'} \varphi^{-1} v_2 = \alpha_{\tau(d')} v_2, \end{aligned}$$

so $\alpha_{\tau(d)} \neq \alpha_{\tau(d')}$, or $\alpha_{d^*} \neq \alpha_{(d')^*}$. So $\alpha_{d^*} = \varphi \alpha_d \varphi^{-1} \neq \varphi \alpha_{d'} \varphi^{-1} = \alpha_{(d')^*}$. Since both α_{d^*} and $\alpha_{(d')^*}$ also map $V_2 \to V_2$, this means for some $v \in V_2$ we have $\alpha_{d^*}(v) \neq \alpha_{(d')^*}(v)$ or $d^* v \neq (d')^* v$. *If* $d^* = (d')^*$ then $d^* v = (d')^* v$ and so we must have $d^* \neq (d')^*$; that is, $\tau(d) \neq \tau(d')$. Hence τ is a monomorphism (one to one and onto homomorphism).

Proposition IX.1.17 (continued 4)

Proof (continued). Now $\varphi : V_1 \to V_2$ and $\varphi^{-1} : V_2 \to V_1$ are isomorphisms (and so are surjective/onto and injective/one to one) so for some $v_2 \in V_2$ we have $\varphi^{-1} v_2 = v_1$ and

$$\begin{aligned} \alpha_{\tau(d)} v_2 &= \varphi \alpha_d \varphi^{-1} v_2 = \varphi \alpha_d v_1 \\ &\neq \varphi \alpha_{d'} v_1 \text{ since } \varphi \text{ is one to one} \\ &= \varphi \alpha_{d'} \varphi^{-1} v_2 = \alpha_{\tau(d')} v_2, \end{aligned}$$

so $\alpha_{\tau(d)} \neq \alpha_{\tau(d')}$, or $\alpha_{d^*} \neq \alpha_{(d')^*}$. So $\alpha_{d^*} = \varphi \alpha_d \varphi^{-1} \neq \varphi \alpha_{d'} \varphi^{-1} = \alpha_{(d')^*}$. Since both α_{d^*} and $\alpha_{(d')^*}$ also map $V_2 \to V_2$, this means for some $v \in V_2$ we have $\alpha_{d^*}(v) \neq \alpha_{(d')^*}(v)$ or $d^* v \neq (d')^* v$. *If* $d^* = (d')^*$ then $d^* v = (d')^* v$ and so we must have $d^* \neq (d')^*$; that is, $\tau(d) \neq \tau(d')$. Hence τ is a monomorphism (one to one and onto homomorphism).

Proposition IX.1.17 (continued 5)

Proof (continued). Reversing the roles of D_1 and D_2 in the previous argument (and replacing φ and σ with φ^{-1} and σ^{-1}, respectively) yields that for every $d_2 \in D_2$ there exists $d_1 \in D_1$ such that $\varphi^{-1}\alpha_{d_2}\varphi = \alpha_{d_1} : V_1 \to V_1$, whence $\alpha_{d_2} = \varphi\alpha_{d_1}\varphi^{-1} = \alpha_{\tau(d_1)}$. So $\tau(d_1) = d_2$ and τ is surjective/onto. Hence $\tau : D_1 \to D_2$ is an isomorphism and so D_1 is isomorphic to D_2, as claimed.

Furthermore, for every $d \in D_1$ and $v \in V_1$,

$$\begin{aligned}\varphi(dv) &= \varphi\alpha_d(v) = \varphi\alpha_d\varphi^{-1}\varphi(v)\\ &= \alpha_{\tau(d)}\varphi(v) \text{ since } \alpha_{\tau(d)} = \varphi\alpha_d\varphi^{-1}\\ &= \tau(d)\varphi(v) \text{ by definition of } \alpha_{\tau(d)}. \qquad (**)\end{aligned}$$

Proposition IX.1.17 (continued 5)

