PMATH 445 Course Notes

Representations of Finite Groups

Jason Bell • Fall 2021 • University of Waterloo

Table of Contents

1 September 8, 2021

We begin the course by recalling Cayley's theorem, a famous result from group theory. It states that every finite group G embeds (there exists an injective homomorphism) into a symmetric group S_n. The proof is simple: let G act on itself by left multiplication, and show that this gives an embedding of G into S_n where $n = |G|$. This result is simple, but it allows us to understand finite groups as subgroups of symmetric groups, where one has many tools to use.

In representation theory, one seeks to understand groups in terms of maps into general linear groups $\mathrm{GL}_n(F)$, where F is a field. This is generally more desirable than an embedding into a symmetric group, as we obtain the full power of linear algebra at our disposal. We will consider all homomorphisms (not just injective ones) from groups to general linear groups, and such homomorphisms are called **representations** of our group. First, we show that every finite field embeds into $\mathrm{GL}_n(F)$ for some field F.

Proposition 1.1. Let F be a field. Every finite group embeds into $\mathrm{GL}_n(F)$ for some $n \geq 1$.

Proof. Let G be a finite group. By Cayley's theorem, we have an embedding $G \hookrightarrow S_n$ where $n = |G|$. Hence, it suffices to show that S_n embeds into $\mathrm{GL}_n(F)$. Define $\varphi : S_n \to \mathrm{GL}_n(F)$ by $\psi(\sigma) = P_\sigma$, where P_σ denotes the permutation matrix. Notice that for $\sigma_1, \sigma_2 \in S_n$, we have $\varphi(\sigma_1\sigma_2) = P_{\sigma_1\sigma_2} = P_{\sigma_1}P_{\sigma_2} = \varphi(\sigma_1\sigma_2)$, so φ is a group homomorphism. One can also check that if $\varphi(\sigma) = I$, the identity matrix, then σ must be the identity permutation, so φ is injective. □

It turns out that this result is not true for infinite groups in general.

Example 1.2. Let G be the group consisting of bijective maps from $\mathbb{Z}^+$ to itself such that f fixes all but finitely integers. We claim that there does not exist a field F and $n \geq 1$ such that G embeds into $\mathrm{GL}_n(F)$.

Proof. First, we note the following fact from linear algebra.

Fact 1. If A and B are commuting diagonalizable matrices, then they are simultaneously diagonalizable. That is, there is a common change of basis that makes both matrices diagonalizable. This result also extends to families of commuting diagonalizable matrices.

Now, we denote by (i, j) the bijective mapping from $\mathbb{Z}^+$ to itself which swaps i and j and fixes all other integers. Consider the permutations $(1, 2)$, $(3, 4)$, $(5, 6)$, and so on. Note that they pairwise commute. Suppose that there exists an injective homomorphism $\varphi : G \to \mathrm{GL}_n(F)$ for some $n \geq 1$ and a field F. Let $A_1 = \varphi(1, 2)$, $A_2 = \varphi(3, 4)$, and so on. Observe that we have

$$\varphi((i, i + 1)^2) = \varphi(\mathrm{id}) = I,$$

which implies that $A_1^2 = A_2^2 = \cdots = I$. We now recall another fact from linear algebra.

Fact 2. If the minimal polynomial of a matrix has distinct roots over the (algebraically closed) field F, then the matrix is diagonalizable.

We see from above that the minimal polynomial of the A_i must divide $x^2 - 1$, since $A_i^2 - I = 0$. As $x^2 - 1$ has distinct roots, it follows from Fact 2 that all the A_i are diagonalizable. Moreover, by Fact 1, we can assume after a change of basis that each A_i is of the form

$$A_i = \begin{pmatrix} \varepsilon_{1,i} & & 0 \\ & \ddots & \\ 0 & & \varepsilon_{n,i} \end{pmatrix}$$

where $\varepsilon_{1,i}, \ldots, \varepsilon_{n,i} \in \{\pm 1\}$. Now we have a problem: there are only 2^n such matrices of the above form, and infinitely many positive integers. Thus, there exist positive integers $i < j$ such that $\varphi(A_i) = \varphi(A_j)$, so φ is not injective, and this yields our contradiction.

Note that this argument needs an adjustment for an algebraically closed field of characteristic 2, since $x^2 - 1 = (x - 1)^2$ does not have distinct roots. In such a case, we can proceed in the same way, except we use distinct 3-cycles instead of 2-cycles. □

We now turn to the notion of a group algebra.

DEFINITION 1.3. The **group algebra** of the group G over the field k is defined by

$$k[G] = \left\{ \sum_{g \in G} \alpha_g \cdot g : \alpha_g \in k,\ \alpha_g = 0 \text{ for all but finitely many } g \right\}.$$

We note that $k[G]$ is a ring with a natural addition, and multiplication given by

$$\left(\sum_{g \in G} \alpha_g \cdot g \right) \left(\sum_{h \in G} \beta_h \cdot h \right) = \sum_{y \in G} \left(\sum_{(g,h):gh=y} \alpha_j \cdot \beta_h \right) \cdot y.$$

Notice that the inner sum is finite because by definition, there are only finitely many non-zero α_g and β_h.

REMARK 1.4. We call $k[G]$ a group *algebra* because we have a "copy" of k in $k[G]$ given by $\lambda \mapsto \lambda \cdot 1_G$ for elements $\lambda \in k$, with $\lambda \cdot g = g \cdot \lambda$ for all $g \in G$. We see that $k[G]$ is a k-vector space of dimension $|G|$.

EXERCISE 1.5. Show that $\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. Fun fact: using the naive approach to multiply matrices takes $O(n^3)$ operations, but applying this fact reduces the time complexity to $O(n^{2.373})$.

We now prove a version of Cayley's theorem for group algebras.

PROPOSITION 1.6. Let G be a finite group with $n = |G|$. Then G embeds into $\mathrm{GL}_n(k[G])$.

PROOF. Let G act on $k[G]$ by left multiplication. That is, for $g \in G$, define

$$L_g : k[G] \to k[G] : \sum_{h \in G} \alpha_h \cdot h \mapsto \sum_{h \in G} \alpha_h \cdot (g \cdot h).$$

Observe that for $g_1, g_2 \in G$, we have

$$L_{g_1} \circ L_{g_2}(x) = L_{g_1}(L_{g_2}(x)) = L_{g_1}(g_2 \cdot x) = g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x = L_{g_1 g_2}(x).$$

For the second equality, we can think of G as sitting inside $k[G]$ by identifying $g \in G$ with $1 \cdot g \in k[G]$, so we simply have multiplication in the group algebra. Hence, we see that the map $L : G \to \mathrm{GL}_n(k[G]) : g \mapsto L_g$ is a group homomorphism. Finally, if L_g is the identity matrix, then $g \cdot x = x$ for all $x \in k[G]$. This implies that $g \cdot 1 = 1$ and so $g = 1$, so $\ker L = \{1\}$. Thus, L is injective and is the desired embedding. □

Later in the course, we will prove the following important theorem. In short, it states that if G is a finite group and k is an algebraically closed field of characteristic zero, then $k[G]$ is isomorphic to a finite direct product of matrix rings over k. The isomorphism and these matrix rings will completely determine the representation of the group G.

THEOREM 1.7. Let G be a finite group and let k be an algebraically closed field of characteristic zero. Then we have

$$k[G] \cong \prod_{i=1}^{s} M_{n_i}(k),$$

where

(1) s is the number of conjugacy classes of G;

(2) $n_1^2 + n_2^2 + \cdots + n_s^2 = |G|$;

(3) $|\{i : n_i = 1\}| = |G/G'|$, where G' denotes the commutator subgroup; and

(4) $n_i \mid |G|$ for all $1 \leq i \leq s$.

As a corollary of this theorem, one can prove Exercise 1.5 by noting that $\mathbb{C}[S_3]$ has three conjugacy classes: $\{(1)\}$, $\{(12),(13),(23)\}$, and $\{(123),(132)\}$.

To finish off the lecture, we give one more interesting linear algebra fact.

FACT. If $q = p^j$ where p is prime and $j \geq 1$, then

$$|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

It is not hard to see why. Let A be an invertible $n \times n$ matrix, and note that A must have linearly independent columns. For the first column, say v_1, we have $q^n - 1$ choices as we can pick any vector except the zero vector. For the second column, we can choose any vector except those in the span of v_1, which yields $q^n - q$ choices. One can repeat this argument to obtain the result.

2 September 10, 2021

Recall that for a ring R, the **center** of R is the set

$$Z(R) = \{z \in R : zr = rz \text{ for all } r \in R\}.$$

Note that $Z(R)$ is a commutative subring of R. We can also write $[z, r] = 0$ to denote that $zr = rz$.

DEFINITION 2.1. Let k be a field. We say that R is a **k-algebra** if

(a) R is a ring; and

(b) there exists a homomorphism $\phi : k \to Z(R)$ sending 1_k to 1_R (we assume that ϕ is injective).

Notice that if we identify k with $\phi(k) \subseteq R$, we have a "copy" of k in R. This means that R is a k-vector space in addition to being a ring.

DEFINITION 2.2. Let k be a field, and let R and S be k-algebras. A **k-algebra homomorphism** is a ring homomorphism $\psi : R \to S$ such that $\psi(\lambda) = \lambda$ for all $\lambda \in k$.

We also have the notion of a module. A module over a ring is a generalization of a vector space over a field.

DEFINITION 2.3. A **(left) R-module** M is an abelian group $(M, +)$ equipped with a map

$$\cdot : R \times M \to M$$

such that for all $r, s \in R$ and $m, n \in M$, we have

(a) $(r + s) \cdot m = r \cdot m + s \cdot m$;

(b) $r \cdot (m + n) = r \cdot m + r \cdot n$;

(c) $(r \cdot s) \cdot m = r \cdot (s \cdot m)$; and

(d) $1 \cdot m = m$.

