# PMATH 445 Course Notes

Representations of Finite Groups

Jason Bell • Fall 2021 • University of Waterloo

## Table of Contents


1 Embeddings and group algebras (09/08/2021) 3

2 $k$-algebras, modules, and Schur's lemma (09/10/2021) 5

3 Endomorphism ring, Jacobson density theorem (09/13/2021) 9

4 Proof of the Jacobson density theorem (09/15/2021) 12

5 Faithful and simple modules, left Artinian rings (09/17/2021) 14

6 Simple rings, characterization of left Artinian rings (09/20/2021) 17

7 Opposite ring, spectrum of a ring, Nullstellensatz (09/22/2021) 19

8 Sun-tzu, the Artin-Wedderburn theorem (09/24/2021) 22

9 Corollary of Sun-tzu, Maschke's theorem (09/27/2021) 25

10 Class functions, abelianization of a group (09/29/2021) 27

11 Applications of the big theorem, representations (10/01/2021) 31

12 Direct sums, decompositions of modules (10/04/2021) 34

13 Number of inequivalent irreducible representations (10/06/2021) 37

14 Semisimple rings and a characterization (10/08/2021) 39

15 Uniqueness of decompositions, characters (10/18/2021) 42

16 Character tables, an "inner product" of maps (10/20/2021) 45

17 Orthogonality of characters over "inner product" (10/22/2021) 48

18 Orthonormality of characters over "inner product" (10/25/2021) 52

19 Character tables of $S_4$ and $S_5$ (10/27/2021) 55

20 Algebraic numbers and algebraic integers (10/29/2021) 61

21 Degree of irreps divide order of the group (11/01/2021) 64

22 Burnside's theorem (11/03/2021) 65

23 Galois theory (11/05/2021) 67

# 1 Embeddings and group algebras (09/08/2021)

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 $P_\sigma$ 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 $\varphi$ is a group homomorphism. One can also check that if $\varphi(\sigma) = I$, the identity matrix, then $\sigma$ must be the identity permutation, so $\varphi$ 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. 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 $\varphi$ 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 $\alpha_g$ and $\beta_h$.

**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 $k$-algebras, modules, and Schur's lemma (09/10/2021)

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 $\phi$ 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 $\Phi$ is an $R$-module homomorphism.

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

(3) Show that $\operatorname{im} \Phi$ 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 $M = \operatorname{im} \Phi$.

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 $\Phi$ 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** $\Delta$ 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

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

# 3 Endomorphism ring, Jacobson density theorem (09/13/2021)

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

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

Therefore, $\Phi_\lambda$ is $R$-linear and so $\Phi_\lambda \in \mathrm{End}_R(M)$. However, it is not enough to show that each $\Phi_\lambda$ 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 $\psi$ 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 $\Delta$ 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 $\Delta$ be a division ring and let $M$ be a left $\Delta$-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 $\Delta$-module, we can call it a **left $\Delta$-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 $\Delta$-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 $\Delta$-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 $\Phi$ is a ring homomorphism and if $R$ is a $k$-algebra, then $\Phi$ is a $k$-algebra homomorphism.

(2) The kernel of $\Phi$ 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 $\Delta$ 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 $\Phi_r$ are $\Delta$-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 $\Phi_r$ is $\Delta$-linear as desired.

# 4 Proof of the Jacobson density theorem (09/15/2021)

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 $\Phi$ 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 $\Phi_r$ 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 $\Delta$, 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 $\theta$ is well-defined. We now show that $\theta$ 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 $\theta$ 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 $\Delta$, which is a contradiction. Therefore, the claim holds, and the result follows by induction. □

# 5 Faithful and simple modules, left Artinian rings (09/17/2021)

Note that if $M$ is finite-dimensional as a $\Delta$-vector space, then the map $\Phi$ from the Jacobson Density Theorem is surjective. To see why, take a basis $\{m_1, \ldots, m_n\}$ for $M$ as a $\Delta$-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 $\Phi$ 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, $\Phi$ 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 $2 \times 2$ 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 $1 \times 1$. 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 Simple rings, characterization of left Artinian rings (09/20/2021)

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 $\Delta$-vector space. Then there exist elements $m_1, m_2, \cdots \in M$ that are $\Delta$-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 Opposite ring, spectrum of a ring, Nullstellensatz (09/22/2021)

**Definition 7.1**

Let $S$ be a ring. The **opposite ring** $S^{\mathrm{op}}$ 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 $S^{\mathrm{op}}$ is the same as $S$ (since $*$ is the same as $\cdot$).

(2) If $\Delta$ is a division ring, then $\Delta^{\mathrm{op}}$ 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 $\Delta$ be a division ring. If $M$ is an $n$-dimensional left $\Delta$-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 $\Delta$-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 $\Delta$-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 $\Delta$-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 $\Delta$ 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 $F = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{M}$, 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 $\mathbb{C}[x_1, \dots, x_n]$ has a basis $\{x_1^{i_1} \cdots x_n^{i_n} : i_1, \dots, i_n \geq 0\} \cong \mathbb{N}^n$, 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 $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ and $c_1, \dots, c_n \in \mathbb{C}$, 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 $\mathbb{C}[x_1, \dots, x_n]/\mathfrak{M} \cong \mathbb{C}$. Hence, there is a homomorphism

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

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

**THEOREM 7.10**

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

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

is a nil ideal of $R$.