Proof (continued). Reversing the roles of D_1 and D_2 in the previous argument (and replacing φ and σ with φ^{-1} and σ^{-1}, respectively) yields that for every $d_2 \in D_2$ there exists $d_1 \in D_1$ such that $\varphi^{-1}\alpha_{d_2}\varphi = \alpha_{d_1} : V_1 \to V_1$, whence $\alpha_{d_2} = \varphi\alpha_{d_1}\varphi^{-1} = \alpha_{\tau(d_1)}$. So $\tau(d_1) = d_2$ and τ is surjective/onto. Hence $\tau : D_1 \to D_2$ is an isomorphism and so D_1 is isomorphic to D_2, as claimed.

Furthermore, for every $d \in D_1$ and $v \in V_1$,

$$\begin{aligned}\varphi(dv) &= \varphi\alpha_d(v) = \varphi\alpha_d\varphi^{-1}\varphi(v) \\ &= \alpha_{\tau(d)}\varphi(v) \text{ since } \alpha_{\tau(d)} = \varphi\alpha_d\varphi^{-1} \\ &= \tau(d)\varphi(v) \text{ by definition of } \alpha_{\tau(d)}. \qquad (**)\end{aligned}$$

Consider the sets $A = \{u_1, u_2, \ldots, u_k\}$ and $B = \{\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_k)\}$. Suppose A is D_1-linearly independent; then for $r_1, r_2, \ldots, r_k \in D_1$ we have that $r_1u_1 + r_2u_2 + \cdots + r_ku_k = 0$ implies that $r_1 = r_2 = \cdots = r_k = 0$.

Proposition IX.1.17 (continued 5)

Proof (continued). Reversing the roles of D_1 and D_2 in the previous argument (and replacing φ and σ with φ^{-1} and σ^{-1}, respectively) yields that for every $d_2 \in D_2$ there exists $d_1 \in D_1$ such that $\varphi^{-1}\alpha_{d_2}\varphi = \alpha_{d_1} : V_1 \to V_1$, whence $\alpha_{d_2} = \varphi\alpha_{d_1}\varphi^{-1} = \alpha_{\tau(d_1)}$. So $\tau(d_1) = d_2$ and τ is surjective/onto. Hence $\tau : D_1 \to D_2$ is an isomorphism and so D_1 is isomorphic to D_2, as claimed.

Furthermore, for every $d \in D_1$ and $v \in V_1$,

$$\begin{aligned} \varphi(dv) &= \varphi\alpha_d(v) = \varphi\alpha_d\varphi^{-1}\varphi(v) \\ &= \alpha_{\tau(d)}\varphi(v) \text{ since } \alpha_{\tau(d)} = \varphi\alpha_d\varphi^{-1} \\ &= \tau(d)\varphi(v) \text{ by definition of } \alpha_{\tau(d)}. \qquad (**) \end{aligned}$$

Consider the sets $A = \{u_1, u_2, \ldots, u_k\}$ and $B = \{\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_k)\}$. Suppose A is D_1-linearly independent; then for $r_1, r_2, \ldots, r_k \in D_1$ we have that $r_1u_1 + r_2u_2 + \cdots + r_ku_k = 0$ implies that $r_1 = r_2 = \cdots = r_k = 0$.

Proposition IX.1.17 (continued 6)