EXAMPLE 2.4. Let $R = M_n(\mathbb{C})$ and $M = \mathbb{C}^{n \times 1}$, the set of column vectors of length n. One can check that M is a (left) R-module equipped with the operation of matrix-vector multiplication.

EXAMPLE 2.5. Left ideals are R-modules by left multiplication. In particular, R itself is a left R-module. If L is a left ideal of R (and we write $L \trianglelefteq_\ell R$), then L is a submodule of R as a left R-module.

REMARK 2.6. If M_1 and M_2 are R-modules, we define the set

$$\mathrm{Hom}_R(M_1, M_2) = \{f : M_1 \to M_2 \mid f \text{ is } R\text{-linear}\}.$$

That is, we have $f(r \cdot m_1 + m_2) = r \cdot f(m_1) + f(m_2)$ for all $r \in R$ and $m_1, m_2 \in M_1$. In the case that $M_1 = M_2 = M$, we write

$$\mathrm{Hom}_R(M_1, M_2) = \mathrm{End}_R(M),$$

the endomorphisms from M to itself. Note that $\mathrm{End}_R(M)$ is a ring with composition as the multiplication operation, as the set of linear transformations from a vector space to itself forms a ring.

FACT. If R is a k-algebra and M is a left R-module, then M is a k-vector space.

In a sense, this is clear. We know that M already has scalar multiplication by R, and we have a copy of k sitting inside of R, so if we restrict R to k, we obtain scalar multiplication by k.

DEFINITION 2.7. A left R-module M is **simple** if $M \neq (0)$, and (0) and M are the only submodules of M.

EXAMPLE 2.8. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/p\mathbb{Z}$ for a prime p. Suppose that $N \subseteq M$ is a submodule with $N \neq (0)$. Then there exists $i \in \{1, \ldots, p-1\}$ such that the coset $[i]_p$ is in N. But this implies that $[i]_p^{-1} \cdot [i]_p = [1]_p \in N$. It follows that $N = \mathbb{Z}/p\mathbb{Z}$ and hence M is simple.

EXERCISE 2.9. Let $R = M_n(\mathbb{C})$ and $M = \mathbb{C}^{n \times 1}$. Show that M is simple. (Hint: If we are given a non-zero vector, then we can extend it to a basis, and we can always find a linear transformation to send a basis wherever we like.)

DEFINITION 2.10. A left ideal L of R is a **maximal left ideal** if

(a) $L \subsetneq R$; and

(b) there does not exist a left ideal L' such that $L \subsetneq L' \subsetneq R$.

EXERCISE 2.11. Let R be a non-zero ring (that is, $0_R \neq 1_R$). If L is a proper left ideal of R, then there exists a maximal left ideal M such that $L \subseteq M$. In particular, taking $L = (0)$ shows that a maximal left ideal always exists.

FACT. If R is a ring and M is a simple left R-module, then M is isomorphic to R/L (as R-modules), where L is a maximal left ideal.

We give a sketch of the proof of this fact. First, pick $m_0 \in M \setminus \{0\}$. Consider R as a left R-module over itself (by left multiplication), and define

$$\begin{aligned} \Phi : R &\to M \\ r &\mapsto r \cdot m_0. \end{aligned}$$

(1) Check that Φ is an R-module homomorphism.

(2) Show that $\ker \Phi = L$ is a left ideal.

(3) Show that $\mathrm{im}\, \Phi$ is a non-zero submodule of M, and hence must be equal to M (as M is simple).

By the first isomorphism theorem, it follows that $R/\ker \Phi = R/L$ is isomorphic to $M = \mathrm{im}\, \Phi$.

Finally, why must L be maximal? Similarly to the correspondence for groups and rings, we also have correspondence for modules. Indeed, for a module M and a submodule $N \trianglelefteq M$, there is a bijection between the submodules of M/N and the submodules of M that contain N.

We have the canonical projection

$$\begin{aligned} \pi : M &\to M/N \\ m &\mapsto m + N. \end{aligned}$$

For a submodule Q of M/N, notice that

$$\pi^{-1}(Q) = \{m \in M : \pi(m) \in Q\}$$

is a submodule of M which contains N, since

$$N = \pi^{-1}(0) \subseteq \pi^{-1}(Q).$$

Now, there is a correspondence between submodules of M and the left ideals of R containing L. Since M is simple, it has two submodules. Thus, there are two left ideals of R containing L, namely L and R. Therefore, there is no ideal L' such that $L \subsetneq L' \subsetneq R$, so L is maximal.

As a corollary of the above fact, we obtain the following.

COROLLARY 2.12. If R is a finite dimensional k-algebra and M is a simple left R-module, then M is a finite dimensional k-vector space.

PROOF. We showed that there was a surjection $\Phi : R \to M : r \mapsto r \cdot m_0$ for $m_0 \neq 0$. The fact that Φ is an R-module homomorphism implies that it is k-linear, as there is a copy of k sitting inside of R. Since R is finite dimensional, it follows that M is also finite dimensional. □

For the remainder of this lecture, we will turn to proving Schur's lemma.

DEFINITION 2.13. A **division ring** Δ is a ring in which every non-zero element $a \in \Delta$ has a multiplicative inverse $b \in \Delta$ (that is, $ab = ba = 1$).

EXAMPLE 2.14. Consider the quaternions

$$\mathbb{H} = \{a + ib + jc + kd : a, b, c, d \in \mathbb{R}\}$$

with properties $i^2 = j^2 = k^2 = 1$, $ij = k$, and $ji = -k$. Check that $\mathbb{H}$ is a division ring, but not a field.

THEOREM 2.15 (Schur's lemma). Let R be a ring and let M be a simple left R-module. Then $\mathrm{End}_R(M)$ is a division ring.

PROOF. We already know that $\mathrm{End}_R(M)$ is a ring, so we only need to show that every non-zero element has an inverse. Let $0 \neq f \in \mathrm{End}_R(M)$, which is a linear map $f : M \to M$. Notice that $\ker f$ is a submodule of M. Since M is simple, $\ker f$ is either (0) or M. The latter is impossible as this would mean that $f = 0$, so we have $\ker f = (0)$, so f is injective. Similarly, $\operatorname{im} f$ is a submodule of M and $\operatorname{im} f \neq (0)$ since $f \neq 0$, so $\operatorname{im} f = M$ since M is simple. This shows that f is surjective. Therefore, f has a set theoretic inverse g. We now show that $g \in \mathrm{End}_R(M)$; that is,

$$g(r \cdot m_1 + m_2) = r \cdot g(m_1) + g(m_2)$$

for all $r \in R$ and $m_1, m_2 \in M$. But f is bijective, so this is equivalent to showing that

$$f(g(r \cdot m_1 + m_2)) = f(r \cdot g(m_1) + g(m_2)).$$

This is indeed the case; we have

$$f(g(r \cdot m_1 + m_2)) = r \cdot m_1 + m_2 = r \cdot f \circ g(m_1) + f \circ g(m_2) = f(r \cdot g(m_1) + g(m_2)).$$ □

3 September 13, 2021

Recall the setting from before: we had a ring R, a simple left R-module M, and $\Delta := \mathrm{End}_R(M)$, which we showed was a division ring.

Proposition 3.1.

(a) If R is a k-algebra for a field k, then $\Delta := \mathrm{End}_R(M)$ is also a k-algebra.

(b) If k is algebraically closed and R is a finite-dimensional k-algebra, then $\Delta \cong k$.

Proof.

(a) For each $\lambda \in k$, define the map

$$\begin{aligned} \Phi_\lambda : M &\to M, \\ \lambda &\mapsto \lambda \cdot m. \end{aligned}$$

By $\lambda \cdot m$, we mean that we have a copy $k \subseteq Z(R) \subseteq R$, and M is an R-module and hence a k-vector space. Note that

$$\begin{aligned} \Phi_\lambda(r \cdot m_1 + m_2) &= \lambda \cdot (r \cdot m_1 + m_2) \\ &= \lambda \cdot r \cdot m_1 + \lambda \cdot m_2 \\ &= r \cdot \lambda \cdot m_1 + \lambda \cdot m_2 && (\text{since } k \subseteq Z(R)) \\ &= r \cdot \Phi_\lambda(m_1) + \Phi_\lambda(m_2). \end{aligned}$$

Therefore, Φ_λ is R-linear and so $\Phi_\lambda \in \mathrm{End}_R(M)$. However, it is not enough to show that each Φ_λ is in $\Delta = \mathrm{End}_R(M)$. We also require that our map $\lambda \mapsto \Phi_\lambda$ is a map $k \to Z(\Delta)$; in other words, we also need $\Phi_\lambda \in Z(\Delta)$. Let $\psi \in \Delta$, and observe that

$$\Phi_\lambda \circ \psi(m) = \lambda \cdot \psi(m) = \psi(\lambda \cdot m) = \psi \circ \Phi_\lambda(m),$$

where the second equality is because the R-linearity of ψ implies k-linearity.

(b) Recall that if R is a finite dimensional k-algebra, then M is a finite dimensional k-vector space (see Corollary 2.12). Suppose that $\dim_k M =: n < \infty$. Then we have

$$\begin{aligned} \Delta = \mathrm{End}_R(M) &\subseteq \mathrm{End}_k(M) && (R\text{-linearity imposes more conditions than } k\text{-linearity}) \\ &\cong \mathrm{End}_k(k^n) && (M \text{ is an } n\text{-dimensional } k\text{-vector space}) \\ &\cong M_n(k) && (k\text{-linear maps } k^n \to k^n \text{ are the } n \times n \text{ matrices}) \end{aligned}$$

and thus $\dim_k \Delta = m \leq n^2 < \infty$ for some $m \in \mathbb{Z}$.

