Math 552: Abstract Algebra II

Wolmer V. Vasconcelos

Set 4

Spring 2009

Outline

Artin Rings

In this set, **A** will be an Artinian ring, or simply an Artin ring. Typically, we assume that **A** is a left Artin ring, but side is not significant. We make use of both left and right modules when discussing Artin rings.

The main aspects we will treat are:

- The Jacobson radical of **A**
- Semi-simplicity
- Wedderburn theorem
- Major classes of examples: division rings, group rings

Examples: Matrix rings

- Let **K** be a field and **A** the ring of $n \times n$ matrices over **K**. This is the premier example. Any of its subrings **B** which is a **K** vector subspace is also Artinian.
- Among the subrings, a noteworthy is given by the upper triangular matrices

$$\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}$$

- One can also form matrix rings with entries in other matrix rings...

More examples: Artin algebras

Given a field **K** and a **K**-vector space **V** with a basis $\{e_1, \ldots, e_n\}$, an algebra structure on **V** is given by specifying a product rule

$$e_i \cdot e_j \;=\; \sum_k c_{ijk} e_k,$$

with $c_{ijk} \in \mathbf{K}$ (the **structure constants**).

The c_{ijk} must satisfy certain relations to accommodate the axioms for an algebra. Thus, to have a unit, say, e_1 must satisfy $e_1 e_i = e_i$, that means $c_{1ij} = 1$.

The commutativity axiom will translate as

$$c_{ijk} = c_{jik}.$$

The most demanding is the **associative axiom**: to have $e_i(e_je_k) = (e_ie_j)e_k$, It translates into

$$\sum_{mn} c_{imn}c_{jkn} = \sum_{mn} c_{ijn}c_{nkm}$$

For a field **K** and a group **G**, the **group ring of G over K** is the vector space **k**[**G**] with a basis indexed by **G**:

$$\sum_{\sigma \in \mathbf{G}}{}' a_\sigma \sigma$$

The associative axiom follows from the group law. If **G** is finite, **K**[**G**] is Artinian.

Earlier, in our discussion of field theory, we met a more delicate ring, the **twisted group ring**: $\mathbf{L}/\mathbf{K}$ an extension of Galois group **G**, and **L**[**G**]. Note differences...

Radical of a Ring

If **A** is a ring with 1, we have several classes of interesting ideals. For example: there are maximal left ideals, maximal right ideals, two-sided maximal ideals. They are usually very distinct.

Proposition

For any left ideal I TFAE:

1. $1 + a$ *is left invertible* $\forall a \in I$.
2. *If M is a finitely generated left* **A***-module and $M = IM$, then $M = 0$.*
3. $I \subseteq \bigcap P$ all maximal left ideals.

Proof. (1) $\Rightarrow$ (2): Let $M = (m_1, \ldots, m_r)$, with r as small as possible. Then

$$\begin{aligned} m_1 &= a_1 m_1 + a_2 m_2 + \cdots + a_r m_r, \quad a_i \in I \\ (1 - a_1) m_1 &= a_2 m_2 + \cdots + a_r m_r, \end{aligned}$$

and since $1 - a_1$ is invertible, $m_1 \in (m_2, \ldots, m_r)$, a contradiction.

(2) $\Rightarrow$ (3): Let P be a maximal left ideal and set $M = \mathbf{A}/P$. M is a simple module, so $IM = 0$ (and $I \subset P$), or $IM = M$. In this case, $M = 0$, which is a contradiction.

(3) $\Rightarrow$ (1): For $a \in I$, the ideal $\mathbf{A}(1 + a)$ cannot be contained in any maximal left ideal P as $a \in P$. Thus $\mathbf{A}(1 + a) = \mathbf{A}$.

Example: An ideal I is **nil** if for each $a \in I$, $a^n = 0$ for some n (that may depend on a), while I is **nilpotent** if $I^n = 0$ for some n. If $a^n = 0$,

$$(1 + a + \cdots + a^{n-1})(1 - a) = 1,$$

so nil ideals satisfy the conditions above.