PROOF. Let $N = \bigcap_{P \in \operatorname{Spec}(R)} P$. 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 Sun-tzu, the Artin-Wedderburn theorem (09/24/2021)

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 $P_1, \ldots, P_s$ be all the prime ideals of $R$. Then for all $i = 1, \ldots, s$, 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 $P_1, P_2, \ldots$ 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

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

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, $\Psi$ is also a ring homomorphism. We now show that $\Psi$ 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 $\Psi$ 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 $\Psi$ 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 Corollary of Sun-tzu, Maschke's theorem (09/27/2021)

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 $\lambda$. 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 $\text{char}(k) \mid |G|$, 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 $\text{char}(k) \nmid |G|$, 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 Class functions, abelianization of a group (09/29/2021)

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

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

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

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

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 $\alpha$ 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 $\alpha$ 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 $z = x^{-1} z x$ for all $x \in G$ by rearranging. Now, this is equivalent to

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

holding for all $x \in G$, where the last equality follows from making the substitution $h = x^{-1} g x$. 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, $\alpha(h) = \alpha(x h x^{-1})$ 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 $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the conjugacy classes of $G$. For $i = 1, \ldots, s$, 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 $\mathcal{C}_1, \dots, \mathcal{C}_s$. Then the elements

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

for $i = 1, \dots, s$ 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 $\{z_1, \dots, z_s\}$ spans $Z(k[G])$, recall that $z \in \sum_{g \in G} \alpha(g) g \in Z(k[G])$ if and only if $\alpha$ is a class function. Let $\beta_i$ be the unique value of $\alpha$ 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 $g, h \in G$ (we call these elements commutators).

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

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

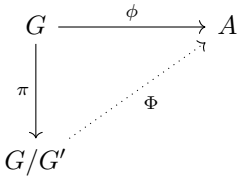
so we have

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

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 $\Phi \circ \pi = \phi$.



# 11 Applications of the big theorem, representations (10/01/2021)

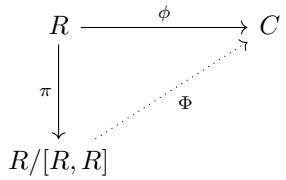
There is a similar notion of abelianization for rings. Let $R$ be a ring. The **commutator ideal** $[R, R]$ is the smallest ideal containing all elements of the form $ab - ba$ where $a, b \in R$. We can also think of $[R, R]$ as the intersection of all two-sided ideals $J$ such that $ab - ba \in J$ for all $a, b \in R$.

Remark 11.1

(1) Note that $R/[R, R]$ is commutative because for all $a, b \in R$, we have

$$\begin{aligned}(a + [R, R])(b + [R, R]) &= ab + [R, R] \\ &= ab + (ba - ab) + [R, R] \\ &= ba + [R, R] \\ &= (b + [R, R])(a + [R, R]).\end{aligned}$$

(2) We also have a universal property here; if $R$ is a ring, $C$ is a commutative ring, $\phi : R \to C$ is a ring homomorphism, and $\pi : R \to R/[R, R]$ is the canonical quotient map, then there exists a unique ring homomorphism $\Phi : R/[R, R] \to C$ such that $\Phi \circ \pi = \phi$.




In Assignment 3, we will prove the following results.

(1) If $k$ is a field and $G$ is a group, then there is a $k$-algebra homomorphism

$$k[G]/[k[G], k[G]] \cong k[G/G'].$$

Said another way, the abelianization of the group algebra is isomorphic to the group algebra of the abelianization.

(2) If $R = M_{n_1}(k) \times \cdots \times M_{n_s}(k)$, then

$$R/[R, R] \cong k^t,$$

where $t = \#\{i : n_i = 1\}$.

As an immediate consequence of these results, we have the following corollary.

Corollary 11.2

If $k[G] \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k)$, then $|G/G'| = \#\{i : n_i = 1\}$.

Proof. Since $k[G]$ and $M_{n_1}(k) \times \cdots \times M_{n_s}(k)$ are isomorphic, so are their abelianizations. It follows that there is a $k$-algebra homomorphism

$$k[G/G'] \cong k^t$$

where $t = \#\{i : n_i = 1\}$. By looking at the dimensions, we see that

$$|G/G'| = \dim_k k[G/G'] = \dim_k k^t = t = \#\{i : n_i = 1\}.$$ □

### Example 11.3

Let's look at $\mathbb{C}[S_4]$. Recall that the conjugacy classes of $S_n$ are just sets of permutations with the same disjoint cycle structure. For $n = 4$, the conjugacy classes are

$$[(1)(2)(3)(4)], [(12)(3)(4)], [(12)(34)], [(123)(4)], [(1234)].$$

Notice that we can think of these as

$$1+1+1+1=4,\ 2+1+1=4,\ 2+2=4,\ 3+1=4,\ 4=4.$$

In particular, there is a bijective correspondence between the conjugacy classes of $S_n$ and the partitions of $n$.

We can look at the sizes of the conjugacy classes. We have

$$\begin{aligned}\#[(1)(2)(3)(4)] &= 1,\\ \#[(1)(2)(34)] &= 6,\\ \#[(1)(234)] &= 8,\\ \#[(1234)] &= 6,\\ \#[(12)(34)] &= 3.\end{aligned}$$

Since there are 5 conjugacy classes of $S_4$, we have

$$\mathbb{C}[S_4] \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_5}(\mathbb{C})$$

for some integers $n_1, \ldots, n_5 \geq 1$.