We now show that $\Delta \cong k$. Indeed, pick $a \in \Delta$. Notice that a commutes with all elements of k since $k \subseteq Z(\Delta)$, where we can identify k with the set $\{\Phi_\lambda : \lambda \in k\}$. Consider

$$k \subseteq k(a) \subseteq \Delta,$$

where $k(a)$ is the field formed from adjoining a to k; it is a field because Δ is a division ring and hence a is invertible. Thus, $\dim_k k(a) \leq \dim_k \Delta = m < \infty$. Therefore, $\{1, a, a^2, \ldots, a^m\}$ is a linearly dependent set over k, so there exist elements $c_0, c_1, \ldots, c_m \in k$, not all zero, such that

$$c_0 + c_1 a + \cdots + c_m a^m = 0.$$

But k is algebraically closed, so $a \in k$. This implies that $\Delta \subseteq k$, and hence $\Delta \cong k$. □

Exercise 3.2. Let Δ be a division ring and let M be a left Δ-module. Then M has a basis $B \subseteq M$. That is, there do not exist $\delta_1, \ldots, \delta_m \in \Delta$ such that

$$\delta_1 b_1 + \cdots + \delta_m b_m = 0$$

for distinct $b_1, \ldots, b_m \in B$, and for all $m \in M$, we can write

$$m = \sum_{b \in B} \delta_b b$$

where $\delta_b = 0$ for all but finitely many $b \in B$. (Hint: Use Zorn's lemma.)

For this reason, instead of calling it a left Δ-module, we can call it a **left Δ-vector space**.

REMARK 3.3. Let R be a ring, let M be a simple left R-module, and let $\Delta = \mathrm{End}_R(M)$. Then M is a left Δ-vector space.

PROOF. Recall that $\delta \in \Delta$ is an R-linear map from M to itself. We can consider the operation

$$\begin{aligned} \Delta \times M &\to M, \\ (\delta, m) &\mapsto \delta \cdot m := \delta(m). \end{aligned}$$

It is straightforward to see that

- $(\delta_1 + \delta_2) \cdot m = \delta_1 \cdot m + \delta_2 \cdot m$,
- $\delta \cdot (m_1 + m_2) = \delta \cdot m_1 + \delta \cdot m_2$,
- $\delta \cdot (\delta \cdot m) = (\delta_1 \cdot \delta_2) \cdot m$, and
- $\mathrm{id} \cdot m = m$,

so M is a left Δ-vector space. □

EXAMPLE 3.4. Let $R = M_n(\mathbb{C})$ and recall that $M = \mathbb{C}^{n\times 1}$ is a simple left R-module. We have

$$\Delta = \mathbb{C} = \{\Phi_\lambda : \lambda \in \mathbb{C}\},$$

where each $\Phi_\lambda(m) = \lambda \cdot m$ for each $\lambda \in \mathbb{C}$. One can show that $\Phi(Av) = A \cdot \Phi(v)$ for all $A \in M_n(\mathbb{C})$ and $v \in \mathbb{C}^{n\times 1}$ only when $\Phi = \Phi_\lambda$ for some $\lambda \in \mathbb{C}$.

We now state the Jacobson Density Theorem, which we will prove in the next lecture.

THEOREM 3.5 (Jacobson Density Theorem). Let R be a ring, let M be a simple left R-module, and let $\Delta = \mathrm{End}_R(M)$. Then we have a ring $\mathrm{End}_\Delta(M)$ and a map

$$\begin{aligned} \Phi : R &\to \mathrm{End}_\Delta(M) \\ r &\mapsto \Phi_r : M \to M \\ &\qquad m \mapsto r \cdot m. \end{aligned}$$

Moreover, we have the following properties.

(1) The map Φ is a ring homomorphism and if R is a k-algebra, then Φ is a k-algebra homomorphism.

(2) The kernel of Φ is the annihilator of M; that is,

$$\ker \Phi = \{r \in R : r \cdot m = 0 \text{ for all } m \in M\}.$$

(3) **Density:** If $m_1, \ldots, m_n \in M$ are left linearly independent over Δ and $w_1, \ldots, w_n \in M$ are arbitrary elements, then there exists $r \in R$ such that

$$\Phi_r(m_i) = w_i$$

for all $1 \le i \le n$ (in particular, we can send finite linear combinations wherever we like).

For now, let's see why the maps Φ_r are Δ-linear so that $\Phi_r \in \mathrm{End}_\Delta(M)$ for each $r \in R$. Let $\delta \in \Delta$ and $m_1, m_2 \in M$. Then we have

$$\begin{aligned} \Phi_r(\delta \cdot m_1 + m_2) &= r \cdot (\delta \cdot m_1 + m_2) \\ &= r \cdot (\delta \cdot m_1) + r \cdot m_2 && \text{(multiplication by } R \text{ is linear)} \\ &= r \cdot \delta(m_1) + r \cdot m_2 && \text{(we have } \delta \in \Delta) \\ &= \delta(r \cdot m_1) + r \cdot m_2 && (\delta \text{ is an } R\text{-linear map}) \\ &= \delta \cdot \Phi_r(m_1) + \Phi_r(m_2), \end{aligned}$$

so Φ_r is Δ-linear as desired.

4 September 15, 2021

We now prove the Jacobson Density Theorem, which we stated in the previous lecture. Recall that R is a ring, M is a simple left R-module, and $\Delta = \mathrm{End}_R(M)$. We already showed that $\mathrm{End}_\Delta(M)$ is a ring, and we defined the map

$$\begin{aligned} \Phi : R &\to \mathrm{End}_\Delta(M) \\ r &\mapsto \Phi_r : M \to M \\ &\qquad m \mapsto r \cdot m. \end{aligned}$$

Proof of the Jacobson Density Theorem.

(1) First, observe that for all $r_1, r_2 \in R$ and $m \in M$, we have

$$\begin{aligned} \Phi(r_1 r_2)(m) &= \Phi_{r_1 r_2}(m) \\ &= (r_1 \cdot r_2) \cdot m \\ &= r_1 \cdot (r_2 \cdot m) \\ &= r_1 \cdot \Phi_{r_2}(m) \\ &= \Phi_{r_1} \circ \Phi_{r_2}(m) \\ &= \Phi(r_1) \circ \Phi(r_2)(m). \end{aligned}$$

Similarly, one can show that $\Phi(r_1 + r_2) = \Phi(r_1) + \Phi(r_2)$ and $\Phi(1) = \mathrm{id}_M$, so Φ is a ring homomorphism. Moreover, if R is a k-algebra, then we can identify k with the set $\{\Phi_\lambda : \lambda \in k\}$, so we have a copy of k in $Z(\Delta)$.

(2) Notice that

$$\begin{aligned} r \in \ker \Phi &\iff \Phi_r : M \to M \text{ is the zero map} \\ &\iff \Phi_r(m) = 0 \text{ for all } m \in M \\ &\iff r \cdot m = 0 \text{ for all } m \in M, \end{aligned}$$

where the last equivalence follows since we defined Φ_r to be left multiplication by r.

(3) We will proceed by induction on n. For $n = 1$, linear independence just means that $m_1 \neq 0$. For arbitrary $w_1 \in R$, we need to show that there exists $r \in R$ such that $\Phi_r(m_1) = r \cdot m_1 = w_1$. Let

$$N = \{s \cdot m_1 : s \in R\} \subseteq M,$$

which is an R-submodule of M. Notice that $N \neq (0)$ since $m_1 \neq 0$. Since M is simple, we must have $N = M$. In particular, we see that $w_1 \in N$, so there exists $r \in R$ such that $r \cdot m_1 = w_1$.

Assume the result holds for $1 \leq k \leq n-1$ where $n \geq 2$. Let $m_1, \ldots, m_n$ be linearly independent over Δ, and let $w_1, \ldots, w_n \in M$ be arbitrary. We wish to find $r \in R$ such that $r \cdot m_i = w_i$ for all $1 \leq i \leq n$.

By the induction hypothesis, there exists $a \in R$ such that

$$a \cdot m_i = w_i$$

for all $1 \leq i \leq n-1$. However, we don't know that $a \cdot m_n = w_n$, so we will set $a \cdot m_n =: w \in M$.

Claim. There exists $r \in R$ such that

$$r \cdot m_1 = \cdots = r \cdot m_{n-1} = 0$$

and $r \cdot m_n =: w' \neq 0$.

To complete the proof, it is enough to prove this claim. To see why, suppose we know the claim holds. We know from the base case that we can send w' wherever we like; in particular, there exists $b \in R$ such that $b \cdot w' = w_n - w$. Notice that we have

$$(a + b \cdot r) \cdot m_i = \begin{cases} w_i & \text{if } 1 \leq i \leq n-1, \\ w + (w_n - w) & \text{if } i = n. \end{cases}$$

Thus, choosing $a + b \cdot r \in R$ does the trick.

Proof of Claim. Suppose that no such $r \in R$ exists. In particular, if

$$r \cdot m_1 = \cdots = r \cdot m_{n-1} = 0,$$

then this will force $r \cdot m_n = 0$ as well. For $a_1, \ldots, a_{n-1} \in M$, we know by the induction hypothesis that there exists $s \in R$ such that

$$s \cdot m_i = a_i$$

for all $1 \leq i \leq n-1$. We can define the map $\theta : M^{n-1} \to M$ by

$$\theta(a_1, \ldots, a_{n-1}) = s \cdot m_n.$$

Is this well-defined? We know such an s exists, but we aren't guaranteed that it is unique. Suppose that $s_1, s_2 \in R$ are such that

$$a_i = s_1 \cdot m_i = s_2 \cdot m_i$$

for all $1 \leq i \leq n-1$. Then

$$(s_1 - s_2) \cdot m_i = a_i - a_i = 0$$

for all $1 \leq i \leq n-1$, and by our assumption above, we obtain

$$(s_1 - s_2) \cdot m_n = 0.$$

This means that $s_1 \cdot m_n = s_2 \cdot m_n$, so even if the choice of s is not unique, the map θ is well-defined. We now show that θ is R-linear. For $b \in R$, we have

$$\begin{aligned} \theta(b \cdot (a_1, \ldots, a_n)) &= \theta(b \cdot (s \cdot m_1, \ldots, s \cdot m_{n-1})) \\ &= \theta(b \cdot s \cdot (m_1, \ldots, m_{n-1})) \\ &= (b \cdot s) \cdot m_n \\ &= b \cdot (s \cdot m_n) \\ &= b \cdot \theta(s \cdot (m_1, \ldots, m_{n-1})) \\ &= b \cdot \theta(a_1, \ldots, a_{n-1}). \end{aligned}$$

Addition follows from the module structure, and we leave it as an exercise.

