THE JACOBSON DENSITY THEOREM AND APPLICATIONS

We consider rings not necessarily with identity. By modules we mean right modules.

1. Basic definitions

1.1. Strictly Cyclic Modules and Modular Right Ideals. For a ring A with identity, cyclic modules are precisely those of the form $\mathfrak{a}\backslash A$ where $\mathfrak{a}$ is a right ideal.[1] What might be a useful analogous statement for a ring without identity? This question motivates what follows in this subsection.

A module M is *strictly cyclic* if there exists m in M such that $mA = M$ (such an m is called a *generator*); a right ideal $\mathfrak{a}$ is *modular* if there exists e in A such that $a - ea$ belongs to $\mathfrak{a}$ for every a in A (such an e is a *left identity* for $\mathfrak{a}$). These two notions are related thus: strictly cyclic modules are precisely those of the form $\mathfrak{a}\backslash A$ for modular right ideals $\mathfrak{a}$. Proof: the image of a left identity for $\mathfrak{a}$ in $\mathfrak{a}\backslash A$ is a generator; if m is a generator for M, then any element e such that $me = m$ is a left identity for the right ideal consisting of annihilators of m.

The usefulness of the notion of a modular right ideal is further borne out by the following basic observations. To set these up, first note that the annihilator of a module is a two sided ideal. Thus, for modules $N \subseteq M$, the "colon" $(N : M) := \{a \in A \,|\, Ma \subseteq N\}$ is a two sided ideal in A. In the case when M is A and N a right ideal $\mathfrak{a}$, we can compare $\mathfrak{a}$ with $(\mathfrak{a} : A)$. For a modular right ideal $\mathfrak{a}$ with left identity e,

- $(\mathfrak{a} : A) \subseteq \mathfrak{a}$; in fact, $(\mathfrak{a} : A)$ is the largest two sided ideal contained in $\mathfrak{a}$.[2]
- There is no proper right ideal containing both $\mathfrak{a}$ and e. Thus, by an application of Zorn's Lemma, $\mathfrak{a}$ is contained in a maximal (proper) right ideal (which is necessarily modular—see the next item).
- e continues to be a left identity for right ideals containing $\mathfrak{a}$.[3]

1.2. Irreducibility and Primitivity. A module M is *irreducible* if $MA \neq 0$ and there are no proper non-zero submodules. Here are two other equivalent ways of expressing the irreducibility of a module M:

- $M \neq 0$, and $mA = M$ for any $m \neq 0$ in M (this means any $m \neq 0$ is a generator for M).
- M is of the form $\mathfrak{a}\backslash A$ where $\mathfrak{a}$ is a maximal modular right ideal.[4]

Date: May 2005; *Author*: K. N. Raghavan; please send corrections to `knr@imsc.res.in`.

[1] Given our conventions, the notation $\mathfrak{a}\backslash A$ seems more appropriate than $A/\mathfrak{a}$ for the quotient of A by its right submodule $\mathfrak{a}$.

[2] In general, without the hypothesis of modularity on a right ideal $\mathfrak{a}$, we have:
– Any left ideal $\mathfrak{b}$ contained in $\mathfrak{a}$ is contained in $(\mathfrak{a} : A)$ for $A\mathfrak{b} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$.
– The largest left ideal contained in $\mathfrak{a}$ is a two sided ideal.

[3] $(1 - e)A := \{x - ex \,|\, x \in A\}$ is a right ideal; and e is a left identity for a right ideal $\mathfrak{b}$ iff $\mathfrak{b}$ contains $(1 - e)A$. See §1.4 on quasi-regular elements for more.

[4] Maximal modular right ideals are maximal as right ideals as observed in §1.1.

The proof of the equivalence of these conditions is left as an exercise for the reader.

Annihilators of irreducible modules are called *primitive ideals*.[5] They are precisely those of the form $(\mathfrak{a} : A)$ for maximal modular right ideals $\mathfrak{a}$.