Annihilators

Let **A** be a ring, and M a left **A**-module. We will make use of the following constructions of annihilators:

- If $a \in \mathbf{A}$, its left annihilator is the set $L = \{r \in \mathbf{A} : ra = 0\}$. Note that L is a left ideal.
- If $m \in M$, its annihilator is the set $L = \{r \in \mathbf{A} : rm = 0\}$. Note that L is a left ideal.
- The annihilator of M is the set

$$L = \{r \in \mathbf{A} : rm = 0, \forall m \in M\}.$$

Note $\mathbf{A} \cdot L \cdot \mathbf{A} \cdot M = \mathbf{A} \cdot L \cdot M = 0$, so L is a two-sided ideal.

Cute reversal

Proposition

Let I be a left ideal such that $1 + a$ has a left inverse for all $a \in I$. Then $1 + a$ has a right inverse.

Proof. Let $a \in I$ and let b be a left inverse of $1 + a$

$$\begin{aligned} b(1+a) &= 1 = b + ba \\ 1 - b &= ba \in I, \quad \text{therefore } 1 - (1-b) \text{ has a left inverse} \\ cb &= 1 \quad \text{therefore} \\ c(b(1+a)) &= c = 1 + a \end{aligned}$$

Primitive ideals

Definition

Let $\mathbf{A}$ be a ring with 1.

1. A left module M is **faithful** if its annihilator $\operatorname{ann} M = 0$.
2. $\mathbf{A}$ is **primitive** if there is a simple, faithful module.
3. The ideal I is **left primitive** if I is two-sided and $\mathbf{A}/I$ is (left) primitive.

For example, $\mathbf{V} = \mathbf{K}^n$ is a left module over the matrix ring $\mathbf{A} = \mathrm{Hom}_{\mathbf{K}}(\mathbf{V}, \mathbf{V})$. $\mathbf{V}$ is faithful [check] and simple [check]. Thus 0 is a left primitive ideal of $\mathbf{A}$.

Primitive ideals

Proposition

Every left maximal ideal P contains a left primitive ideal.

Proof.

Let I be the annihilator of $\mathbf{A}/P$. I is a two-sided ideal and $\mathbf{A}/P$ is a left, faithful $\mathbf{A}/I$-module. $\square$

Proposition

A left primitive ideal I is the intersection of the left maximal ideals containing it.

Recall that if M is a left $\mathbf{A}$-module, the annihilator $\operatorname{ann} M$ is a two-sided ideal, and for $m \in M$, $\operatorname{ann}(m)$ is a left ideal.

Proof.

Let M be a faithful, simple left $\mathbf{A}/I$-module. Note

$$I = \bigcap_{0 \neq m \in M} \operatorname{ann}(m).$$

For $0 \neq m \in M$, $\mathbf{A}m = M$. Let P be the annihilator of m. P is a left maximal ideal as $\mathbf{A}/P$ is simple and $I \subset M$. □

Jacobson radical

Proposition

For any ring **A**, *let*

1. $J_1 = \bigcap P_1, \quad \text{left primitive ideals}$;
2. $J_2 = \bigcap P_2, \quad \text{maximal left ideals}$;
3. $J_1 = \bigcap P_3, \quad \text{maximal right ideals}$.

Then $J_1 = J_2 = J_3$. *This ideal is called the Jacobson radical of* **A**, *and will be denoted by* $J(\mathbf{A})$.

Jacobson radical of an Artin ring

Theorem

If $\mathbf{A}$ is a left Artin ring, then $J(\mathbf{A})$ is nilpotent.

Proof. Consider the descending chain

$$J \supseteq J^2 \supseteq \cdots \supseteq J^k = J^{k+1} = \cdots \quad \text{set } L = J^k.$$

From $L = L^2$ we are going to argue $L = 0$. If $L \neq 0$, pick I a minimal left nonzero ideal such that $LI \neq 0$. Thus there is $u \in I$ such that $Lu \neq 0$, so since $L = L^2$, $Lu = I$.

This means that $u = su$, for $s \in L$, so $(1 - s)u = 0$, whence $u = 0$ since $1 - s$ is invertible.