We claim that $S_4' = A_4$. First, note that $S_4' \subseteq A_4$ since $S_4'/A_4$ is abelian. Now, notice that

$$(123) = (12)(13)(12)(13) = (12)(13)(12)^{-1}(13)^{-1} \in S_4'.$$

Therefore, every 3-cycle is in $S_4'$ as normal subgroups are unions of conjugacy classes. Hence, we see that

$$|S_4'| \geq 9 = \#[(1)(234)] + \#[(1)(2)(3)(4)].$$

Since $|S_4'| \mid |S_4| = 24$ by Lagrange's theorem, we obtain $|S_4'| = 12$, and so $S_4' = A_4$. From this, we have

$$\#\{i : n_i = 1\} = |S_4/S_4'| = |S_4/A_4| = 2.$$

Now, we have $n_3, n_4, n_5 \geq 2$ with $n_3^2 + n_4^2 + n_5^2 = 22$. The only solution to this is $2^2 + 3^2 + 3^2 = 22$, so we conclude that

$$\mathbb{C}[S_4] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}) \times M_3(\mathbb{C}) \times M_3(\mathbb{C}).$$

### Example 11.4

If $A$ is abelian with $|A| = n$, then $|A/A'| = n$ so that $\#\{i : n_i = 1\} = n$. It follows that

$$\mathbb{C}[A] \cong \mathbb{C}^n.$$

We can give an alternate argument: if we had $n_i \geq 2$ for some $i = 1, \ldots, s$, then the product of matrix rings is no longer commutative, which is a contradiction since $\mathbb{C}[A]$ is commutative.

**Example 11.5**

Let $D_5$ be the dihedral group of order 10. We can write

$$D_5 = \langle x, y : x^2 = 1,\, y^5 = 1,\, xyx = y^{-1} \rangle.$$

We have an isomorphism

$$\mathbb{C}(D_5) \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_s}(\mathbb{C})$$

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

$$10 = 1^2 + 3^2 = 1^2 + 1^2 + 2^2 + 2^2 = \underbrace{1^2 + \cdots + 1^2}_{6} + 2^2 = \underbrace{1^2 + \cdots + 1^2}_{10}.$$

One can check that $D_5$ has 4 conjugacy classes. Therefore, only the choice $10 = 1^2 + 1^2 + 2^2 + 2^2$ works, and we must have

$$\mathbb{C}(D_5) \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}) \times M_2(\mathbb{C}).$$

Let's now study representations. Let $G$ be a group and let $k$ be an algebraically closed field such that $\mathrm{char}(k) \nmid |G|$. A **representation** of $G$ is a group homomorphism

$$\rho : G \to \mathrm{GL}_n(k).$$

**Remark 11.6**

The group homomorphism $\rho : G \to \mathrm{GL}_n(k)$ extends to a $k$-algebra homomorphism

$$\tilde{\rho} : k[G] \to M_n(k).$$

Conversely, if $\phi : k[G] \to M_n(k)$ is a $k$-algebra homomorphism, then $\phi$ restricted to $G$ is a map

$$\phi|_G : G \to \mathrm{GL}_n(k).$$

This is because $\phi(1) = I$, so for any $g \in G$, we have

$$\phi(g) \cdot \phi(g)^{-1} = \phi(g \cdot g^{-1}) = \phi(1) = I.$$

Thus, $\phi(g)$ must be an invertible matrix. Moreover, $\tilde{\rho}|_G = \rho$.

**Remark 11.7**

If $\phi : k[G] \to M_n(k)$ is a $k$-algebra homomorphism, then

$$V = k^{n \times 1} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_1, \ldots, a_n \in k \right\}$$

can be given a left $k[G]$-module structure with the rule

$$r \cdot v := \Phi(r) \cdot v$$

for $r \in k[G]$ and $v \in V$.

Notice that if $V$ is a $k[G]$-module, then we have a $k$-algebra homomorphism

$$\Psi : k[G] \to \mathrm{End}_k(V)$$

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

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

and extend linearly over $k$. In particular,

$$\Psi|_G : G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(k),$$

where $\mathrm{GL}(V)$ denotes the invertible linear transformations over $M$. For this reason, if $V$ is a $k[G]$-module, we will call $V$ a **representation** of $G$.

# 12 Direct sums, decompositions of modules (10/04/2021)

We'll first make some definitions.

**Definition 12.1**

Let $V$ and $W$ be $k[G]$-modules; that is, they are representations of $G$.

(1) If $V$ is simple, we say that $V$ is a **irreducible representation** (or an **irrep**).

(2) If $W \subseteq V$ is a $k[G]$-submodule of $V$, we say that $W$ is a **subrepresentation** of $G$.

(3) We call two representations $V$ and $W$ **equivalent** if $V \cong W$ as left $k[G]$-modules.

(4) We say that $V$ is **decomposable** if $V = V_1 \oplus V_2$, where $V_1$ and $V_2$ are proper submodules of $V$.

Let's define what a direct sum is. First, let $M$ be an $R$-module. If $M_1$ and $M_2$ are submodules of $M$, then

$$M_1 + M_2 = \{m_1 + m_2 : m_1 \in M_1,\, m_2 \in M_2\} \subseteq M.$$

More generally, if we have a family $(M_\alpha)_\alpha \in X$ of submodules of $M$, then

$$\sum_{\alpha \in X} M_\alpha = \left\{ \sum_{\alpha \in X} m_\alpha : m_\alpha \in M_\alpha,\ m_\alpha = 0 \text{ for all but finitely many } \alpha \right\} \subseteq M.$$

Then, we call $\sum_{\alpha \in X} M_\alpha \subseteq M$ **direct** when $\sum_{\alpha \in X} m_\alpha = 0$ if and only if $m_\alpha = 0$ for all $\alpha \in X$. In the case where $\sum_{\alpha \in X} M_\alpha$ is a direct sum, we write

$$\bigoplus_{\alpha \in X} M_\alpha := \sum_{\alpha \in X} M_\alpha.$$

**Remark 12.2**

Let $M$ be an $R$-modules, and let $M_1$ and $M_2$ be submodules of $M$. Then $M_1 + M_2$ is a direct sum if and only if $M_1 \cap M_2 = (0)$.