A ring is *primitive*[6] if 0 is a primitive ideal, that is, if there exists a faithful irreducible module. Division rings are primitive—the ring itself is a faithful irreducible module. In the commutative case, we have a converse: a primitive commutative ring is a field. Proof: By primitivity, the zero ideal equals $(\mathfrak{a} : A)$ for some maximal modular right ideal $\mathfrak{a}$. By commutativity, $(\mathfrak{a} : A) \supseteq \mathfrak{a}$, so $\mathfrak{a} = 0$. The modularity of 0 shows that A has an identity. The maximality shows that every non-zero element is invertible.

1.3. **Radical and Semi-simplicity.** The *radical*[7] is the intersection[8] of all primitive ideals, or, what amounts to the same, any of the following:

- the intersection over all irreducible modules of their annihilators.
- the intersection over all maximal modular right ideals $\mathfrak{a}$ of $(\mathfrak{a} : A)$.[9]
- the intersection of all maximal modular right ideals.

It is only the third alternative description that requires comment. The annihilator of a module M is the intersection over all elements m in M of their annihilators $(0 : m)$. For M irreducible, each $(0 : m)$ is a maximal modular right ideal as $(0 : m)\backslash A$ is isomorphic to M.[10]

A ring is *semi-simple* if its radical is 0 and *radical* if its radical is itself.

1.4. **Quasi-regular elements.** The internal characterization of the radical in §1.5 below is in terms of quasi-regular elements, whence the motivation for the notion of quasi-regularity. To understand the definition, suppose that a ring A has an identity 1. The map $z \mapsto 1 - z$ is an involution (as a map of sets) of A. Pulling back the multiplication of A via this involution gives a new multiplication on A called the "circle" composition:

$$z \circ z' := z + z' - zz'$$

This makes sense even when A does not have an identity. It is associative (proof: embed A into a larger ring with identity and pull back) and 0 acts as the identity for it. An element z of A is *right quasi-regular* if it has a right inverse[11] with respect to this composition, i.e., if there exists z' such that $z \circ z' = z + z' - zz' = 0$.

Left quasi-regularity is similarly defined, and z is *quasi-regular* if it is both right and left quasi-regular (in which case there exists z' such that $z \circ z' = z' \circ z = 0$).

[5]More precisely, although these ideals are themselves two-sided, they should be called *right primitive ideals*, for they arise as annihilators of irreducible right modules. There is the analogous notion of *left primitive ideal*. An ideal could be right primitive without being left primitive as was shown by Bergman, Proceedings of the A. M. S., 1964.

[6]Again, more precisely, *right primitive*. See the previous footnote.

[7]More precisely, at least for now, we should say *right radical*, but, as we will see in §1.5, it follows as a consequence of the internal characterization of the (right) radical that the left and right radicals coincide.

[8]Here and elsewhere, an intersection of a family of subsets is taken to be the whole set when the family is empty.

[9]It seems natural to wonder if $(\mathfrak{a} : A)$ is a maximal two sided ideal when $\mathfrak{a}$ a maximal modular right ideal. We will see in §3.1 that this is the case when A is right Artinian.

[10]This may take some getting used to: unlike in the case when A is commutative with identity, it is possible (and quite common) that $\mathfrak{a}\backslash A$ and $\mathfrak{b}\backslash A$ are isomorphic for distinct right ideals $\mathfrak{a}$, $\mathfrak{b}$.

[11]Caution: quasi-regularity means nearness to 0, not to 1.

If all elements of a right ideal $\mathfrak{a}$ are right quasi-regular then they are all quasi-regular: if a is in $\mathfrak{a}$ with a right circle inverse b, then b belongs to $\mathfrak{a}$ and so has a right circle inverse c; then $a = a \circ 0 = a \circ (b \circ c) = (a \circ b) \circ c = 0 \circ c = c$, so that b is a left circle inverse for $a = c$. Such a right ideal is called *quasi-regular*.