Local algebras of endomorphisms

Here is a minor research topic. Let R be a Noetherian local ring of maximal ideal $\mathfrak{m}$ and let E be a finitely generated R-module. We now treat conditions for the algebra $\Lambda = \mathrm{Hom}_R(E, E)$ to have a unique two-sided maximal ideal.

Proposition

Let $(R, \mathfrak{m})$ be a Noetherian local ring and let E be a finitely generated R-module.

1. *If E has no free summand, then the image of $E^* \otimes E$ in Λ is a two-sided ideal contained in the Jacobson radical.*
2. *Moreover if R is a Gorenstein ring and E is a module of syzygies of perfect module R/I, then Λ is a local algebra. In particular Λ will be a local algebra when I is generated by a regular sequence.*

Proof

Proof. The action of Λ on $E^* \otimes E$ is as follows. For $\mathbf{h} \in \Lambda$, $(f \otimes e)\mathbf{h} = f \circ \mathbf{h} \otimes e$ and $\mathbf{h}(f \otimes e) = f \otimes \mathbf{h}(e)$.

Let $\mathbf{I}$ be the identity of Λ. To prove that

$$\mathbf{h} = \mathbf{I} + \sum_{i=1}^{n} f_i \otimes e_i$$

is invertible, note that for each $e \in E$,

$$\mathbf{h}(e) = e + \sum_{i=1}^{n} f_i(e) e_i \in e + \mathfrak{m}E,$$

since $f_i(e) \in \mathfrak{m}$ as E has no free summand. From the Nakayama Lemma, it follows that $\mathbf{h}$ is a surjective endomorphism, and therefore must be invertible.

Payoff

Let **A** be a left Artin ring. Will now discuss the following properties of **A**:

- Semi-simple **A**-modules
- Semi-simple Artin ring
- Left Artin $\Rightarrow$ right Artin
- Left Artin $\Rightarrow$ left Noetherian

Outline

Assignment #15

1. Let T_n be the set of upper triangular matrices over the field $\mathbf{K}$. Describe all the maximal left ideals of T_n and its Jacobson radical.

Outline

Semisimple Modules

Definition

Let **A** be a ring and M a left **A**-module. M is semisimple if

$$M = \bigoplus_{i \in I} M_i, \quad M_i \text{ simple.}$$

Besides vector spaces, what are they? Their properties...

Summands

- A submodule L of A is a **direct summand** if there another submodule $L' \subset A$ such that
$$A = L + L', \quad L \cap L' = 0.$$
- Another way: There exists a homomorphism $\varphi : A \to L$ such that $\varphi(x) = x$ for $x \in L$. φ is called a **projection**. We can take $L' = \ker(\varphi)$ for summand.
- Yet another way: There exists a homomorphism $\mathbf{f} : A \to A$, with $\mathbf{f} \circ \mathbf{f} = \mathbf{f}$ and $\mathbf{f}(A) = L$.

Characterization of semisimple modules

Proposition

An **A***-module M is semisimple iff every submodule is a direct summand.*

Proof. Suppose $M = \bigoplus_{i \in I} M_i$, M_i simple, and let L be a submodule.

For each subset $J \subseteq I$, write $M_J = \bigoplus_{i \in J} M_i$. Let J be a maximum subset of I such that $L \cap M_J = 0$. We claim that

$$M = L \oplus M_J.$$

Let $i \in I \setminus J$,

$$(M_J + M_i) \cap L \neq 0 \quad \Rightarrow \quad (M_J + L) \cap M_i \neq 0$$

Thus $(M_J + L) \cap M_i = M_i$, so $M_J + A = M$.

Conversely, suppose every submodule of M is a direct summand. Note that every submodule inherits the property: If $L_0 \subset L \subset M$ and L_0 is a direct summand of M then it is also a direct summand of L.