Proof (continued). Suppose $s_1\varphi(u_1) + s_2\varphi(u_2) + \cdots + s_k\varphi(u_k) = 0$ for $s_1, s_2, \ldots, s_k \in D_2$. Since $\tau : D_1 \to D_2$ is an isomorphism, then there are $r_1, r_2, \ldots, r_k \in D_1$ such that $\tau(r_1) = s_1, \tau(r_2) = s_2, \ldots, \tau(r_k) = s_k$ and so $\tau(r_1)\varphi(u_1) + \tau(r_2)\varphi(u_2) + \cdots + \tau(r_k)\varphi(u_k) = 0$, or by $(**)$, $\varphi(r_1u_1) + \varphi(r_2u_2) + \cdots + \varphi(r_ku_k) = 0$, or since φ is a homomorphism, $\varphi(r_1u_1 + r_2u_2 + \cdots + r_ku_n) = 0$. Since φ is an isomorphism, it is injective (one to one) and so $r_1u_1 + r_2u_2 + \cdots + r_ku_k = 0$. Since A is linearly independent, then $r_1 = r_2 = \cdots = r_k = 0$. Since τ is a homomorphism, $s_1 = s_2 = \cdots = s_k = 0$.

Proposition IX.1.17 (continued 6)

Proof (continued). Suppose $s_1\varphi(u_1) + s_2\varphi(u_2) + \cdots + s_k\varphi(u_k) = 0$ for $s_1, s_2, \ldots, s_k \in D_2$. Since $\tau : D_1 \to D_2$ is an isomorphism, then there are $r_1, r_2, \ldots, r_k \in D_1$ such that $\tau(r_1) = s_1, \tau(r_2) = s_2, \ldots, \tau(r_k) = s_k$ and so $\tau(r_1)\varphi(u_1) + \tau(r_2)\varphi(u_2) + \cdots + \tau(r_k)\varphi(u_k) = 0$, or by $(**)$, $\varphi(r_1u_1) + \varphi(r_2u_2) + \cdots + \varphi(r_ku_k) = 0$, or since φ is a homomorphism, $\varphi(r_1u_1 + r_2u_2 + \cdots + r_ku_n) = 0$. Since φ is an isomorphism, it is injective (one to one) and so $r_1u_1 + r_2u_2 + \cdots + r_ku_k = 0$. Since A is linearly independent, then $r_1 = r_2 = \cdots = r_k = 0$. Since τ is a homomorphism, $s_1 = s_2 = \cdots = s_k = 0$. Similarly, since φ^{-1} and σ^{-1} are isomorphisms, if B is linearly independent then A is linearly independent. So A is linearly independent if and only if B is. Therefore A is a basis for V_1 if and only if B is a basis for V_2 and so $\dim_{D_1}(V_1) = \dim_{D_2}(V_2)$, as claimed (recall that V_1 and V_2 are finite dimensional, by hypothesis).

Proposition IX.1.17 (continued 6)

Proof (continued). Suppose $s_1\varphi(u_1) + s_2\varphi(u_2) + \cdots + s_k\varphi(u_k) = 0$ for $s_1, s_2, \ldots, s_k \in D_2$. Since $\tau : D_1 \to D_2$ is an isomorphism, then there are $r_1, r_2, \ldots, r_k \in D_1$ such that $\tau(r_1) = s_1, \tau(r_2) = s_2, \ldots, \tau(r_k) = s_k$ and so $\tau(r_1)\varphi(u_1) + \tau(r_2)\varphi(u_2) + \cdots + \tau(r_k)\varphi(u_k) = 0$, or by $(**)$, $\varphi(r_1 u_1) + \varphi(r_2 u_2) + \cdots + \varphi(r_k u_k) = 0$, or since φ is a homomorphism, $\varphi(r_1 u_1 + r_2 u_2 + \cdots + r_k u_n) = 0$. Since φ is an isomorphism, it is injective (one to one) and so $r_1 u_1 + r_2 u_2 + \cdots + r_k u_k = 0$. Since A is linearly independent, then $r_1 = r_2 = \cdots = r_k = 0$. Since τ is a homomorphism, $s_1 = s_2 = \cdots = s_k = 0$. Similarly, since φ^{-1} and σ^{-1} are isomorphisms, if B is linearly independent then A is linearly independent. So A is linearly independent if and only if B is. Therefore A is a basis for V_1 if and only if B is a basis for V_2 and so $\dim_{D_1}(V_1) = \dim_{D_2}(V_2)$, as claimed (recall that V_1 and V_2 are finite dimensional, by hypothesis).