A nilpotent element is quasi-regular: if $z^n = 0$, then $-(z + \cdots + z^{n-1})$ is a circle inverse for z as the familiar identity $(1 - z)^{-1} = 1 + z + \cdots + z^{n-1}$ shows. Thus *nil-ideals*—those ideals all of whose elements are nilpotent—are quasi-regular.

Here is another way of looking at right quasi-regularity: for an element z in a ring A, $\{a - za \,|\, a \in A\}$ is a right ideal which we denote by $(1 - z)A$ even if A does not have 1; it is the smallest right ideal for which z is a left identity.[12] Now, z is right quasi-regular iff $(1 - z)A = A$, for "clearly" $1 - z$ has a right multiplicative inverse iff $(1 - z)A = A$.[13]

1.5. **Internal characterization of the radical.** We can now state the main result of this section, namely, the following characterization of the radical due to Jacobson[14], following Perlis[15].

> *The radical consists of quasi-regular elements and contains every quasi-regular right ideal.*

Before turning to the proof, let us record some consequences:

- The left analogue of the second assertion says that the left radical contains every quasi-regular left ideal. On the other hand, by the first assertion, the (right) radical is quasi-regular as a left ideal. Thus the left radical contains the radical. The other way around is similarly true, so that the radical and left radical are equal.
- The following are all equal to the radical:
  - The union of all quasi-regular right ideals.
  - The union of all quasi-regular left ideals.
  - $\{z \in A \,|\, xzy$ quasi-regular for all x and y in $A\}$.

  The proofs of these equalities are left as exercises for the reader.
- The radical contains all one-sided nil ideals for these are quasi-regular.

Turning to the proof of the result, first suppose that z is not right quasi-regular, which means $(1 - z)A \neq A$. Let $\mathfrak{a}$ be a maximal (proper) right ideal containing $(1-z)A$. Then z is a left identity for $\mathfrak{a}$, and so does not kill[16] the irreducible module $\mathfrak{a}\backslash A$, and so is not in the radical. The first assertion is thus proved.

For the second assertion, suppose that zA is quasi-regular for some z not in the radical. Let m be an element of an irreducible module M such that $mz \neq 0$. By the irreducibility of M, we have $mzA = M$. In particular, there exists y in A such that $mzy = m$ or $m(1 - zy) = 0$. Since $(1 - zy)$ has a right inverse, this means $m = 0$, a contradiction, and the proof of the second assertion is complete.

---

[12] Recall that z is a left identity for a right ideal $\mathfrak{a}$ if $x - zx$ belongs to $\mathfrak{a}$ for every x in A.

[13] Here as elsewhere it is to be understood that the arguments involving 1 can easily be replaced by those that do not involve 1 and hold for rings without identity.

[14] The Radical and Semi-simplicity for Arbitrary Rings, *Amer. Jour. of Math.*, 1945

[15] A characterization of the radical of an algebra, *Bulletin of the A. M. S.*, vol. **48**, 1942.

[16] Proof: $\mathrm{Ann}(\mathfrak{a}\backslash A) = (\mathfrak{a} : A) \subseteq \mathfrak{a}$ since $\mathfrak{a}$ is modular; if $z \in (\mathfrak{a} : A)$, then, on the one hand, $zA + (1 - z)A \subseteq \mathfrak{a}$ since $\mathfrak{a}$ is a right ideal, but, on the other, $zA + (1 - z)A = A$, so $\mathfrak{a} = A$, a contradiction to the properness of $\mathfrak{a}$.

2. The Density Theorem

2.1. **The Density Theorem.** The density theorem was proved by Jacobson in his beautiful paper "Structure theory of simple rings without finiteness assumptions," *Trans. Amer. Math. Soc.*, 1945. The exposition below follows Chapter II of Jacobson's "Structure of Rings," AMS Colloquium Publications Vol. XXXVII, Second Edition, 1963.