Claim: Every nonzero submodule B of M contains a nonzero simple submodule. Let $0 \neq b \in B$ and C a maximal submodule of B such that $b \notin C$.

$$B = C \oplus D$$

Claim: D is simple. Otherwise there is $0 \neq E \subsetneq D$, and $D = E \oplus F$, and so $B = C \oplus E \oplus F$, in particular $b = c + e + f$. But then we cannot have $b \in C \oplus E$ and $b \in C \oplus F$.

Let $\{M_i : i \in I\}$ be a maximal family of simple submodules of M and such that $L = \sum_{i \in I} M_i$ is a direct sum.

Since L is a direct summand of M, $M = L \oplus B$. If B is nonzero, by the argument above, it contains a nonzero simple submodule, that contradicts the choice of I, thus

$$M = \bigoplus_{i \in I} M_i.$$

Corollary

If M is semisimple, then any submodule or factor module are semisimple.

Semisimple Rings

Theorem

Let $\mathbf{A}$ *be a ring. TFAE*

1. $\mathbf{A}$ *is left semisimple (as a module over itself);*
2. $\mathbf{A}$ *is left Artinian and* $J(\mathbf{A}) = 0$*;*
3. $\mathbf{A}$ *is left Artinian and* $I^2 \neq 0$ *for every minimal left ideal;*
4. *Every nonzero left* $\mathbf{A}$*-module is semisimple;*
5. *Every left* $\mathbf{A}$*-module is projective;*
6. *Every left* $\mathbf{A}$*-module is injective.*

A technical point

Proposition

Let $\mathbf{A}$ be a ring and I a left ideal. Then

1. *I is a direct summand iff $I = \mathbf{A}x$, $x^2 = x$.*
2. *A minimal left ideal I of $\mathbf{A}$ is a direct summand iff $I^2 \neq 0$.*

Proof. (1) If $I \oplus J = \mathbf{A}$,

$$\begin{aligned} 1 &= x + y \quad x \in I, y \in J \quad \text{so for all } z \in I \\ z &= zx + zy \quad zy \in I \cap J \quad \text{therefore } zy = 0 \end{aligned}$$

Thus $I = \mathbf{A}x$, $x^2 = x$.

Conversely, if $I = \mathbf{A}x$, $x^2 = x$, $1 = x + (1 - x)$,
$\mathbf{A} = \mathbf{A}x \oplus \mathbf{A}(1 - x)$ and $\mathbf{A}x \cap \mathbf{A}(1 - x) = 0$.

(2) If $I^2 \neq 0$ there is $x \in I$ such that $Ix \neq 0$, and therefore $\mathbf{A}x = Ix = I$ since I is minimal.
In particular, $x = zx$ for some $z \in I$. Let J be the annihilator of x, $J = \{r \in \mathbf{A} : rx = 0\}$. From $x = zx$, that is $1 - z \in J$. Thus

$$1 = z + (1 - z) \Rightarrow \quad \mathbf{A} = I + J \quad \text{and } I \cap J = I, \text{or } I \cap J = 0$$

But $J \cap I = I$ is not possible as $Ix \neq 0$. Thus

$$\mathbf{A} \;=\; I \oplus J$$

Proof of Theorem

(1) $\mathbf{A}$ is left semisimple (as a module over itself) $\Rightarrow$ (2) $\mathbf{A}$ is left Artinian and $J(\mathbf{A}) = 0$

Suppose $\mathbf{A} = \oplus_i I_i$, I_i simple left ideal. In particular

$$1 \;=\; x_1 + \cdots + x_n,$$

for finitely many indices. This shows the family $\{I_i\}$ is finite:

$$z = zx_1 + \cdots + zx_n, \quad \forall z \in \mathbf{A}$$

Thus **A** has a composition series

$$0 \subset I_1 \subset I_1 \oplus I_2 \subset \cdots \subset I_1 \oplus \cdots \oplus I_n = \mathbf{A},$$

in particular it has both chain conditions.

Moreover, if $J(\mathbf{A}) \neq 0$ it cannot be a direct summand of **A** since it is nilpotent.