**Example 12.3**

Let $V$ be a vector space over a field $k$, and let $v_1, v_2 \in V \setminus \{0\}$. Consider the submodules $V_1 = \{\lambda v_1 : \lambda \in k\}$ and $V_2 = \{\lambda v_2 : \lambda \in k\}$. Then $V_1 + V_2$ is a direct sum if and only if $v_1$ and $v_2$ are linearly independent.

We'll study some module theory for the group algebra $k[G]$. Let $k$ be an algebraically closed field such that $\text{char}(k) \nmid |G|$.

In the next few lectures, we will work towards proving the following theorem.

**Theorem 12.4**

Suppose that

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

where $s$ is the number of conjugacy classes of $G$.

(1) Up to isomorphism, $k[G]$ has $s$ pairwise non-isomorphic simple left modules $V_1, \ldots, V_s$ (that is, $s$ pairwise inequivalent irreducible representations).

(2) Every $k[G]$-module decomposes as a direct sum of copies of $V_1, \ldots, V_s$.

(3) **Uniqueness:** If $V_1^{a_1} \oplus V_2^{a_2} \oplus \cdots \oplus V_s^{a_s} \cong V_1^{b_1} \oplus V_2^{b_2} \oplus \cdots \oplus V_s^{b_s}$, then $a_i = b_i$ for all $i = 1, \ldots, s$, where by $V^a$, we mean $V^a := V \oplus \cdots \oplus V$ ($a$ times).

What is the significance of this theorem? First, let's ask what the $V_i$'s are. We know that

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

and for each $i = 1, \ldots, s$, we have the projection

$$\pi_i : M_{n_1}(k) \times \cdots \times M_{n_s}(k) \to M_{n_i}(k).$$

Note that $M_{n_i}(k)$ has the module $V_i \cong k^{n_i \times 1}$. Now, if $V$ is a representation of $G$ which looks like

$$V = V_{i_1} \oplus \cdots \oplus V_{i_q},$$

we recall that $k[G]$ acting on $V$ gives us a representation

$$\rho : G \to \text{GL}(V)$$

given by $\rho(g)(v) := g \cdot v$. Now, what's the significance of the decomposition of $V$ above? Suppose for simplicity that we had $V = W_1 \oplus W_2$, where $W_1$ and $W_2$ are $k[G]$-submodules of $V$. Let $\{v_1, \ldots, v_d\}$ be a basis for $W_1$, and let $\{v_{d+1}, \ldots, v_n\}$ be a basis for $W_2$. Then we have

$$\rho(g)(v_j) = g \cdot v_j = \begin{cases} a_{1j}v_1 + \cdots + a_{d_j}v_d, & \text{if } j \leq d, \\ a_{(d+1)_j}v_{d+1} + \cdots + a_{n_j}v_n, & \text{if } d+1 \leq j \leq n. \end{cases}$$

In particular, by setting $\mathcal{B} = \{v_1, \ldots, v_n\}$, we see that

$$[\rho(g)]_{\mathcal{B}} = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right),$$

where $A_1$ is a $d \times d$ matrix and $A_2$ is an $(n-d) \times (n-d)$ matrix. Therefore, the importance of the theorem is that if we are given a finite-dimensional representation, we can uniquely write it as a block diagonal matrix

(up to ordering of the blocks), where the blocks are representations coming from the irreducibles $V_i \cong k^{n\times 1}$. Therefore, if we understand irreducibles, then we understand every representation.

First, in order to understand $k[G]$, we looked at Artinian rings with no nonzero nil ideals. Now that we understand $k[G]$, our main goal is to understand representations. Our discussion above shows that it suffices to understand the simples $V_i \cong k^{n\times 1}$. We will use character theory to do so, which we will get to soon, and we'll understand everything.

Due to the isomorphism

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

we can just think of $k[G]$ as a product of matrix rings. Therefore, it suffices to understand the left modules of $M_{n_1}(k) \times \cdots \times M_{n_s}(k)$ to know the left modules of $k[G]$. Let $R$ and $S$ be rings with an isomorphism $\phi : R \to S$. If we have an $R$-module $M$, we obtain an $S$-module by taking

$$s \cdot m := \phi^{-1}(s) \cdot m.$$

Conversely, if $N$ is a left $S$-module, then we can give it an $R$-module structure by

$$r \cdot n = \phi(r) \cdot n.$$

That is, the isomorphism $\phi$ is just a way of relabelling these elements.

**Lemma 12.5**

Let $R = M_{n_1}(k) \times \cdots \times M_{n_s}(k)$, and let $V_i = k^{n_i \times 1}$ for each $i = 1, \ldots, s$. For each $i = 1, \ldots, s$ we define

$$(A_1, \ldots, A_i, \ldots, A_s) \cdot v := A_i v$$

where $(A_1, A_2, \ldots, A_s) \in R$ and $v \in V_i$. Then $V_i$ is a simple left $R$-module, and if $i \neq j$, then $V_i \ncong V_j$.