Let R be a ring (not necessarily with identity) and M a (right) R-module. Suppose that M is irreducible—this means that $MR \neq 0$ and M has no proper non-zero submodules. By Schur, $\Gamma := \mathrm{End}_R(M)$ is a division ring. It is natural to let Γ act on the left on M, turning M into a Γ-R bimodule.[17] The Jacobson density theorem states:

> *R is dense for M as a Γ vector space, i.e., given a finite sequence $m_1, \ldots, m_n$ of Γ-linearly independent elements of M and a sequence $m'_1, \ldots, m'_n$ of elements of M, there exists r in R such that $m_1 r = m'_1, \ldots, m_n r = m'_n$.*

The following result of Burnside follows as an immediate corollary: if V is a finite dimensional complex irreducible representation of a group G, then $\mathrm{End}_{\mathbb{C}} V$ is spanned by the images in it of elements of G.

The density theorem above follows from a more general statement which we call, for want of a better name, the "general density theorem":

> *Let R and Γ be rings, M a left Γ-module, M' a Γ-R bimodule, and B a subset of Γ-linear maps from M to M'. Assume that M is an irreducible R-module, that $\Gamma = \mathrm{End}_R(M)$, and that B is closed under addition and $BR \subseteq B$. Then, given a sequence $m_1, \ldots, m_n$ of elements of M that are Γ-linearly independent modulo $B^\perp$, and a sequence $m'_1, \ldots, m'_n$ of elements of M', there exists b in B such that $m_1 b = m'_1, \ldots, m_n b = m'_n$.*

To deduce the density theorem from this, set $M' = M$ and $B = R$. Since M' is irreducible as an R-module, it follows that $B^\perp = 0$.

The general density theorem is in turn deduced from the following "double annihilator" lemma:

> *Let R and Γ be rings, M a left Γ-module, M' a Γ-R bimodule, and B a subset of Γ-linear maps from M to M'. Assume that every R-map from an R-submodule of M' to M' is obtained as left multiplication by an element of Γ, and that B is closed under addition and $BR \subseteq B$. Then, given finitely many elements $u_1, \ldots, u_p$ of M, we have*
>
> $$(u_1^\perp \cap \cdots \cap u_p^\perp \cap B)^\perp = B^\perp + \Gamma u_1 + \cdots + \Gamma u_p.$$

Before turning to the proof of the lemma, let us deduce the general density theorem from the lemma. It is enough to find b_1 in B such that $x_1 b_1 = y_1$, and $x_2 b_1 = \ldots = x_n b_1 = 0$, for in that case we will have $b_2, \ldots, b_n$ with analogous properties, and $b = b_1 + \ldots + b_n$ will do the job (b belongs to B because B is closed under addition). In turn, it is enough to find b'_1 in B such that $x_1 b'_1 \neq 0$, and $x_2 b'_1 = \ldots = x_n b'_1 = 0$,

[17] If A and B are rings and M a left A-module and also a right B-module, we say that M is an A-B *bimodule* if the actions on it of A and B commute, i.e., $(am)b = a(mb)$ for a, b, and m respectively in A, B, and M.

for, then, by the irreducibility of M', there exists r in R such that $x_1 b_1' r = y_1$, and we can take b_1 to be $b_1' r$ (this belongs to B because $BR \subseteq B$).

To find such a b_1', we apply the lemma, taking $u_1, \ldots, u_p$ to be $x_2, \ldots, x_n$. Since M' is irreducible and $\Gamma = \mathrm{End}_R(M')$, it follows that the hypothesis in the lemma about R-maps from R-submodules of M' to M' is satisfied. Since $x_1, \ldots, x_n$ are linearly independent modulo $B^\perp$, it follows that x_1 does not belong to $B^\perp + \Gamma x_2 + \ldots + \Gamma x_n$. By the lemma, x_1 does not belong to $(x_2^\perp \cap \cdots \cap x_n^\perp \cap B)^\perp$, which means precisely the existence of a b_1' in B with the required properties.