(2) **A** is left Artinian and $J(\mathbf{A}) = 0 \Rightarrow$ (3) **A** is left Artinian and $I^2 \neq 0$ for every minimal left ideal

A cannot have nilpotent ideals as $J(\mathbf{A}) = 0$, thus every nonzero minimal left ideal I has $I^2 \neq 0$.

(3) **A** is left Artinian and $I^2 \neq 0$ for every minimal left ideal $\Rightarrow$ (4) Every nonzero left **A**-module is semisimple

We first show that **A** is semisimple.
If I_1 is a minimal left ideal, $\mathbf{A} = I_1 \oplus J_1$. If J_1 is simple we are done. If not, left I_2 be a nonzero minimal left ideal $\subset J_1$ (use Artinian condition). I_2 is a direct summand of J_1, $J_1 = I_2 \oplus J_2$. In this manner we get a chain $J_1 \supsetneq J_2 \supsetneq \cdots$ that must stop. The corresponding I_i give a decomposition of **A**.

For any module M there is a surjection of a free module $F = \oplus \mathbf{A} e_i \to M$. The kernel L is a submodule of the semisimple module F, so L is a direct summand and $F = L \oplus M$. It follows that M is also semisimple.

The other equivalencies uses this argument.

Consequences

Theorem

If $\mathbf{A}$ *is left Artinian then* $\mathbf{A}$ *is left Noetherian.*

Proof. If $J(\mathbf{A}) = 0$, $\mathbf{A}$ is semisimple, and as we remarked, $\mathbf{A}$ has a composition series, in particular has both chain conditions.

If $J^n = 0$ for $n > 0$, consider the tower

$$0 = J^n \subsetneq J^{n-1} \subsetneq \cdots \subsetneq J \subsetneq \mathbf{A}$$

Its factors, J^i/J^{i+1} are Artinian modules over the semisimple ring $\mathbf{A}/J$. Thus each has a composition series, whence $\mathbf{A}$ has a composition series as well.

Scholium

$\mathbf{A}$ *is left Artinian iff* $\mathbf{A}$ *is right Artinian.*

Semisimple rings versus Simple rings

Let $\mathbf{A}$ be a semisimple ring,

$$\mathbf{A} = I_1 \oplus \cdots \oplus I_n, \quad I_i \text{ minimal left ideal}$$

Proposition

Every simple left $\mathbf{A}$-module M is isomorphic to one of the ideals I_i, in particular there are only a finite number of isomorphism classes of simple left modules.

Proof. Since $\mathbf{A}M = M$, we must have $I_iM \neq 0$ for some I_i. Because M is simple, $I_iM = M$. We claim that $I_i \simeq M$. Let $m \in M$ such that $I_im \neq 0$.
Define the mapping $\varphi : I_i \to M$ by $\varphi(x) = xm$. φ is a nonzero homomorphism of left modules, and since I_i and M are simple, φ is an isomorphism.

This leads to the following relationships amongst the I_i:

1. If $I_i \simeq I_j$, then

$$I_i = I_i^2 \simeq I_i I_j = I_j = I_j^2, \quad \text{while } I_i \not\simeq I_j$$
$$I_i I_j = 0 \Rightarrow (I_j I_i)^2 = 0 \Rightarrow I_j I_i = 0 \quad \text{since } \mathbf{A} \text{ is semisimple}$$

2. We can write **A** as a direct product of semisimple rings

$$\mathbf{A} \;=\; \mathbf{A}_1 \times \cdots \times \mathbf{A}_r,$$

such that each $\mathbf{A}_k$ is semisimple and all simple $\mathbf{A}_k$-modules are isomorphic.

Simple Artin Rings

Theorem

Let $\mathbf{A}$ *be a semisimple Artin ring such that all simple left modules are isomorphic. Then* $\mathbf{A}$ *is a simple ring, that is* 0 *and* $\mathbf{A}$ *are the only two-sided ideals.*

Proof.

Let $\mathbf{A} = I_1 \oplus \cdots \oplus I_n$ be a simple decomposition of $\mathbf{A}$. We have that $I_i I_j = I_j$ for any pair I_i, I_j.