Proof. If $(A_1, \ldots, A_s), (B_1, \ldots, B_s) \in R$ and $v \in V_i$, then

$$\begin{aligned}(A_1, \ldots, A_i, \ldots, A_s) \cdot (B_1, \ldots, B_i, \ldots, B_s) \cdot v &= (A_1B_1, \ldots, A_iB_i, \ldots, A_sB_s)v \\ &= A_iB_iv \\ &= A_i(B_iv) \\ &= (A_1, \ldots, A_s)[(B_1, \ldots, B_s) \cdot v]\end{aligned}$$

Therefore, $V_i$ is a left $R$-module; the other properties come for free since $V_i$ is already a module over $M_{n_i}(k)$, and hence it is an abelian group.

Why is $V_i$ simple as an $R$-module? Notice that it suffices to show that if $v_1 \in V_i \setminus \{0\}$ and $v_2 \in V_i$, then there exists $r \in R$ such that $r \cdot v_1 = v_2$. Indeed, if $V_i$ is simple, then the only submodules are $(0)$ and $V_i$ itself. If we have a nonzero element of $V_i$, then it should generate all of $V_i$.

We already know that $V_i$ is a simple $M_{n_i}(k)$-module. Therefore, there exists $A \in M_{n_i}(k)$ such that $Av_1 = v_2$. Let $r = (0, \ldots, 0, A, 0, \ldots, 0)$, where $A$ is located at the $i$-th coordinate. Then $r \cdot v_1 = v_2$, so $V_i$ is a simple left $R$-module.

Next, we show that if $i \neq j$, then $V_i \ncong V_j$ as left $R$-modules. Suppose that we have an $R$-linear isomorphism $f : V_i \to V_j$. If $v \in V_i$, then

$$f((0, \ldots, 0, I, 0, \ldots, 0) \cdot v) = f(0 \cdot v) = 0 \in V_j,$$

where $I$ is in the $j$-th position, and the $i$-th position is one of the zeros. Since $f$ is $R$-linear, then

$$f((0, \ldots, 0, I, 0, \ldots, 0) \cdot v) = (0, \ldots, 0, I, 0, \ldots, 0) \cdot f(v) = I \cdot f(v) = f(v).$$

This means that $f$ is identically zero, contradicting the fact that it is an isomorphism from $V_i$ to $V_j$. □

**Remark 12.6**

In fact, we have shown that if $i \neq j$, then

$$\mathrm{Hom}_R(V_i, V_j) = \{0\}.$$

When $i = j$, we have $\mathrm{Hom}_R(V_i, V_j) = \mathrm{End}_R(V_i)$. In the case that $k$ is algebraically closed and $R$ is a finite-dimensional $k$-algebra, we have $\mathrm{End}_R(V_i) \cong k$ by Proposition 3.1, since $V_i$ is a simple left $R$-module.

# 13 Number of inequivalent irreducible representations (10/06/2021)

Last time, we were looking at a ring

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

We saw that $V_i = k^{n_i \times 1}$ is a left $R$-module with the action

$$(A_1, \ldots, A_s) \cdot v := A_i v \in V_i$$

for $(A_1, \ldots, A_s) \in R$ and $v \in V_i$. Moreover, $V_i$ is a simple left $R$-module with $V_i \ncong V_j$ when $i \neq j$.

Now, we observe that

$$\begin{aligned}\mathrm{Ann}_R(V_i) &= \{(A_1, \ldots, A_{i-1}, 0, A_{i+1}, \ldots, A_s) : A_j \in M_{n_j}(k)\} \\ &= M_{n_1}(k) \times \cdots \times M_{n_{i-1}}(k) \times \{0\} \times M_{n_{i+1}}(k) \times \cdots \times M_{n_s}(k).\end{aligned}$$

In particular, if $i \neq j$, then $\mathrm{Ann}_R(V_i) \ncong \mathrm{Ann}_R(V_j)$. Assignment 3 Question 2 then gives us another proof of the fact that $V_i \ncong V_j$.

**Definition 13.1**

If $R$ is a ring, we will write ${}_R R$ to mean $R$ considered as a left $R$-module. (Similarly, the notation $R_R$ means $R$ taken as a right $R$-module.)

Let $A, B \in M_n(k)$. We can think of $B$ as $n$ columns concatenated with each other. In particular, if $v_1, \ldots, v_n$ are the columns of $B$, then the columns of $AB$ are given by $Av_1, \ldots, Av_n$. Therefore, if $R = M_n(k)$ and $V = k^{n \times 1}$, then

$${}_R R \cong \underbrace{V \oplus \cdots \oplus V}_{n}$$

with the $R$-module isomorphism

$$B \mapsto (v_1, \ldots, v_n),$$

where as before, $v_1, \ldots, v_n$ are the columns of $B$.

More generally, if $R = M_{n_1}(k) \times \cdots \times M_{n_s}(k)$ and $V_i = k^{n_i \times 1}$, then we have

$$(A_1, \ldots, A_s) \cdot v = A_i v$$

for $(A_1, \ldots, A_s) \in R$ and $v \in V_i$, so we see that

$${}_R R \cong \underbrace{V_1 \oplus \cdots \oplus V_1}_{n_1} \oplus \underbrace{V_2 \oplus \cdots \oplus V_2}_{n_2} \oplus \cdots \oplus \underbrace{V_s \oplus \cdots \oplus V_s}_{n_s}$$

with the explicit $R$-module isomorphism

$$(B_1, \ldots, B_s) \in {}_R R \mapsto (\underbrace{v_{11}, \ldots, v_{1n_1}}_{\in V_1^{n_1}}, \ldots, \underbrace{v_{s1}, \ldots, v_{sn_s}}_{\in V_s^{n_s}}),$$