For $1 \leq j \leq n-1$, we define the canonical inclusion maps

$$\begin{aligned} i_j : M &\to M^{n-1} \\ m &\mapsto (0, \ldots, 0, m, 0, \ldots, 0), \end{aligned}$$

where m is placed in the j-th coordinate. It is easy to see that the i_j are R-linear. We have

$$M \xrightarrow{i_j} M^{n-1} \xrightarrow{\theta} M$$

where i_j and θ are both R-linear, so we have

$$\delta_j := \theta \circ i_j \in \Delta = \mathrm{End}_R(M).$$

Now, we obtain

$$\begin{aligned}\delta_1 \cdot m_1 + \cdots + \delta_{n-1} \cdot m_{n-1} &= \delta_1(m_1) + \cdots + \delta_{n-1}(m_{n-1}) \\ &= \theta \circ i_1(m_1) + \cdots + \theta \circ i_{n-1}(m_{n-1}) \\ &= \theta(i_1(m_1) + \cdots + i_{n-1}(m_{n-1})) \\ &= \theta(m_1, \ldots, m_{n-1}) \\ &= \theta(1 \cdot m_1, \ldots, 1 \cdot m_{n-1}) \\ &= 1 \cdot m_n \\ &= m_n.\end{aligned}$$

This implies that $m_1, \ldots, m_n$ are left linearly dependent over Δ, which is a contradiction. Therefore, the claim holds, and the result follows by induction. □

5 September 17, 2021

Note that if M is finite-dimensional as a Δ-vector space, then the map Φ from the Jacobson Density Theorem is surjective. To see why, take a basis $\{m_1, \ldots, m_n\}$ for M as a Δ-vector space. If $f \in \mathrm{End}_\Delta(M)$, there exist elements $w_1, \ldots, w_n \in M$ such that $f(m_i) = w_i$ for all $1 \leq i \leq n$. But by the Jacobson Density Theorem, there exists $r \in R$ such that $r \cdot m_i = w_i$ for all $1 \leq i \leq n$. Note that a linear transformation is completely determined by where the basis is sent, so $f = \Phi_r$.

Recall that by (2) in the Jacobson Density Theorem, we have

$$\ker \Phi = \mathrm{Ann}_R(M) := \{r \in R : r \cdot m = 0 \text{ for all } m \in M\}.$$

Definition 5.1. A left R-module M is called **faithful** if $\mathrm{Ann}_R(M) = (0)$.

From above, we see that M is faithful if and only if Φ is injective.

Definition 5.2. A ring R is said to be **primitive** if it has a faithful simple module.

Putting our above observations together, we obtain the following result.

Corollary 5.3. If R has a faithful simple left R-module M such that $\dim_\Delta M < \infty$ where $\Delta = \mathrm{End}_R(M)$, then the map

$$\Phi : R \to \mathrm{End}_\Delta(M)$$

from the Jacobson Density Theorem is an isomorphism.

Proof. The assumption $\dim_\Delta(M) < \infty$ gives surjectivity, and since M is faithful, Φ is also injective. □

Corollary 5.4. If k is an algebraically closed field, R is a finite-dimensional k-algebra, and M is a faithful simple left R-module, then $R \cong M_n(k)$ where $n = \dim_k(M)$.

Proof. By Proposition 3.1, we know that $\Delta = \mathrm{End}_R(M) \cong k$. Moreover, we showed that $\dim_k M = n < \infty$ in Corollary 2.12. Therefore, we see that

$$\begin{aligned} R &\cong \mathrm{End}_\Delta(M) && \text{(by Corollary 5.3)} \\ &\cong \mathrm{End}_k(M) && \text{(since } \Delta \cong k\text{)} \\ &\cong \mathrm{End}_k(k^n) && \text{(M is an n-dimensional k-vector space)} \\ &\cong M_n(k) && \text{(k-linear maps $k^n \to k^n$ are the $n \times n$ matrices)}\end{aligned}$$

which completes the proof. □

Definition 5.5. Let R be a ring. We say that R is **left Artinian** if every descending chain of left ideals of R terminates. That is, for a chain of left ideals

$$L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots$$

of R, there exists $n \geq 1$ such that $L_n = L_m$ for all $m \geq n$.

Example 5.6.

(1) We see that $\mathbb{Z}$ is not left Artinian since we can take the chain of ideals

$$2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq \cdots .$$

(2) Intuitively, $M_n(\mathbb{C})$ is left Artinian since it is an n^2-dimensional $\mathbb{C}$-vector space, so for a chain of ideals

$$L_1 \supsetneq L_2 \supsetneq L_3 \supsetneq \cdots ,$$

the dimension must eventually decrease, so the chain terminates.

(3) Similarly, $\mathbb{Z}/6000\mathbb{Z}$ is left Artinian as it only has finitely many subsets, so the sizes of the ideals in a descending chain must decrease.

We can generalize our observations from the previous example. We leave the proof as an exercise.

Remark 5.7.

(1) If R is a finite-dimensional k-algebra, then R is left Artinian.

(2) If R is a finite ring, then R is left Artinian.

Definition 5.8. Let R be a ring. Let I be a two-sided ideal of R. We say that I is a **nil ideal** if for every $x \in I$, there exists $n = n(x) \geq 1$ such that $x^n = 0$ (that is, every element in I is nilpotent).

Example 5.9.

(1) Let R be any ring. Then (0) is a nil ideal.

(2) Let $R = \mathbb{Z}/2\mathbb{Z}$. Then $I = 6R = \{[0]_R, [6]_R\}$ is a nil ideal since $[0]_R^1 = [0]_R$ and $[6]_R^2 = [36]_R = [0]_R$.

(3) Let R be the ring of 2×2 upper triangular matrices over $\mathbb{C}$; that is,

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C}).$$

Then one can check that

$$I = \left\{ \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} : \alpha \in \mathbb{C} \right\}$$

is an ideal of R, and that it is a nil ideal (by squaring).

We now state the Artin-Wedderburn Theorem and give some remarks.

Theorem 5.10 (Artin-Wedderburn). Let R be a left Artinian ring. If R has no non-zero nil ideals, then there exists $s \geq 1$, division rings $D_1, \ldots, D_s$, and integers $n_1, \ldots, n_s \geq 1$ such that

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s).$$

Remark 5.11.

(1) If k is an algebraically closed field and R is a finite-dimensional k-algebra, then

$$R \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k).$$

(2) By using Exercise 3 on Assignment 1, we see that if R is also finite, then

$$R \cong M_{n_1}(\mathbb{F}_{q_1}) \times \cdots \times M_{n_s}(\mathbb{F}_{q_s}).$$

This can be observed by noting that if R is finite, then the division rings must also be finite.

(3) If R is also commutative, then

$$R \cong F_1 \times \cdots \times F_s$$

for fields $F_1, \ldots, F_s$. This is because commutativity forces the matrix rings to be 1×1. Moreover, the division rings must also be commutative, and so they are fields.

We finish the lecture by giving one last definition.

DEFINITION 5.12. Let R be a ring. Then a proper two-sided ideal P is called a **prime ideal** if whenever $a, b \in R$ are such that $aRb = \{arb : r \in R\} \subseteq P$, we either have $a \in P$ or $b \in P$. We say that R is a **prime ring** if (0) is a prime ideal of R.

EXAMPLE 5.13. Observe that $p\mathbb{Z}$ for a prime p is a prime ideal of $\mathbb{Z}$. Indeed, if $a, b \in \mathbb{Z}$ are such that $a\mathbb{Z}b = ab\mathbb{Z} \subseteq p\mathbb{Z}$, then $p \mid ab$. This occurs if and only if $p \mid a$ or $p \mid b$, or equivalently, $a \in p\mathbb{Z}$ or $b = p\mathbb{Z}$. In fact, $\mathbb{Z}$ is a prime ring as it has (0) as a prime ideal.

6 September 20, 2021

When R is commutative, notice that R is prime if and only if R is an integral domain. Indeed, observe that

$$\begin{aligned} R \text{ is prime} &\iff aRb = (0) \text{ implies } a = 0 \text{ or } b = 0 \\ &\iff abR = (0) \text{ implies } a = 0 \text{ or } b = 0 \\ &\iff ab \cdot 1 = 0 \text{ implies } a = 0 \text{ or } b = 0 \\ &\iff ab = 0 \text{ implies } a = 0 \text{ or } b = 0 \\ &\iff R \text{ is an integral domain.} \end{aligned}$$

Being prime can be thought of as an extension of being an integral domain in the case where R is not a commutative ring.

DEFINITION 6.1. A ring R is **simple** if (0) and R are its only two-sided ideals.

PROPOSITION 6.2. If R is a simple ring, then R is prime.