Now to the proof of the lemma. It is in general true that the right hand side is contained in the left hand side. To obtain the other containment, proceed by induction on p. First suppose that $p = 1$. Let v belong to $(u_1^\perp \cap B)^\perp$. Then $u_1 b \mapsto vb$ is a well-defined R-map from the R-submodule $u_1 B$ of M' to M'. By hypothesis, there exists $\gamma \in \Gamma$ such that $vb = \gamma u_1 b$ for all b in B, which means that $v - \gamma u_1$ belongs to $B^\perp$. Writing $v = \gamma u_1 + (v - \gamma u_1)$, and we are done with the case $p = 1$.

The induction step of the proof is rather easy. Set $B' := u_2^\perp \cap \cdots \cap u_n^\perp \cap B$. Then B' too satisfies the hypothesis on B: it is closed under addition and $B'R \subseteq B'$. By the case $p = 1$, we have $(u_1^\perp \cap B')^\perp \subseteq {B'}^\perp + \Gamma u_1$. By the induction hypothesis, we have ${B'}^\perp \subseteq B^\perp + \Gamma u_2 + \cdots + \Gamma u_p$. □

3. Artinian Semisimple Rings

A ring, not necessarily with identity, is called *(right) Artinian* if the following equivalent conditions hold:

- Any non-empty collection of right ideals has minimal elements (with respect to inclusion).
- Dcc on right ideals: any descending chain of right ideals stabilizes.

There is the analogous notion of *left Artinian ring*. In general, right and left Artinian-ness are distinct notions,[18] although, as we shall see, for a semisimple ring they coincide.

3.1. Structure of primitive Artinian rings.

The Jacobson density theorem says the following about a primitive ring: it is a dense ring of endomorphisms of a vector space over a division ring.[19] If a primitive ring happens to be Artinian, then, as is readily seen,[20] this vector space is finite dimensional over the division ring, and so the ring is the full ring of linear transformations. This proves (1)⇒(3) of the following structure theorem:

The following are equivalent for an Artinian ring:
(1) *It is primitive.*
(2) *It is simple.*

[18]**Exercise:** Let $\mathbb{Q}$ be the field of rational numbers and $A := \mathbb{Q}e \oplus \mathbb{Q}z$ a two dimensional vector space over $\mathbb{Q}$ with basis $\{e, z\}$. Make A into a ring by defining $e^2 = e$, $ez = 0$, $ze = z$, and $z^2 = 0$. Show that A is right Artinian but not left Artinian.

[19]A dense ring of linear transformations of a vector space over a division ring is primitive: the vector space is a faithful irreducible module for the ring. What the theorem says is that every primitive ring can be realized in this way.

[20]If m_1, m_2, … is an unending sequence of linearly independent elements, then, since the action of the ring is dense, $\mathrm{Ann}\,(m_1) \supsetneq \mathrm{Ann}\,(m_1, m_2) \supsetneq \ldots$ is a strictly descending chain of right ideals.

(3) *It is the full ring of linear transformations of a finite dimensional vector space over a division ring.*

That (3)⇒(2) is easy to see "geometrically" and left as an exercise for the reader. That (2)⇒(1) is also easy: recall that a ring A is called *simple* if $A^2 \neq 0$ and it has no proper non-zero two-sided ideals. The Artinian assumption guarantees that A has a minimal non-zero ideal, say $\mathfrak{a}$. The annihilator of $\mathfrak{a}$ being a two sided ideal, it is either 0 or A. But it cannot be A, for, then, $\mathfrak{a}A = 0$, which implies since $\mathfrak{a} \neq 0$ that the annihilator $\mathrm{Ann}(A)$ of A as a left module is non-zero, but $\mathrm{Ann}(A)$ being a two sided ideal it then equals A, which means $A^2 = 0$, a contradiction. So the annihilator of $\mathfrak{a}$ is 0, which means $\mathfrak{a}$ is faithful as a right module. In particular $\mathfrak{a}A \neq 0$, and $\mathfrak{a}$ is an irreducible right module.

Example. The whole ring of linear transformations of an infinite dimensional vector space over a division ring is primitive but not simple: the finite rank linear transformations form a two sided ideal.