If L is a nonzero two-sided ideal, $LI_i \neq 0$ for some I_i. Since I_i is minimal, $LI_i = I_i$ and thus $I_i \subseteq L$ since L is a right ideal.

Therefore, from $I_j = I_i I_j \subset L$, and so $L = \mathbf{A}$. $\square$

Maschke's Theorem

Theorem

Let $\mathbf{G}$ *be a finite group and* $\mathbf{A} = \mathbf{K}[G]$ *its group ring over the field* $\mathbf{K}$. *Then* $\mathbf{A}$ *is semisimple iff char* $\mathbf{K}$ *does not divide* $|\mathbf{G}|$.

Proof. Suppose the order of $\mathbf{G}$ is not divisible by the characteristic of $\mathbf{K}$. We are going to argue that every left $\mathbf{A}$-module is semisimple.

- Let M be a left $\mathbf{A}$-module and L a submodule. We will prove that L is a direct summand.
- As a $\mathbf{K}$-vector subspace of M, there is direct summand decomposition $M = L \oplus L'$. Denote by $\mathbf{f} : M \to L$ the corresponding $\mathbf{K}$-homomorphism: $\mathbf{f}$ is surjective and $\mathbf{f}(m) = m$ for $m \in L$.

Maschke's Cont'd

- Now we modify $\mathbf{f}$ into a $\mathbf{A}$-linear homomorphism

$$\varphi(m) = \frac{1}{|\mathbf{G}|}\sum_{\sigma\in\mathbf{G}} \sigma^{-1}\mathbf{f}(\sigma m).$$

- If $m \in L$, as L is a submodule, $\sigma m \in L$, so $\sigma^{-1}\mathbf{f}(\sigma m) = \sigma^{-1}\sigma m = m$, and $\varphi(m) = m$.
- It is easy to verify that for any $\tau \in \mathbf{G}$ and $m \in M$,

$$\varphi(\tau m) = \tau\varphi(m),$$

and φ is $\mathbf{A}$-linear, as desired.

Maschke's Cont'd

Now suppose $|\mathbf{G}|$ is divisible by char KK. Consider the element

$$x = \sum_{\sigma \in \mathbf{G}} \sigma \neq 0$$

It satisfies

$$x^2 = |\mathbf{G}|x = 0.$$

Thus the nonzero ideal $I = \mathbf{A}x$ is nilpotent (note that x lies in the center of $\mathbf{A}$), so $\mathbf{A}$ is not semisimple.

Outline

Assignment #16

Let $\mathbf{V}$ be a finite dimensional vector space over the field $\mathbf{K}$. Prove the following assertions about the matrix ring $\mathbf{A} = \mathrm{Hom}_{\mathbf{K}}(\mathbf{V}, \mathbf{V})$:

- $\mathbf{A}$ has no two-sided ideal $\neq 0, \mathbf{A}$.
- If I is a left ideal, then there is a unique subspace $\mathbf{W}$ such that
$$I = \{\mathbf{f} \in \mathbf{A} : \mathbf{f}(w) = 0 \quad \forall w \in \mathbf{W}\}.$$
- If I is a right ideal, then there is a unique subspace $\mathbf{W}$ such that
$$I = \{\mathbf{f} \in \mathbf{A} : \mathbf{f}(v) \in \mathbf{W} \quad \forall v \in \mathbf{V}\}.$$

Outline

Wedderburn Theorem

Proposition

Let $\mathbf{A}$ *be a ring and e an idempotent such that* $\mathbf{A}e\mathbf{A} = \mathbf{A}$*. Denote by* $\mathbf{D}$ *the subring* $e\mathbf{A}e$*. Then* $M = \mathbf{A}e$ *is a right* $\mathbf{D}$*-module and*

$$\mathbf{A} \simeq \mathrm{Hom}_{\mathbf{D}}(M_{\mathbf{D}}, M_{\mathbf{D}}).$$

Proof. We define the following homomorphism $\mathbf{f} : \mathbf{A} \to \mathrm{Hom}_{\mathbf{D}}(M_{\mathbf{D}}, M_{\mathbf{D}})$: For $a \in \mathbf{A}$, and $m \in M$, $\mathbf{f}(a)(m) = am$.