PROOF. Let R be simple. Suppose that $aRb = (0)$ with $a \neq 0$ and $b \neq 0$. Since $a \neq 0$, the two-sided ideal

$$RaR := \{u_1 a v_1 + \cdots + u_s a v_s : s \geq 0,\, u_i, \ldots, u_s, v_1, \ldots, v_s \in R\}$$

is equal to R by the simplicity of R. In particular, there exists $s \geq 1$ and $u_s, v_1, \ldots, v_s \in R$ such that

$$1 = u_1 a v_1 + \cdots + u_s a v_s. \tag{6.1}$$

Similarly, there exists $t \geq 1$ and $y_1, \ldots, y_t, z_1, \ldots, z_t \in R$ such that

$$1 = y_1 b z_1 + \cdots + y_t a z_t. \tag{6.2}$$

Multiplying equations (6.1) and (6.2) together gives

$$1 \cdot 1 = (u_1 a v_1 + \cdots + u_s a v_s)(y_1 b z_1 + \cdots + y_t a z_t) = \sum_{i=1}^{s} \sum_{j=1}^{t} u_i (a v_i y_j b) z_j = 0,$$

where the last equality is because $aRb = (0)$ and thus $a v_i y_j b = 0$ for any $1 \leq i \leq s$ and $1 \leq j \leq t$. □

PROPOSITION 6.3. Let D be a division ring and let $n \geq 1$. Then $M_n(D)$ is simple and hence prime.

PROOF. Let I be a non-zero ideal of $M_n(D)$. We want to show that $I = M_n(D)$. Since I is non-zero, there exists a matrix

$$x = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in I$$

with each $a_{ij} \in D$ and $a_{i_0 j_0} \neq 0$ for some $1 \leq i_0, j_0 \leq n$. For all $1 \leq i, j \leq n$, let e_{ij} be the matrix where the (i,j)-th entry is 1 and all other entries are 0. Then we find that

$$e_{ii_0} x e_{j_0 j} = a_{i_0 j_0} e_{ij} \in I.$$

Since D is a division ring, we know that $a_{i_0 j_0}$ has an inverse. It follows that

$$\begin{pmatrix} a_{i_0 j_0}^{-1} & & 0 \\ & \ddots & \\ 0 & & a_{i_0 j_0}^{-1} \end{pmatrix} a_{i_0 j_0} e_{ij} = e_{ij} \in I$$

for all $1 \leq i, j \leq n$. In particular, we obtain

$$e_{11} + \cdots + e_{nn} = 1 \in I,$$

so we conclude that $I = M_n(D)$ and hence $M_n(D)$ is simple. □

We now prove a nice characterization of left Artinian rings.

PROPOSITION 6.4. Let R be a ring. Then R is left Artinian if and only if whenever S is a non-empty collection of left ideals of R, then S has a minimal element with respect to inclusion.

PROOF. For the forward direction, suppose that R is left Artinian. Let S be a non-empty collection of left ideals of R. Pick $L_1 \in S$. If L_1 is minimal, we are done. Otherwise, we can pick $L_2 \in S$ such that $L_2 \subsetneq L_1$. We can continue this process, and since R is left Artinian, this terminates at some step L_n as we cannot have an infinite strictly descending chain.

For the converse, assume that for every non-empty collection S of left ideals of R, then S has a minimal element with respect to inclusion. Let $L_1 \supseteq L_2 \supseteq \cdots$ be a descending chain of left ideals of R. Let $S = \{L_1, L_2, \dots\}$. By assumption, there exists $n \geq 1$ such that L_n is a minimal element of S. In particular, we have $L_n = L_m$ for all $m \geq n$, so R is left Artinian. □

The next theorem will be a key step towards proving the Artin-Wedderburn theorem.

THEOREM 6.5. Let R be a prime left Artinian ring. Then $R \cong M_n(D)$ for some $n \geq 1$ and division ring D. (In fact, the converse is also true.)

PROOF. Let $S = \{Ru : u \in R,\, u \neq 0\}$ be a collection of left ideals of R. Note that S is non-empty since $R \cdot 1 = R \in S$. Then there exists a minimal element in S by Proposition 6.4, say Rb for some $b \in R$. Notice that Rb is a left R-module (since left ideals are left R-modules).

First, we show that $M = Rb$ is simple. If $N \subsetneq M = Rb$ is a proper left ideal with $N \neq (0)$, then there exists $u \neq 0$ in N such that

$$(0) \subsetneq Ru \subsetneq N \subsetneq M.$$

But we assumed that $M = Rb$ was minimal in S, which is a contradiction.

Next, we show that $M = Rb$ is faithful; that is, $\mathrm{Ann}_R(M) = (0)$. Suppose there exists $a \neq 0$ in $\mathrm{Ann}_R(M)$. Then we have $aM = (0)$ and hence $aRb = (0)$. Since R is prime, it must be that $a = 0$ or $b = 0$. But we assumed that $a \neq 0$ and $b \neq 0$, so this is a contradiction.

Now, we show that $\dim_\Delta M < \infty$ where $\Delta = \mathrm{End}_R(M)$. Suppose to the contrary that M were an infinite-dimensional left Δ-vector space. Then there exist elements $m_1, m_2, \cdots \in M$ that are Δ-linearly independent. By the Jacobson Density Theorem, for every $n \geq 1$, there exists $r_n \in R$ such that

$$r_n m_1 = r_n m_2 = \cdots = r_n m_{n-1} = 0$$

and $r_n m_n \neq 0$. Define the left ideal

$$L_i = \{r \in R : rm_1 = rm_2 = \cdots = rm_i = 0\}$$

for all $i \geq 1$. Notice that $L_1 \supseteq L_2 \supseteq \cdots$ and $r_n \in L_{n+1} \setminus L_n$, which implies that these are proper containments. But this is an infinite descending chain of left ideals, which contradicts the fact that R is left Artinian.

In the next lecture, we will finish off the proof of this theorem. □

7 September 22, 2021

Definition 7.1. Let S be a ring. The **opposite ring** S^{op} of S is defined to be another ring with the same elements and addition as S, but the multiplication $* : S^{\mathrm{op}} \times S^{\mathrm{op}} \to S^{\mathrm{op}}$ is given by

$$s_1 * s_2 := s_2 \cdot s_1,$$

where $\cdot$ denotes the multiplication in S.

Remark 7.2.

(1) If S is commutative, then S^{op} is the same as S (since $*$ is the same as $\cdot$).

(2) If Δ is a division ring, then Δ^{op} is also a division ring. Indeed, let $a \in \Delta^{\mathrm{op}}$ be non-zero. Then there exists $b \in \Delta$ such that $a \cdot b = b \cdot a = 1_\Delta$, so we have $b * a = a * b = 1_{\Delta^{\mathrm{op}}}$. Hence, a is invertible.

Exercise 7.3. Let Δ be a division ring. If M is an n-dimensional left Δ-vector space, then $\mathrm{End}_\Delta(M) \cong M_n(\Delta^{\mathrm{op}})$. Note that if $\Delta = k$ for a field k, then this is just saying that $\mathrm{End}_k(M) \cong M_n(k)$, which is a familiar fact.

Hint: Construct the map $\Psi : \mathrm{End}_\Delta(M) \to M_n(\Delta^{\mathrm{op}})$ as follows: pick a basis $\{m_1, \ldots, m_n\}$ as a left Δ-vector space. For $f \in \mathrm{End}_\Delta(M)$, we have

$$f(m_j) = \sum_{i=1}^{n} a_{ij} m_i$$

where $a_{ij} \in \Delta$ since f is Δ-linear. Define $\Psi(f) := (a_{ij})$, and show that $\Psi(f \circ g) = \Psi(g) \cdot \Psi(f) = \Psi(f) * \Psi(g)$.

Last time, we were proving Theorem 6.5, which stated that if R is a prime left Artinian ring, then $R \cong M_n(D)$ for some $n \geq 1$ and division ring D. We can now finish the proof.

We can set $n := \dim_\Delta M$ as we showed that M is a finite-dimensional left Δ-vector space. Then we have

$$R \cong \mathrm{End}_\Delta(M) \cong M_n(\Delta^{\mathrm{op}})$$

by Exercise 7.3, and we are done since $D = \Delta^{\mathrm{op}}$ is a division ring. □

Corollary 7.4. Let k be an algebraically closed field, and let R be a prime finite-dimensional k-algebra. Then $R \cong M_n(k)$.

Proof. Since R is a finite-dimensional k-algebra, it is left Artinian (see Remark 5.7). Moreover, Proposition 3.1 shows that $\Delta = \mathrm{End}_R(M) \cong k$ where M is a simple left R-module, since k is algebraically closed. □

For the rest of the lecture, we will consider the connection between prime ideals and nil ideals.

Definition 7.5. We define the **spectrum** of a ring R to be the set of all prime ideals of R, denoted $\mathrm{Spec}(R)$.

Example 7.6. For $R = \mathbb{Z}$, we have $\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} : p \text{ prime}\} \cup \{(0)\}$.

Example 7.7. For $R = M_n(\Delta)$ for Δ a division ring, we have $\mathrm{Spec}(M_n(\Delta)) = \{(0)\}$ as we showed that $M_n(\Delta)$ is a simple ring in Proposition 6.3.

Example 7.8. For $R = \mathbb{C}[x, y]$, we have

$$\mathrm{Spec}(\mathbb{C}[x, y]) = \{(0)\} \cup \{(f) : f \text{ irreducible}\} \cup \{(x - a, y - b) : a, b \in \mathbb{C}\}.$$

Note that (0) is a prime ideal as $\mathbb{C}[x, y]$ is an integral domain. Every maximal ideal of $\mathbb{C}[x, y]$ is of the form $(x - a, y - b)$, and this is due to the Nullstellensatz which we will prove. The other prime ideals are generated by irreducible polynomials f.