3.2. **Structure of semisimple Artinian Rings.** Let A be a ring, Artinian and semisimple. Semisimplicity means that the zero ideal is an intersection of primitive ideals. Combined with Artinian-ness, it implies that the zero ideal is a finite intersection of primitive ideals: an ideal that is minimal among finite intersections of primitive ideals is zero, for, otherwise, by intersecting with one more primitive ideal we can make it smaller.

Thus we can write the zero ideal as an irredundant intersection[21] $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$ of primitive ideals $\mathfrak{p}_i$. It follows from the structure theorem of §3.1 that the $A/\mathfrak{p}_i$ are simple rings. Using this, we prove, by induction on m, that $A = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ where $\mathfrak{a}_i := \mathfrak{p}_1 \cap \cdots \cap \hat{\mathfrak{p}}_j \cap \cdots \cap \mathfrak{p}_m$.

For $m = 1$, we have $\mathfrak{a}_1 = A$ by definition, and so the assertion holds.

Suppose that $m \geq 2$. Since $\mathfrak{a}_m$ is not contained in $\mathfrak{p}_m$, its image in $A/\mathfrak{p}_m$ is a non-zero two sided ideal. But $A/\mathfrak{p}_m$ being simple, the image is all of $A/\mathfrak{p}_m$, which translates to $A = \mathfrak{p}_m + \mathfrak{a}_m$. Since $\mathfrak{a}_m \cap \mathfrak{p}_m = 0$, we get $A = \mathfrak{p}_m \oplus \mathfrak{a}_m$.

Consider the ideals $\mathfrak{p}_1 \cap \mathfrak{p}_m, \ldots, \mathfrak{p}_{m-1} \cap \mathfrak{p}_m$ in the ring $\mathfrak{p}_m$. We have $\mathfrak{p}_m/\mathfrak{p}_i \cap \mathfrak{p}_m \cong \mathfrak{p}_i + \mathfrak{p}_m/\mathfrak{p}_i = A/\mathfrak{p}_i$, since $\mathfrak{p}_i \not\subseteq \mathfrak{p}_m$ and $\mathfrak{p}_m$ is a maximal ideal. Thus we may apply induction to conclude that $\mathfrak{p}_m = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_{m-1}$. This finishes the proof that $A = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$.

The $\mathfrak{a}_i$ are primitive and Artinian, for $\mathfrak{a}_i \cong A/\mathfrak{p}_i$. By the structure theorem of §3.1, there exist integers n_i and division rings Γ_i such that $\mathfrak{a}_i$ is the matrix ring $M_{n_i}(\Gamma_i)$ of $n_i \times n_i$ matrices over Γ_i. Thus we have proved the "existence" part of

The Artin-Wedderburn Structure Theorem: *An Artinian semisimple ring is a finite direct sum of matrix rings over division rings. The decomposition is unique up to rearrangement of the summands: if $\oplus M_{n_i}(\Gamma_i)$ and $\oplus M_{n'_i}(\Gamma'_i)$ are two decompositions, then the number of summands in the two are same, and, after rearrangement, $n_i = n'_i$ and $\Gamma_i \cong \Gamma_i$ for all i.*

The uniqueness part of the theorem is proved in two steps, the first of which is to prove the following: *In a finite direct sum $A = \oplus_{i=1}^m \mathfrak{a}_i$ where $\mathfrak{a}_i \cong M_{n_i}(\Gamma_i)$ are matrix rings over division rings, any two sided ideal is of the form $\mathfrak{a}_{i_i} \oplus \cdots \oplus \mathfrak{a}_{i_k}$ for some $1 \leq i_1 < \ldots < i_k \leq m$.* It follows from the existence of such elements as

[21]An intersection $\mathfrak{b} = \cap \mathfrak{b}_i$, where i ranges over an index set I, is *irredundant* if, for any subset J of I such that $J \neq I$, we have $\mathfrak{b} \subsetneq \cap_{i \in J} \mathfrak{b}_i$.