where $v_{i1}, \ldots, v_{in_i}$ are the columns of $B_i$ for each $i = 1, \ldots, s$. Indeed, we can see that this is an $R$-module isomorphism because for $(A_1, \ldots, A_s) \in R$ and $(B_1, \ldots, B_s) \in {}_R R$, the columns of $A_i B_i$ are $Av_{i1}, \ldots, Av_{in_i}$, and on the other hand, we have

$$(A_1, \ldots, A_s) \cdot (v_{11}, \ldots, v_{1n_1}, \ldots, v_{s1}, \ldots, v_{sn_s}) = (\underbrace{A_1 v_{11}, \ldots, A_1 v_{1n_1}}_{A_1 B_1}, \ldots, \underbrace{A_s v_{s1}, \ldots, A_s v_{sn_s}}_{A_s B_s}).$$

From this discussion, we obtain the key fact that if $R = M_{n_1}(k) \times \cdots \times M_{n_s}(k)$ and $V_i = k^{n_i \times 1}$, then

$${}_R R \cong V_1^{n_1} \oplus \cdots \oplus V_s^{n_s}$$

as $R$-modules. Now, we are almost in the position to finish proving Theorem 12.4.

**Remark 13.2**

Let $N$ and $M_\alpha$ for $\alpha \in X$ be left $R$-modules.

(1) From Exercise 4 on Assignment 2, we have

$$\mathrm{Hom}_R\left(\bigoplus_{\alpha \in X} M_\alpha, N\right) \cong \prod_{\alpha \in X} \mathrm{Hom}_R(M_\alpha, N).$$

(2) If $N \neq (0)$ is a left $R$-module, then

$$\mathrm{Hom}_R(R, N) \neq (0).$$

Notice that for all $n \in N$, there exists a map

$$\begin{aligned} \varphi_n : {}_R R &\to N \\ r &\mapsto r \cdot n. \end{aligned}$$

For $a \in R$ and $r \in {}_R R$, we have $\varphi_n(ar) = ar \cdot n = a \cdot (rn) = a \cdot \varphi_n(r)$, so $\varphi_n$ is $R$-linear. Moreover, when $n \neq 0$, we have $\varphi_n(1) = n \neq 0$, so $\varphi_n \neq 0$.

**Exercise 13.3**

Define the map

$$\begin{aligned} e : \mathrm{Hom}_R({}_R R, N) &\to N \\ \varphi &\mapsto \varphi(1). \end{aligned}$$

If $R$ is commutative, show that $e$ is an isomorphism of $R$-modules.

Now, we can prove part (1) of Theorem 12.4.

**Theorem 13.4**

Let $R \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k)$ and $V_i \cong k^{n_i \times 1}$. If $N$ is a simple left $R$-module, then there exists some $i = 1, \ldots, s$ such that $N \cong V_i$ as $R$-modules. In particular, $R$ has exactly $s$ simple left $R$-modules up to isomorphism.

Proof. Let $N$ be a simple $R$-module. Then we have

$$\mathrm{Hom}_R({}_R R, N) \neq (0)$$

since $N \neq (0)$. In particular, we obtain

$$\mathrm{Hom}_R({}_R R, N) \cong \mathrm{Hom}_R(V_1^{n_1} \oplus \cdots \oplus V_s^{n_s}, N) \cong \prod_{i=1}^{s} \mathrm{Hom}_R(V_i, N)^{n_i}.$$

Since $\mathrm{Hom}_R({}_R R, N) \neq (0)$, there exists $i = 1, \ldots, s$ such that $\mathrm{Hom}_R(V_i, N) \neq (0)$. Therefore, there exists a nonzero $R$-modulo homomorphism $f : V_i \to N$. Now, $V_i$ is simple, and since $\ker(f)$ is a submodule of $V_i$, we either have $\ker(f) = (0)$ or $\ker(f) = V_i$. But $f$ is nonzero, so we have $\ker(f) = V_i$. Similarly, $\mathrm{im}(f)$ is a submodule of $N$. Again, $f$ is nonzero, so $\mathrm{im}(f) \neq (0)$, and since $N$ is simple, $\mathrm{im}(f) = N$.

As in the proof of Schur's lemma (Theorem 2.15), the set theoretic inverse of $f$ is an $R$-module homomorphism with $f \circ f^{-1} = \mathrm{id}_N$ and $f^{-1} \circ f = \mathrm{id}_{V_i}$. Therefore, $f : V_i \to N$ is an $R$-module isomorphism. □

Towards proving (2) of Theorem 12.4, we'll first prove the following fact.

**Proposition 13.5**

Every $R$-module $M$ satisfies

$$M \cong R^{\oplus X}/L$$

where $R^{\oplus X} = \bigoplus_{x \in X} R$, and $L$ is a submodule of $R^{\oplus X}$.