Theorem 7.9 (Nullstellensatz). Let $\mathfrak{M}$ be a maximal ideal of $\mathbb{C}[x_1, \ldots, x_n]$. Then there exist $a_1, \ldots, a_n \in \mathbb{C}$ such that

$$\mathfrak{M} = (x_1 - a_1, \ldots, x_n - a_n).$$

Proof. Let $F = \mathbb{C}[x_1, \ldots, x_n]/\mathfrak{M}$, which is a field because $\mathfrak{M}$ is maximal. Note that $F \supseteq \mathbb{C}$. Moreover, we have $\dim_{\mathbb{C}} F \leq \aleph_0$ since $\mathbb{C}[x_1, \ldots, x_n]$ has a basis $\{x_1^{i_1} \cdots x_n^{i_n} : i_1, \ldots, i_n \geq 0\} \cong \mathbb{N}^n$, which is countable.

We claim that F is algebraic over $\mathbb{C}$. That is, if $t \in F$, then F satisfies $p(t) = 0$ for some $p(x) \in \mathbb{C}[x] \setminus \{0\}$. Note that this implies $F = \mathbb{C}$ since $\mathbb{C}$ is algebraically closed.

Let $t \in F \setminus \mathbb{C}$. Consider the set

$$S = \left\{ \frac{1}{t - \lambda} : \lambda \in \mathbb{C} \right\} \subseteq F.$$

Then S is linearly dependent since $\mathbb{C}$ is uncountable while $\dim_{\mathbb{C}} F \leq \aleph_0$. Thus, there exist distinct elements $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ and $c_1, \ldots, c_n \in \mathbb{C}$, not all zero, such that

$$\frac{c_1}{t - \lambda_1} + \cdots + \frac{c_n}{t - \lambda_n} = 0.$$

Multiplying by $\prod_{i=1}^n (t - \lambda_i)$ gives

$$\sum_{i=1}^n c_i \prod_{j \neq i} (t - \lambda_j) = p(t) = 0,$$

where $p(x)$ is a polynomial in $\mathbb{C}[x]$. Note that $p(x)$ is non-trivial since

$$p(\lambda_i) = c_i \prod_{j \neq i} (\lambda_i - \lambda_j) \neq 0.$$

This proves the claim, so $\mathbb{C}[x_1, \ldots, x_n]/\mathfrak{M} \cong \mathbb{C}$. Hence, there is a homomorphism

$$\phi : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$$

such that $\ker \phi = \mathfrak{M}$. Letting $a_i = \phi(x_i)$ for all $1 \leq i \leq n$, we have

$$\phi(x_1^{i_1} \cdots x_n^{i_n}) = a_1^{i_1} \cdots a_n^{i_n}$$

as ϕ is a homomorphism. Since the $x_1^{i_1} \cdots x_n^{i_n}$ form a basis for $\mathbb{C}[x_1, \ldots, x_n]$, it then follows that ϕ is simply the evaluation at $(a_1, \ldots, a_n)$ map. In particular, $\mathfrak{M} = (x_1 - a_1, \ldots, x_n - a_n)$ as desired. □

Theorem 7.10. Let R be a ring. Then the intersection of all prime ideals

$$\bigcap_{P \in \mathrm{Spec}(R)} P$$

is a nil ideal of R.

PROOF. Let $N = \bigcap_{P \in \mathrm{Spec}(R)} P$. Suppose that there exists some $x \in N$ which is not nilpotent, and let

$$\mathcal{T} = \{1, x, x^2, x^3, \dots\}.$$

Notice that $0 \notin \mathcal{T}$ since x is not nilpotent. Let

$$S = \{I \trianglelefteq R : I \cap \mathcal{T} = \varnothing\}.$$

We have $(0) \in S$, so S is non-empty. We leave it as an exercise to show that S has a maximal element P.

We claim that P is a prime ideal. Suppose otherwise, so that there exists $a, b \notin P$ such that $aRb \subseteq P$. Since $a \notin P$, we have $RaR + P \supsetneq P$, and similarly, $RbR + P \supsetneq P$ as $b \notin P$. As P is maximal in S, this implies that $RaR + P \notin S$, so there exists $i \geq 1$ such that $x^i \in RaR + P$. Analogously, we have $RbR + P \notin S$, so there exists $j \geq 1$ such that $x^j \in RbR + P$. It follows that

$$x^{i+j} = x^i \cdot x^j \in (RaR + P)(RbR + P) \subseteq R(aRb)R + P \subseteq P.$$

But this is a contradiction since $P \in S$ implies that $P \cap \mathcal{T} = \varnothing$, but we have $x^{i+j} \in P \cap \mathcal{T}$. Thus, P is a prime ideal, proving the claim.

Now, we find that $x \in N \subseteq P$ since P is prime and N is the intersection of all the prime ideals. However, $x \in \mathcal{T}$, which again contradicts the fact that $P \cap \mathcal{T} = \varnothing$. We conclude that every $x \in N$ must be nilpotent, so N is a nil ideal, as required. □

8 September 24, 2021

We almost have all the tools we need to prove the Artin-Wedderburn theorem. First, we make a remark and prove a couple of results that we need.

REMARK 8.1. If R is a left Artinian ring, then so is R/P where P is an ideal of R by correspondence. Moreover, if P is a prime ideal, then R/P is a prime ring. The converse of this holds when R is commutative.

LEMMA 8.2. Let R be a left Artinian ring.

(1) Every prime ideal of R is a maximal ideal.

(2) There are only finitely many prime ideals of R.

(3) Let $P_1, \dots, P_s$ be all the prime ideals of R. Then for all $i = 1, \dots, s$, we have

$$P_i + \bigcap_{j \neq i} P_j = R.$$

PROOF.

(1) Let P be a prime ideal of R. By Remark 8.1, R/P is a prime left Artinian ring and hence

$$R/P \cong M_n(D)$$

for a division ring D and some $n \geq 1$ by Theorem 6.5. We know that $M_n(D)$ is simple by Proposition 6.3, so its only ideals are (0) and $M_n(D)$. In particular, R/P is also simple. By correspondence, there are only two ideals of R that contain P. We already know that P and R are ideals that contain P, so they are in fact all of them. Thus, P is maximal.

(2) Suppose towards a contradiction that we have infinitely many distinct prime ideals $P_1, P_2, \dots$ of R. Recall that if I and J are ideals of R, we define

$$IJ = \left\{ \sum_{k=1}^{s} i_k j_k : s \geq 1,\ i_k \in I,\ j_k \in J \right\}.$$

We have a descending chain of ideals

$$P_1 \supseteq P_1P_2 \supseteq P_1P_2P_3 \supseteq \cdots$$

and since R is left Artinian, this chain must terminate. Thus, there exists $n \geq 1$ such that

$$P_1 \cdots P_n = P_1 \cdots P_nP_{n+1} \subseteq P_{n+1}.$$

Since $P_1 \neq P_{n+1}$ and P_1 is a maximal ideal by (1), there exists some element $a_1 \in P_1 \setminus P_{n+1}$. Similarly, for all $i = 1, \ldots, n$, there exists $a_i \in P_i \setminus P_{n+1}$. Then, we see that

$$(a_1R)(a_2R)(a_3R)\cdots(a_{n-1}R)a_n \subseteq P_1P_2P_3\cdots P_n \subseteq P_{n+1},$$

so we have

$$a_1Ra_2R\cdots a_{n-1}Ra_n \subseteq P_{n+1}. \tag{8.1}$$

Since neither a_1 nor a_2 are in P_{n+1}, there exists $r_1 \in R$ such that $a_1r_1a_2 \notin P_{n+1}$. This is because P_{n+1} is a prime ideal of R, so $a_1, a_2 \notin P_{n+1}$ implies that $a_1Ra_2 \nsubseteq P_{n+1}$. By (8.1), we find that

$$(a_1Ra_2)Ra_3R\cdots a_{n-1}Ra_n \subseteq P_{n+1}.$$

Now, a_1ra_2 and a_3 are both not in P_{n+1}, so there exists $r_2 \in R$ such that $a_1r_1a_2r_2a_3 \notin P_{n+1}$ since P_{n+1} is a prime ideal. Continuing in this manner, we have elements $r_1, r_2, \ldots, r_{n-1} \in R$ such that

$$a_1r_1a_2r_2\cdots a_{n-1}r_{n-1}a_n \notin P_{n+1},$$

which contradicts (8.1) since

$$a_1r_1a_2r_2\cdots a_{n-1}r_{n-1}a_n \in a_1Ra_2R\cdots a_{n-1}Ra_n.$$

We conclude that R must have finitely many prime ideals.

(3) Let $P_1, \ldots, P_s$ be the prime ideals of R, and fix $1 \leq i \leq s$. We claim that

$$I_i := P_i + \bigcap_{j \neq i} P_j = R.$$

Notice that $P_i \subseteq I_i \subseteq R$. Since P_i is a maximal ideal by part (1), we either have $I_i = P_i$ or $I_i = R$. Suppose towards a contradiction that $I_i = P_i$, and recall the fact that $I + J = I$ if and only if $J \subseteq I$. Then we have

$$\bigcap_{j \neq i} P_j \subseteq P_i,$$

which implies that

$$P_1P_2\cdots P_{i-1}P_{i+1}\cdots P_s \subseteq \bigcap_{j \neq i} P_j \subseteq P_i.$$

Using the same argument as the proof of (2), we can show that $P_1P_2\cdots P_{i-1}P_{i+1}\cdots P_s$ cannot be contained in the prime ideal P_i as each ideal P_j with $j \neq i$ is prime. This contradicts our assumption that $I_i = P_i$, so we must have $I_i = R$. □

THEOREM 8.3 (Sun-tzu). Let R be a ring, and let $I_1, \ldots, I_s$ be two-sided ideals of R such that

(i) $\bigcap_{j=1}^{s} I_j = (0)$, and

(ii) for all $i = 1, \ldots, s$, we have $I_i + \bigcap_{j \neq i} I_j = R$.