$(0, \ldots, 0, 1, 0, \ldots, 0)$ in A that any two sided ideal of A contains its projections on the $\mathfrak{a}_i$. Any two sided ideal is therefore a sum of its projections. The projection on $\mathfrak{a}_i$ is either 0 or all of $\mathfrak{a}_i$ because $\mathfrak{a}_i$ is simple. This proves the assertion. It follows as a consequence that the $\mathfrak{a}_i$ are uniquely determined as the minimal two sided ideals. Thus any decomposition must involve the same $\mathfrak{a}_i$ up to permutation.

The second step in the proof of the uniqueness is this: if $M_n(\Gamma) \cong M_{n'}(\Gamma')$, then $n = n'$ and $\Gamma \cong \Gamma'$. We may pose this as follows: how to recover Γ and n from the ring $M_n(\Gamma)$? The minimal right ideals of $M_n(\Gamma)$ are all isomorphic as $M_n(\Gamma)$-modules to one another and to the "standard" module Γ^n:[22]

> **Proposition:** *Over a primitive ring admitting minimal non-zero right ideals, any faithful irreducible module is isomorphic to any such ideal.*

Proof: Let M be a faithful irreducible module and $\mathfrak{b}$ a minimal non-zero right ideal. Then $M\mathfrak{b} \neq 0$ since M is faithful. Choose m in M such that $m\mathfrak{b} \neq 0$. Since $m\mathfrak{b}$ is a submodule, we have $M = m\mathfrak{b}$ by the irreducibility of M. Since $\operatorname{Ann} m$ is a right ideal not containing $\mathfrak{b}$, we have $\mathfrak{b} \cap \operatorname{Ann} m = 0$ by the minimality of $\mathfrak{b}$. Thus $mb \mapsto b$ defines an module isomorphism from M to $\mathfrak{b}$. □

The action of $M_n(\Gamma)$ on Γ^n being dense, we may recover Γ as $\operatorname{End}_{M_n(\Gamma)}\Gamma^n$:

> **Claim:** *If A is a 2-transitive ring of Γ-endomorphisms of a vector space V over a division ring Γ, then $\operatorname{End}_A V = \Gamma$.*

Proof: Set $\Gamma' := \operatorname{End}_A V$. We have $\Gamma' \supseteq \Gamma$ by hypothesis. Suppose that $\Gamma' \supsetneq \Gamma$. Since A is 2-transitive, it is in particular 1-transitive, so V is irreducible for A. By Schur, Γ' is a division ring. Choose $\gamma' \in \Gamma' \setminus \Gamma$ and $0 \neq v$ in V. Then v, $\gamma' v$ are Γ-linearly independent. By 2-transitivity, there exists a in A such that $va = 0$ and $(\gamma' v)a \neq 0$. But this is a contradiction since $(\gamma' v)a = \gamma'(va) = 0$. □

Finally, we can recover n as the dimension over Γ of Γ^n, and the proof of uniqueness is complete.

4. Modules over Artinian semisimple rings

4.1. **Modules to unital modules.** Let A be a ring with unity and M an A-module, not necessarily unital. Then MA and $M' := \{m - m1 \mid m \in M\}$ are submodules, $M = MA \oplus M'$, MA is unital, and $M'A = 0$. If M is irreducible, then $M' = 0$ and $M = MA$ is unital. Since the ring does not exercise any control over M', the hypothesis of unitality is necessary in any structure theory of A-modules. It is not so restrictive either since, modulo the part over which we have no control, modules are unital.

4.2. **Completely Reducible modules.** Let A be a ring, not necessarily with identity. Recall that a (right) module M is called *irreducible* if $MA \neq 0$ and M has no submodules other than 0 and itself. A module M is *completely reducible* if it satisfies the following equivalent conditions:

(1) It is a sum of irreducible submodules.
(2) It is a direct sum of irreducible submodules.

[22] Exercise: There is a one-to-one inclusion reversing correspondence between Γ-subspaces W of a finite dimensional Γ-vector space V and the right ideals $\mathfrak{a}$ of $\operatorname{End}_\Gamma V$: $W \mapsto W^\perp$ and $\mathfrak{a} \mapsto \mathfrak{a}^\perp$.