Proof. For each $m \in M$, we will define a formal symbol $e_m$. (We can think of this as a vector $e_m = (0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 is in the $m$-th position, but this choice doesn't always work.) Define an $R$-module homomorphism $\Psi : \bigoplus_{m \in M} Re_m \to M$ by

$$\sum_{m \in M} r_m e_m \mapsto \sum_{m \in M} r_m \cdot m.$$

We note that these must be finite sums in order to make sense. When $r \in R$, we have

$$\Psi\left(r \cdot \sum_{m \in M} r_m e_m\right) = \Psi\left(\sum_{m \in M} r \cdot r_m e_m\right) = \sum_{m \in M} r \cdot r_m \cdot m = r \cdot \sum_{m \in M} r_m \cdot m = r \cdot \Psi\left(\sum_{m \in M} r_m e_m\right).$$

Therefore, $\Psi$ is $R$-linear. Moreover, $\Psi(1 \cdot e_m) = m$, so $\Psi$ is onto. Let $L = \ker \Psi$. By the first isomorphism theorem, we obtain $\bigoplus_{m \in M} Re_m / L \cong \mathrm{im}\, \Psi = M$, and we can take $\bigoplus_{m \in M} Re_m$ as $R^{\oplus X}$. □

# 14 Semisimple rings and a characterization (10/08/2021)

**Definition 14.1**

Let $R$ be a ring. We say that a left $R$-module $M$ is **semisimple** of $M$ can be written as the direct sum of simple submodules. We say that $R$ is a **(left) semisimple ring** if every left $R$-module is semisimple.

**Example 14.2**

An example of a non-semisimple ring is $\mathbb{Z}$. The simple modules are isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for primes $p$, and we notice that $\mathbb{Z}/4\mathbb{Z}$ cannot be written as the direct sum of simple submodules.

**Example 14.3**

Let $k$ be a field. A $k$-module is simply a vector space, and a submodule is a subspace. In particular, a simple $k$-module $V$ is a vector space whose only subspaces are (0) and $V$ itself. Therefore, $V$ is a simple $k$-module if and only if $\dim_k V = 1$. Now, if $W$ is a $k$-vector space, then we can write

$$W = \bigoplus_{\alpha \in \mathcal{B}} kv_\alpha,$$

since every vector space has a basis $\mathcal{B}$. Hence, $k$ is a semisimple ring.

Notice that the fact that every vector space has a basis relies on Zorn's lemma. The following theorem generalizes this example, and at some point, we'll have to use Zorn's lemma to prove it.

**Theorem 14.4**

Let $R$ be a ring. Then $R$ is a (left) semisimple ring if and only if ${}_RR$ is a semisimple $R$-module.

To prove this, we'll use the following lemma.

**Lemma 14.5**

Let $R$ be a ring.

(1) If $\{M_\alpha\}_{\alpha \in X}$ is a family of left $R$-modules where each $M_\alpha$ is semisimple, then $\bigoplus_{\alpha \in X} M_\alpha$ is semisimple.

(2) If $M$ is a semisimple left $R$-module and $L \trianglelefteq M$ is a submodule of $M$, then $M/L$ is also semisimple.

First, we'll show that Theorem 14.4 easily follows from Lemma 14.5.

*Proof of Theorem 14.4.* ($\Rightarrow$) If every left $R$-module is semisimple, then certainly ${}_RR$ is semisimple.

($\Leftarrow$) Let $M$ be a left $R$-module. We saw in Proposition 13.5 that $M \cong R^{\oplus X}/L$ where $L \trianglelefteq \bigoplus_{x \in X} R$. If ${}_RR$ is semisimple, then

$$\bigoplus_{x \in X} {}_RR = \bigoplus_{x \in X} R$$

is semisimple by taking $M_\alpha = {}_RR$ for each $\alpha \in X$ and applying (1) of Lemma 14.5. It follows from (2) that $M \cong \bigoplus_{x \in X} R/L$ is semisimple. □

Now, it only remains to prove Lemma 14.5.

*Proof of Lemma 14.5.*

(1) Write each $M_\alpha$ as a direct sum of simple $R$-modules

$$M_\alpha = \bigoplus_{\beta \in X_\alpha} V_{\alpha,\beta}.$$

It follows that

$$\bigoplus_{\alpha\in X} M_\alpha = \bigoplus_{\alpha\in X}\bigoplus_{\beta\in X_\alpha} V_{\alpha,\beta} = \bigoplus_{(\alpha,\beta)\,:\,\alpha\in X,\,\beta\in X_\alpha} V_{\alpha,\beta}$$

is the direct sum of simple modules, so it is semisimple.

(2) Since $M$ is semisimple, we can write

$$M = \bigoplus_{\alpha\in X} V_\alpha,$$

where each $V_\alpha$ is simple. Let $\pi : M \to M/L$ be the canonical projection. Consider $\pi(V_\alpha) \subseteq M/L$. We claim that either $\pi(V_\alpha) \cong V_\alpha$ or $\pi(V_\alpha) = (0)$. First, we restrict $\pi$ to $V_\alpha$ to obtain the map

$$\pi|_{V_\alpha} : V_\alpha \to \pi(V_\alpha),$$

which is a surjective $R$-module homomorphism. Since $\ker(\pi|_{V_\alpha})$ is a submodule of $V_\alpha$, we either have $\ker(\pi|_{V_\alpha}) = (0)$ or $\ker(\pi|_{V_\alpha}) = V_\alpha$ by the simplicity of $V_\alpha$. In the first case, $\pi|_{V_\alpha}$ is a bijection, so $\pi(V_\alpha) \cong V_\alpha$. In the second case, we obtain $\pi(V_\alpha) = (0)$.

Let $Y = \{\alpha \in X : \pi(V_\alpha) \cong V_\alpha\} \subseteq X$. We claim that

$$M/L = \sum_{\alpha\in Y} \pi(V_\alpha).$$

Since $\pi : M \to M/L$ is onto and $M = \sum_{\alpha\in X} V_\alpha$, we have

$$M/L = \pi(M) = \pi\left(\sum_{\alpha\in X} V_\alpha\right) = \sum_{\alpha\in X} \pi(V_\alpha) = \sum_{\alpha\in Y} \pi(V_\alpha),$$

where the last equality is because $\pi(V_\alpha) = (0)$ for all $\alpha \in X \setminus Y$, which contributes nothing to the sum.