1. $\mathbf{f}$ is one-to-one: Otherwise $aM = 0$ that is $a\mathbf{A}e = 0$ and therefore $a\mathbf{A}e\mathbf{A} = a\mathbf{A} = 0$, so $a = 0$ as $\mathbf{A}$ has 1.
2. $\mathbf{f}$ is onto: Since $\mathbf{A}e\mathbf{A} = \mathbf{A}$, there is an equation

$$1 = \sum_i a_i e b_i, \quad a_i, b_i \in \mathbf{A}.$$

Proof Cont'd

Thus for any $m = me \in M$ and $\varphi \in \mathrm{Hom}_{\mathbf{D}}(M, M)$, we have

$$\begin{aligned}
\varphi(m) = \varphi(1 \cdot m) &= \varphi(\sum_i a_i e b_i m) \\
&= \sum_i \varphi[(a_i e)(e b_i)(m e)] = \sum_i \varphi(a_i e)(e b_i m e) \\
&= \sum_i [\varphi(a_i e) e b_i] m \quad \text{and thus} \\
\varphi &= \mathbf{f}(\sum_i (\varphi(a_i e) e b_i)).
\end{aligned}$$

Wedderburn Theorem

Theorem

*Let **A** be a simple ring with* 1 *with a minimal left ideal* $I \neq 0$*. Then **A** is isomorphic to a matrix ring over a division ring.*

Proof. Since **A** is simple, $I^2 \neq 0$, so $I^2 = I$ since I is minimal. Thus $I = Ix$ for $x \in I$.

There is an element $z \in I$ such that $x = zx$. Thus from $z = z(1 - z) + z^2$, $z(1 - z) \in I \cap L$, L the annihilator of x. Since I is minimal, $I \cap L$ is either zero or I. In both cases we have a contradiction.

This means that I is generated by an idempotent, which we will call e. We take this ideal as M in the Proposition.

Proof of Theorem

1. We already have a ring isomorphism $\mathbf{A} \simeq \mathrm{Hom}_{\mathbf{D}}(M_{\mathbf{D}}, M_{\mathbf{D}})$, $\mathbf{D} = e\mathbf{A}e$.
2. We must prove that $e\mathbf{A}e$ is a division ring. If $0 \neq eae \in e\mathbf{A}e$, then $eae \in \mathbf{A}eeae = \mathbf{A}e$, since $\mathbf{A}e$ is minimal.
3. Therefore there is $b \in \mathbf{A}$ such that $beeae = e$, that is $ebe \cdot eae = e$, which shows that every nonzero element of $e\mathbf{A}e$ is invertible.

Outline

Hamilton Quaternions

Let **H** be the set of complex matrices of the form

$$q = \begin{bmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{bmatrix}, \quad z_1, z_2 \in \mathbb{C}.$$

To prove that **H** is a division ring, ETS:

1. **H** is a vector space over $\mathbb{R}$: clear.
2. **H** is closed under multiplication: check.
3. The axioms will follow, inherited from matrix multiplication rules, and the fact that if $0 \neq q \in$ **H** is invertible so for each such quaternion multiplication $q' \to qq'$ is surjective.

Characterization

Theorem

H *is the only non-commutative, finite dimensional division ring over* $\mathbb{R}$*.*

Proof.

- Let **D** be a division ring which is finite dimensional over $\mathbb{R}$. Let **F** a maximal commutative $\mathbb{R}$-subalgebra of **D**.
- **F** is a field, so may be identified to $\mathbb{C}$.
- View **D** as left vector space over $\mathbb{C}$, and define the linear transformation

$$\mathbf{T}(x) = xi, \quad x \in \mathbf{D}$$

- Note that $\mathbf{T}^2 = -\mathbf{I}$, so **T** is diagonalizable, of eigenvalues $\pm i$.