Proposition IX.1.17 (continued 7)

Proof (continued). (ii) Suppose there is an isomorphism of rings

$\mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2)$. By Theorem VII.1.4, $\mathrm{Hom}_{D_1^{\mathrm{op}}}(V_1, V_1) \cong \mathrm{Mat}_{n_1}((D_1^{\mathrm{op}})^{\mathrm{op}})$ and $\mathrm{Hom}_{D_2^{\mathrm{op}}}(V_2, V_2) \cong \mathrm{Mat}_{n_2}((D_2^{\mathrm{op}})^{\mathrm{op}})$. By Exercise III.1.17(d), $(D_1^{\mathrm{op}})^{\mathrm{op}} = D_1$ and $(D_2^{\mathrm{op}})^{\mathrm{op}} = D_2$, so

$$\mathrm{Hom}_{D_1^{\mathrm{op}}}(V_1, V_1) \cong \mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2) \cong \mathrm{Hom}_{D_2^{\mathrm{op}}}(V_2, V_2).$$

Proposition IX.1.17 (continued 7)

Proof (continued). (ii) Suppose there is an isomorphism of rings

$\mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2)$. By Theorem VII.1.4, $\mathrm{Hom}_{D_1^{\mathrm{op}}}(V_1, V_1) \cong \mathrm{Mat}_{n_1}((D_1^{\mathrm{op}})^{\mathrm{op}})$ and $\mathrm{Hom}_{D_2^{\mathrm{op}}}(V_2, V_2) \cong \mathrm{Mat}_{n_2}((D_2^{\mathrm{op}})^{\mathrm{op}})$. By Exercise III.1.17(d), $(D_1^{\mathrm{op}})^{\mathrm{op}} = D_1$ and $(D_2^{\mathrm{op}})^{\mathrm{op}} = D_2$, so

$$\mathrm{Hom}_{D_1^{\mathrm{op}}}(V_1, V_1) \cong \mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2) \cong \mathrm{Hom}_{D_2^{\mathrm{op}}}(V_2, V_2).$$

By part (i), $n_1 = \dim_{D_1^{\mathrm{op}}}(V_1, V_1) = \dim_{D_2^{\mathrm{op}}}(V_2, V_2) = n_2$ and $D_1^{\mathrm{op}} \cong D_2^{\mathrm{op}}$. By Exercise III.1.17(e), $D_1 \cong D_2$, as claimed. □

Proposition IX.1.17 (continued 7)

Proof (continued). (ii) Suppose there is an isomorphism of rings

$\mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2)$. By Theorem VII.1.4, $\mathrm{Hom}_{D_1^{\mathrm{op}}}(V_1, V_1) \cong \mathrm{Mat}_{n_1}((D_1^{\mathrm{op}})^{\mathrm{op}})$ and $\mathrm{Hom}_{D_2^{\mathrm{op}}}(V_2, V_2) \cong \mathrm{Mat}_{n_2}((D_2^{\mathrm{op}})^{\mathrm{op}})$. By Exercise III.1.17(d), $(D_1^{\mathrm{op}})^{\mathrm{op}} = D_1$ and $(D_2^{\mathrm{op}})^{\mathrm{op}} = D_2$, so

$$\mathrm{Hom}_{D_1^{\mathrm{op}}}(V_1, V_1) \cong \mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2) \cong \mathrm{Hom}_{D_2^{\mathrm{op}}}(V_2, V_2).$$

By part (i), $n_1 = \dim_{D_1^{\mathrm{op}}}(V_1, V_1) = \dim_{D_2^{\mathrm{op}}}(V_2, V_2) = n_2$ and $D_1^{\mathrm{op}} \cong D_2^{\mathrm{op}}$. By Exercise III.1.17(e), $D_1 \cong D_2$, as claimed. □