(3) Every submodule has a complement, i.e., given a submodule N, there exists submodule P such that $N \oplus P = M$; and the only element m of M satisfying $mA = 0$ is 0.

Condition (3) passes to quotients and subs (every sub is isomorphic to a quotient and vice-versa); in particular, subquotients of completely reducibles are completely reducible.

The proof of the equivalence of these conditions is left as an exercise for the reader. The only part that is perhaps tricky is to show that under (3) there do exist irreducible submodules. Let us see how to do this. If M has no proper non-zero submodules, then of course M itself is irreducible and we are done. If not, let N be a proper submodule, choose y in $M \setminus N$, let N' be a maximal submodule containing N but not y, and let P be a complement for N'. The maximality of N' implies that every non-zero submodule of P contains y. In particular P is not a direct sum. But (3) holds for P, so P is irreducible.

4.3. **Modules over Artinian semisimple rings.** Let A be a ring, Artinian and semisimple. It follows from the Artin-Wedderburn structure theorem of §3 that A has identity and is a finite sum of minimal right ideals: say $A = \mathfrak{b}_1 + \cdots + \mathfrak{b}_n$ (not uniquely of course except in trivial cases). Using these facts, we can prove:

(1) *A unital module is completely reducible.*
(2) *Every irreducible module is isomorphic to a minimal right ideal.*
(3) *The number of isomorphism classes of irreducible modules equals the number of simple components of A.*

Proof: (1) Given m in M, we have $m = m1 \in m\mathfrak{b}_1 + \cdots + m\mathfrak{b}_n$. Suppose that $m\mathfrak{b}_i \neq 0$. Then, $\operatorname{Ann} m \cap \mathfrak{b}_i$ being a right ideal properly contained in $\mathfrak{b}_i$, it is 0. So $mb \mapsto b$ defines a module isomorphism between $m\mathfrak{b}_i$ and $\mathfrak{b}_i$. In particular, $m\mathfrak{b}_i$ is irreducible. Thus M is the sum of its irreducible submodules.

(2) Let M be an irreducible module. Choose m in M such that $mA \neq 0$, so that $M = mA = m\mathfrak{b}_1 + \cdots + m\mathfrak{b}_n$. Let i be such that $m\mathfrak{b}_i$ is a non-zero. Then $m\mathfrak{b}_i = M$. And, as in the proof of (1), $m\mathfrak{b}_i \cong \mathfrak{b}_i$.

(3) Let $A = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ be a decomposition of A into simple components. Let $\mathfrak{b}$ be a minimal right ideal. Then $\mathfrak{b} = \mathfrak{b}A = \mathfrak{b}\mathfrak{a}_1 + \cdots + \mathfrak{b}\mathfrak{a}_m$. Clearly $\mathfrak{b}\mathfrak{a}_i \neq 0$ for some i. Fix such an i. Then, since $\mathfrak{b}\mathfrak{a}_i \subseteq \mathfrak{b}$, we have $\mathfrak{b}\mathfrak{a}_i = \mathfrak{b}$. And $\mathfrak{b}\mathfrak{a}_j = \mathfrak{b}\mathfrak{a}_i\mathfrak{a}_j = 0$ for $j \neq i$. Let $\mathfrak{b}'$ be another minimal right ideal and i' be such that $\mathfrak{b}' = \mathfrak{b}'\mathfrak{a}_{i'}$. If $i \neq i'$, then $\mathfrak{b} \not\cong \mathfrak{b}'$ (e.g., $\mathfrak{b}\mathfrak{a}_i \neq 0$ and $\mathfrak{b}'\mathfrak{a}_i = 0$); if $i = i'$ then $\mathfrak{b}$ and $\mathfrak{b}'$ are isomorphic as $\mathfrak{a}_i$-modules (by the proposition of §3) and so also as A-modules. Finally, observe that there are minimal right ideals contained in each of the simple components $\mathfrak{a}_i$. $\square$