Proof Cont'd

- The eigenspaces are

$$\begin{aligned} \mathbf{D}^+ &= \{x \in \mathbf{D} : xi = ix\} \\ \mathbf{D}^- &= \{x \in \mathbf{D} : xi = -ix\} \end{aligned}$$

- $\mathbf{D}^+ = \mathbb{C}$. If $x, y \in \mathbf{D}^-$, $xy \in \mathbf{D}^+$.
- If $\mathbf{D}^- = 0$, $\mathbf{D} = \mathbb{C}$, which is against the hypothesis, so if $0 \neq \alpha \in \mathbf{D}^-$, multiplication by $\alpha : \mathbf{D}^- \to \mathbf{D}^+$ is an isomorphism.

- We claim that $\alpha^2 \in \mathbb{R}$ and $\alpha^2 < 0$.
- $\mathbb{R}[\alpha]$ is a field and contains α^2. Since

$$\alpha^2 \quad \in \quad \mathbb{C} \cap \mathbb{R}[\alpha] = \mathbb{R}$$

  if $\alpha^2 > 0$, α^2 would have 3 square roots in $\mathbb{R}[\alpha]$ (including two in $\mathbb{R}$).
- Therefore there is $j \in \mathbf{D}^-$ such that $j^2 = -1$.
- Now define $k = ij$. It follows that $\mathbf{D}$ has an $\mathbb{R}$-basis $\{1, i, j, k\}$, with $i^2 = j^2 = k^2 = -1$, $ij = -ji$, $jk = -kj$, $ik = -ki$, the standard relations that determine $\mathbf{H}$.

Finite Division Rings

Theorem (Wedderburn)

A finite division ring **D** *is a field.*

Proof. Let **K** be the center of **D**. **K** is a field of characteristic p and cardinality $q \geq 2$. Thus **D** is a (left) vector space over **K** so that the cardinality of **D** is q^n. We argue that $\mathbf{K} = \mathbf{D}$.

- For each $0 \neq a \in \mathbf{D}$ its centralizer $N(a) = \{x \in \mathbf{D} : xa = ax\}$ is a subdivision ring containing **K** and a.
- If $a \in \mathbf{D} \setminus \mathbf{K}$, then $N(a)*$ is the centralizer of a in the group $\mathbf{D}^*$ and

$$[\mathbf{D}^* : N(a)^*] = \frac{q^n - 1}{q^r - 1}, \quad 1 \leq r < n, \quad r | d.$$

Proof Cont'd

- By the class equation,

$$q^n - 1 = q - 1 + \sum_r \frac{q^n - 1}{q^r - 1}, \quad 1 \leq r < n, \quad r|n.$$

- For each primitive *n*root ζ of 1 in $\mathbb{C}$, $|q - \zeta| > |q - 1|$ (as $|q^2 - 1| > |q - 1|^2$) therefore $\mathbf{g}_n(q) > q - 1$ where $\mathbf{g}_n(\mathbf{x})$ is the *n*th cyclotomic polynomial.
- To contradict the class equation, for each $r < n$ that divides n, the polynomial $\mathbf{f}_r(\mathbf{x}) = \frac{\mathbf{x}^n - 1}{\mathbf{x}^r - 1}$ lies in $\mathbb{Z}[\mathbf{x}]$ and is divisible by $\mathbf{g}_r(\mathbf{x})$, with $\mathbf{f}_r(\mathbf{x}) = \mathbf{g}_r(\mathbf{x})\mathbf{h}(\mathbf{x})$, $\mathbf{h}(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$.
- Thus for each r $\mathbf{g}_r(q)$ divides $\mathbf{f}_r(q)$ in $\mathbb{Z}$, whence $\mathbf{g}_n(q)|q - 1$, a contradiction.

Outline

Assignment #17

1. Let **G** be the symmetric group S_3 and **A** the group ring $\mathbb{C}[\mathbf{G}]$. Prove that

$$\mathbb{C}[\mathbf{G}] \simeq M_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C}.$$

2. If **G** is a finite group and **K** a field, let **Z** be the center of **K**[**G**]. Find a basis of **Z** as a **K**-vector space in terms of the conjugacy classes of **G**.