Then we have

$$R \cong \prod_{i=1}^{s} R/I_i.$$

PROOF. For $i = 1, \ldots, s$, we have a canonical surjection

$$\begin{aligned} \pi_i : R &\to R/I_i \\ r &\mapsto r + I_i, \end{aligned}$$

which is a ring homomorphism. We define

$$\begin{aligned} \Psi : R &\to R/I_1 \times \cdots \times R/I_s \\ r &\mapsto (\pi_1(r), \ldots, \pi_s(r)). \end{aligned}$$

Note that since $\pi_1, \ldots, \pi_s$ are ring homomorphisms, Ψ is also a ring homomorphism. We now show that Ψ is an isomorphism. Notice that

$$\ker \Psi = \{r \in R : \Psi(r) = 0\} = \{r \in R : \pi_1(r) = \cdots = \pi_s(r) = 0\} = \bigcap_{j=1}^{s} I_j = (0)$$

where the last equality follows from (i), so Ψ is injective. Now, fix $1 \leq i \leq s$. By (ii), we have

$$I_i + \bigcap_{j \neq i} I_j = R,$$

so we can find $a_i \in I_i$ and $b_i \in \bigcap_{j \neq i} I_j$ such that $a_i + b_i = 1$. We can write $b_i = 1 - a_i$, so we find that

$$\pi_i(b_i) = \pi_i(1) - \pi_i(a_i) = (1 + I_i) - (0 + I_i) = 1 + I_i$$

since $a_i \in I_i$. On the other hand, when $n \neq i$, we have $b_i \in \bigcap_{j \neq i} I_j \subseteq I_n$, which gives $\pi_n(b_i) = 0 + I_n$. It follows that

$$\begin{aligned} \Psi(b_i) &= (\pi_1(b_i), \pi_2(b_i), \ldots, \pi_i(b_i), \ldots, \pi_s(b_i)) \\ &= (0 + I_1, 0 + I_2, \ldots, 0 + I_{i-1}, 1 + I_i, 0 + I_{i+1}, \ldots, 0 + I_s). \end{aligned}$$

Therefore, given $r_1, \ldots, r_s \in R$, we have $r = r_1 b_1 + \cdots + r_s b_s \in R$, and we see that

$$\Psi(r) = \Psi(r_1 b_1 + \cdots + r_s b_s) = \Psi(r_1 + I_1, \ldots, r_s + I_s).$$

We conclude that Ψ is surjective, so it is an isomorphism, as required. □

THEOREM 8.4 (Artin-Wedderburn). Let R be a left Artinian ring. If R has no nonzero nil ideals, then there exists $s \geq 1$, division rings $D_1, \ldots, D_s$, and integers $n_1, \ldots, n_s \geq 1$ such that

$$R \cong \prod_{i=1}^{s} M_{n_i}(D_i).$$

PROOF. Let R be a left Artinian ring with no nonzero nil ideals. We showed in Lemma 8.1 that R has finitely many prime ideals; call them $P_1, \ldots, P_s$. Moreover, observe that $\bigcap_{j=1}^{s} P_j$ is a nil ideal by Theorem 7.10, and since R has no nonzero nil ideals, it must be that $\bigcap_{j=1}^{s} P_j = (0)$. We also showed that $P_i + \bigcap_{j \neq i} P_j = R$ for all $i = 1, \ldots s$ in Lemma 8.2. It follows from Sun-tzu that

$$R \cong \prod_{i=1}^{s} R/P_i.$$

We know that R/P_i is a prime left Artinian ring by Remark 8.1, so Theorem 6.5 implies that $R/P_i \cong M_{n_i}(D_i)$ for some $n_i \geq 1$ and division ring D_i. Thus, we conclude that

$$R \cong \prod_{i=1}^{s} R/P_i \cong \prod_{i=1}^{s} M_{n_i}(D_i).$$ □

9 September 27, 2021

Let's first look at a corollary of Sun-tzu (Theorem 8.3).

REMARK 9.1. Let k be a field. If R is a k-algebra, then each canonical surjection $\pi_i : R \to R/I_i$ in the proof of Sun-tzu is a k-algebra homomorphism, which means that the map $\Psi : R \to R/I_1 \times \cdots \times R/I_s$ is also a k-algebra homomorphism.

COROLLARY 9.2. Let k be an algebraically closed field, and let R be a finite-dimensional k-algebra with no nonzero nil ideals. Then we have

$$R \cong \prod_{i=1}^{s} M_{n_i}(k)$$

for some $s \geq 1$ and integers $n_1, \ldots, n_s \geq 1$.

PROOF. Since R is a finite-dimensional k-algebra, we see that R is left Artinian (Remark 5.7). Hence, R has only finitely many prime ideals (Lemma 8.2), say $P_1, \ldots, P_s$. Moreover, since R has no nonzero nil ideals, we have $\bigcap_{j=1}^{s} P_j = (0)$ (Theorem 7.10), and $P_i + \bigcap_{j \neq i} P_j = R$ for all $i = 1, \ldots, s$ since R is left Artinian (Lemma 8.2). By Sun-tzu, we have

$$R \cong R/P_1 \times \cdots \times R/P_s.$$

Then, since k is algebraically closed and each R/P_i is a prime finite-dimensional k-algebra, Corollary 7.4 implies that

$$R \cong R/P_1 \times \cdots \times R/P_s \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k). \qquad \square$$

Now that we have the Artin-Wedderburn theorem in our toolkit, we can finally get started with some representation theory. Let G be a finite group with $|G| = n$, and let k be an algebraically closed field. Recall that $V := k[G]$ is the group algebra of the group G over the field k, with $\dim_k k[G] = |G| = n$. Moreover, we have the embedding

$$\Phi : k[G] \to \mathrm{End}_k(V) \cong M_n(k),$$

where we send each $g \in G$ to the left multiplication map

$$\begin{aligned} L_g : V &\to V \\ x &\mapsto g \cdot x \end{aligned}$$

and extend linearly over k. We call this the **left regular representation** of G.

Next, let's recall some linear algebra. Let W be a vector space with basis $\mathcal{B} = \{w_1, \ldots, w_n\}$, and let $T : W \to W$ be a linear map. Then we can define a matrix $[T]_{\mathcal{B}}$ by setting $[T]_{\mathcal{B}} = (c_{ij})$ where

$$Tw_j = \sum_{i=1}^{n} c_{ij} w_i.$$

Observe that the trace of T is given by

$$\mathrm{Tr}(T) = \sum_{j=1}^{n} c_{jj},$$

which is the sum of the coefficients of w_j in Tw_j (and this is independent of the basis $\mathcal{B}$).

Now, for the map $L_g : V \to V$ with $g \in G$, what is $\mathrm{Tr}(L_g)$? First, note that the elements of G form a basis over $V = k[G]$; that is, we have $\mathcal{B} = \{g_1, \ldots, g_n\} = G$ in this case. Observe that

$$L_g(g_i) = g \cdot g_i = 1 \cdot g \cdot g_i + \sum_{h \in G \setminus \{gg_i\}} 0 \cdot h. \tag{9.1}$$

For $j = 1, \ldots, n$, the coefficient of g_j in gg_j is 1 if $g = 1$, and 0 if $g \neq 1$. Indeed, if $g \neq 1$, then g_j would be different than gg_j, so it would have coefficient 0 in equation (9.1). This implies that

$$\mathrm{Tr}(L_g) = \sum_{j=1}^{n} \begin{cases} 1 & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases} = \begin{cases} n & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$$

THEOREM 9.3 (Maschke). Let k be a field (not necessarily algebraically closed), and let G be a finite group. If $\mathrm{char}(k) \nmid |G|$, then $k[G]$ has no nonzero nil ideals.

PROOF. Suppose towards a contradiction that $k[G]$ has a nonzero nil two-sided ideal N. Pick a nonzero element

$$x = \sum_{g \in G} \alpha_g g \in N.$$

Since x is nonzero, there exists some $g_0 \in G$ such that $\alpha_{g_0} \neq 0$. As N is an ideal of $k[G]$, we also have $x \cdot g_0^{-1} \in N$. The coefficient of 1 in $x \cdot g_0^{-1}$ is $\alpha_{g_0} \neq 0$. Thus, we can assume without loss of generality that $x = \sum_{g \in G} \alpha_g g \in N$ has $\alpha_1 \neq 0$.

Let $A \in M_n(k)$ be nilpotent so that $A^n = 0$. Let v be an eigenvector of A with eigenvalue λ. Then we have

$$Av = \lambda v \implies A^2 v = \lambda^2 v \implies \cdots \implies A^n v = \lambda^n v,$$

which implies that $\lambda = 0$ since $A^n = 0$. In particular, $\mathrm{Tr}(A)$ is the sum of the eigenvalues of A (with multiplicity), and the above argument shows that all the eigenvalues of A are 0, so $\mathrm{Tr}(A) = 0$.

Now, consider the injective k-algebra homomorphism

$$\Phi : k[G] \to \mathrm{End}_k(V) \cong M_n(k) : \sum_{g \in G} \beta_g \cdot g \mapsto \sum_{g \in G} \beta_g \cdot L_g$$

we discussed at the beginning of this lecture (the left regular representation of G). We had an element

$$x = \sum_{g \in G} \alpha_g g \in N$$

with $\alpha_1 \neq 0$. Note that x is nilpotent since N is a nil ideal; say $x^j = 0$ for some $j \geq 1$. Then we have

$$\Phi(x)^j = \Phi(x^j) = \Phi(0) = 0,$$

so $\Phi(x)$ is also nilpotent. Our discussion above implies that $\mathrm{Tr}(\Phi(x)) = 0$. However, we also see that

$$\mathrm{Tr}(\Phi(x)) = \mathrm{Tr}\left(\sum_{g \in G} \alpha_g \cdot L_g \right) = \sum_{g \in G} \alpha_g \cdot \mathrm{Tr}(L_g) = |G| \cdot \alpha_1 \neq 0$$

since $\alpha_1 \neq 0$ and $\mathrm{char}(k) \nmid |G|$. This is a contradiction, so $k[G]$ has no nonzero nil ideals. □

REMARK 9.4. Question 1 of Assignment 1 shows that the converse of Maschke's theorem also holds. Indeed, we proved that if $\mathrm{char}(k) \mid |G|$, then $k[G]u$ is a nonzero nil ideal where $u = \sum_{g \in G} g$.

COROLLARY 9.5. Let k be an algebraically closed field, and let G be a finite group. If $\mathrm{char}(k) \nmid |G|$, then there exists $s \geq 1$ and integers $n_1, \ldots, n_s \geq 1$ such that

$$k[G] \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k).$$

PROOF. By Maschke's theorem, we know that $k[G]$ has no nonzero nil ideals, and it is left Artinian as it is a finite-dimensional k-algebra. Since k is algebraically closed, it follows that

$$k[G] \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k)$$

for some $s \geq 1$ and integers $n_1, \ldots, n_s \geq 1$ by Corollary 9.2. □

This corollary is important because this gives us a nice relationship between $k[G]$, which is something intrinsic to the group G, and the direct product of matrix rings, which is more in the realm of linear algebra.

10 September 29, 2021

By Corollary 9.5, we know that if k is algebraically closed, G is a finite group, and $\mathrm{char}(k) \nmid |G|$, then

$$k[G] \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k)$$

for some $s \geq 1$ and integers $n_1, \ldots, n_s \geq 1$. This will be our setting for this lecture, and we'll derive more properties about the choice of $s \geq 1$ and the integers $n_1, \ldots, n_s \geq 1$.

THEOREM 10.1. We have $|G| = n_1^2 + \cdots + n_s^2$.

PROOF. The isomorphism in Corollary 9.5 is a k-algebra isomorphism, so we find that

$$\begin{aligned} |G| &= \dim_k k[G] \\ &= \dim_k M_{n_1}(k) \times \cdots \times M_{n_s}(k) \\ &= \dim_k M_{n_1}(k) + \cdots + \dim_k M_{n_s}(k) \\ &= n_1^2 + \cdots + n_s^2. \end{aligned}$$

□

Next, we'll work towards showing that s is the number of conjugacy classes of G.

REMARK 10.2. If R is a k-algebra, then $Z(R)$ is also a k-algebra. Indeed, we have an embedding $k \hookrightarrow Z(R) \subseteq R$ which sends 1_k to 1_R, and this also gives us an embedding $k \hookrightarrow Z(Z(R)) = Z(R)$.

REMARK 10.3. If $T_1, \ldots, T_s$ are rings, then

$$Z(T_1 \times \cdots \times T_s) = Z(T_1) \times \cdots \times Z(T_s).$$

PROPOSITION 10.4. We have $Z(M_n(k)) = kI_n = \{\lambda I_n : \lambda \in k\}$.

PROOF. We'll give two proofs: an elementary one, and a high level one.

For the elementary proof, suppose that $(a_{ij}) \in Z(M_n(k))$. Then observe that

$$\begin{aligned} \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix} &= \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \\ &= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}. \end{aligned}$$

In particular, we have $a_{21} = \cdots = a_{n1} = 0$ and $a_{12} = \cdots = a_{1n} = 0$, which shows that

$$A = \left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

for some smaller matrix A'. The argument follows inductively.

For a high level proof (where k is algebraically closed), take $R = M_n(k)$ and consider the simple left R-module

$$M = k^{n\times 1} = \left\{ \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} : \lambda_1, \dots, \lambda_n \in k \right\}.$$

We have shown that $\Delta = \mathrm{End}_R(M) \cong k$ by identifying each $\lambda \in k$ with the map

$$\begin{aligned} \Phi_\lambda : M &\to M \\ v &\mapsto \lambda \cdot v. \end{aligned}$$

Now, if $A \in Z(M_n(k))$, then the map

$$\begin{aligned} f : M &\to M \\ v &\mapsto Av \end{aligned}$$

is R-linear; indeed, for $B \in M_n(k) = R$ and $v_1, v_2 \in M$, we have

$$\begin{aligned} f(Bv_1 + v_2) &= A(Bv_1 + v_2) \\ &= ABv_1 + Av_2 \\ &= BAv_1 + Av_2 \\ &= Bf(v_1) + f(v_2). \end{aligned}$$

In particular, we see that $f \in \Delta$, so $f = \Phi_\gamma$ for some $\gamma \in k$. Then $f(v) = Av = \gamma v$ for all $v \in M$, which implies that $A = \gamma I$. □

Combining Proposition 10.4 with Remark 10.3, we see that

$$\begin{aligned} Z(M_{n_1}(k) \times M_{n_s}(k)) &= Z(M_{n_1}(k)) \times \cdots \times Z(M_{n_s}(k)) \\ &= \{(\lambda_1 I_{n_1}, \dots, \lambda_s I_{n_s}) : (\lambda_1, \dots, \lambda_s) \in k^s\}. \end{aligned}$$

In particular, we have $\dim_k Z(k[G]) = \dim_k Z(M_{n_1}(k) \times \cdots \times M_{n_s}(k)) = s$.

Definition 10.5. We say that a function $\alpha : G \to k$ is a **class function** if α is constant when restricted to each conjugacy class of G.

Lemma 10.6. Let $\alpha : G \to k$ be a function. Then $z := \sum_{g\in G} \alpha(g)g$ is central in $k[G]$ if and only if α is a class function.

Proof. Note that $z \in \sum_{g\in G} \alpha(g)g$ is in $Z(k[G])$ if and only if $xz = zx$ for all $x \in G$; the backwards direction here is because G forms a basis for $k[G]$. This occurs if and only if $z = x^{-1}zx$ for all $x \in G$ by rearranging. Now, this is equivalent to

$$\sum_{g\in G} \alpha(g)g = x^{-1}\left(\sum_{g\in G} \alpha(g)g\right)x = \sum_{g\in G} \alpha(g)x^{-1}gx = \sum_{h\in G} \alpha(xhx^{-1})h$$

holding for all $x \in G$, where the last equality follows from making the substitution $h = x^{-1}gx$. This is true if and only if the coefficient of the left-hand side is the same as the coefficient of the right-hand side. That is, $\alpha(h) = \alpha(xhx^{-1})$ for all $h \in G$ and $x \in G$, and this is exactly the definition of a class function. □

Let G be a finite group, and let $\mathcal{C}_1, \dots, \mathcal{C}_s$ be the conjugacy classes of G. For $i = 1, \dots, s$, observe that

$$\alpha(g) = \begin{cases} 1 & \text{if } g \in \mathcal{C}_i \\ 0 & \text{if } g \notin \mathcal{C}_i \end{cases}$$

is a class function. Then the elements

$$z_i = \sum_{g \in G} \alpha(g) g = \sum_{g \in \mathcal{C}_i} g$$

for $i = 1, \ldots, s$ are central by Lemma 10.6.

PROPOSITION 10.7. Let G be a finite group with conjugacy classes $\mathcal{C}_1, \ldots, \mathcal{C}_s$. Then the elements

$$z_i := \sum_{g \in \mathcal{C}_i} g$$

for $i = 1, \ldots, s$ form a basis for $Z(k[G])$.

PROOF. We have already seen that the z_i are central. To show linear independence, suppose that

$$c_1 z_1 + \cdots + c_s z_s = 0,$$

where we take 0 to mean $\sum_{g \in G} 0 \cdot g$ in $k[G]$. If $g \in \mathcal{C}_i$, then the coefficient of g on the left-hand side is c_i. But the coefficient on the right-hand side is always 0, so $c_1 = \cdots = c_s = 0$. To see that $\{z_1, \ldots, z_s\}$ spans $Z(k[G])$, recall that $z \in \sum_{g \in G} \alpha(g) g \in Z(k[G])$ if and only if α is a class function. Let β_i be the unique value of α on $\mathcal{C}_i$. Then we see that

$$z = \sum_{g \in G} \alpha(g) g = \sum_{i=1}^{s} \sum_{g \in \mathcal{C}_i} \alpha(g) g = \sum_{i=1}^{s} \beta_i \sum_{g \in \mathcal{C}_i} g = \sum_{i=1}^{s} \beta_i z_i,$$

so we can write z as a linear combination of the z_i, completing the proof. □

THEOREM 10.8. In the setting of Corollary 9.5, s is the number of conjugacy classes of G.

PROOF. We previously showed that $\dim_k Z(k[G]) = \dim_k Z(M_{n_1}(k) \times \cdots \times M_{n_s}(k)) = s$. Proposition 10.7 tells us that $\dim_k Z(k[G])$ is the number of conjugacy classes of G. □

For the remainder of the lecture, we recall the abelianization of a group G. We denote by G' the commutator (or derived) subgroup of G, which is the smallest subgroup of G which contains all elements of the form $ghg^{-1}h^{-1}$ with $g, h \in G$ (which we call commutators).

Note that G/G' is abelian. Indeed, take $g, h \in G$ so that $gG', hG' \in G/G'$. Observe that

$$(h^{-1})(g^{-1})(h^{-1})^{-1}(g^{-1})^{-1} = h^{-1}g^{-1}hg \in G',$$

so we have

$$(gG')(hG') = ghG' = gh(h^{-1}g^{-1}hg)G' = hgG' = (hG')(gG').$$

For this reason, we call G/G' the **abelianization** of G.

EXERCISE 10.9. Show that G/G' has the universal property that if A is abelian group, $\phi : G \to A$ is a group homomorphism, and $\pi : G \to G/G'$ is the canonical quotient map, then there is a unique group homomorphism $\Phi : G/G' \to A$ such that $\Phi \circ \pi = \phi$.