Note that the above sum is not necessarily a direct sum. This is where we'll use Zorn's lemma to show that it is isomorphic to a direct sum of simples. Let

$$\mathcal{S} = \left\{ Z \subseteq Y : \sum_{\alpha\in Z} \pi(V_\alpha) \text{ is a direct sum} \right\}.$$

First, we note that $\mathcal{S} \neq \varnothing$ since empty sums are by definition direct sums, so $\varnothing \in \mathcal{S}$. Let $\{Z_\gamma\}_{\gamma\in\Gamma}$ be a chain in $\mathcal{S}$ ordered by inclusion, where $\Gamma$ is a totally ordered set. We must show that

$$Z := \bigcup_{\gamma\in\Gamma} Z_\gamma \in \mathcal{S},$$

which will be an upper bound in the chain, in which case we can apply Zorn's lemma to $\mathcal{S}$. So suppose towards a contradiction that $Z \notin \mathcal{S}$. Then the sum $\sum_{\alpha\in Z} \pi(V_\alpha)$ is not a direct sum. Therefore, there is a finite set of elements $\alpha_1, \ldots, \alpha_s \in Z$ such that

$$\pi(V_{\alpha_1}) + \cdots + \pi(V_{\alpha_s})$$

is not direct. There exists some $\gamma \in \Gamma$ such that $\alpha_1, \ldots, \alpha_s \in Z_\gamma$, which would imply that $\sum_{\alpha\in Z_\gamma} \pi(V_\alpha)$ is not a direct sum, a contradiction. Therefore, $Z \in \mathcal{S}$, and by Zorn's lemma, there exists a maximal element $Y_0 \in \mathcal{S}$ with $Y_0 \subseteq Y$.

Finally, we'll show that $N = \sum_{\alpha\in Y_0} \pi(V_\alpha)$ is direct and equal to $M/L$. The fact that it is direct is immediate since $Y_0 \in \mathcal{S}$. Recall that

$$M/L = \sum_{\alpha\in Y} \pi(V_\alpha).$$

If $\pi(V_\alpha) \subseteq N$ for all $\alpha \in Y$, we have $\sum_{\alpha\in Y} \pi(V_\alpha) \subseteq N$. This gives $M/L \subseteq N$, and hence $N = M/L$. Therefore, it is enough to show that $\pi(V_\alpha) \subseteq N$ for any $\alpha \in Y$. Suppose that this was not the case, so $\pi(V_{\alpha_0}) \not\subseteq N$ for some $\alpha_0 \in Y$. We will show that

$$\pi(V_{\alpha_0}) + \bigoplus_{\alpha\in Y_0} \pi(V_\alpha)$$

is a direct sum, which will give a contradiction as $\{\alpha_0\} \cup Y_0 \in \mathcal{S}$ contradicts the maximality of $Y_0$ in $\mathcal{S}$. Note that $\pi(V_{\alpha_0})$ is simple. If $\pi(V_{\alpha_0}) = (0)$, then $\pi(V_{\alpha_0}) + \bigoplus_{\alpha\in Y_0} \pi(V_\alpha)$ is a direct sum. Otherwise, $\pi(V_{\alpha_0})$ is already in $\bigoplus_{\alpha\in Y_0} \pi(V_\alpha)$, which means that $\pi(V_{\alpha_0}) \subseteq N$, a contradiction. □

# 15 Uniqueness of decompositions, characters (10/18/2021)

We were looking at rings of the form

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

So far, we have shown the following facts.

- Up to isomorphism of $R$-modules, $R$ has exactly $s$ simple left $R$-modules $V_1, \ldots, V_s$.
- We have the decomposition ${}_RR \cong V_1^{n_1} \oplus \cdots \oplus V_s^{n_s}$.
- The ring $R$ is semisimple; that is, every $R$-module can be written as the direct sum of simple submodules.

Observe that we have (2) of Theorem 12.4, because we already know that

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

where $s$ is the number of conjugacy classes of $G$ so that $k[G]$ is a semisimple ring. It only remains to prove (3), the uniqueness part. That is, if $V_1^{a_1} \oplus \cdots \oplus V_s^{a_s} \cong V_1^{b_1} \oplus \cdots \oplus V_s^{b_s}$ is an $R$-module isomorphism, then $a_i = b_i$ for all $i = 1, \ldots, s$. First, we will make a remark.

**Remark 15.1**

If $R$ is a $k$-algebra and $M$ and $N$ are left $R$-modules, then $\mathrm{Hom}_R(M, N)$ is a $k$-vector space. Indeed, for a homomorphism $\Phi : M \to N$ and $\lambda \in k$, we can define scalar multiplication by

$$(\lambda \cdot \Phi)(m) := \lambda \cdot \Phi(m).$$

Note that this only works because $k$ is central; in the general case where $R$ is not a $k$-algebra, we can only say that $\mathrm{Hom}_R(M, N)$ is an abelian group.

Proof of uniqueness. Suppose that

$$f : V_1^{a_1} \oplus \cdots \oplus V_s^{a_s} \to V_1^{b_1} \oplus \cdots \oplus V_s^{b_s}$$

is an $R$-module isomorphism. Then for each $i = 1, \ldots, s$, we have

$$\mathrm{Hom}_R(V_1^{a_1} \oplus \cdots \oplus V_s^{a_s}, V_i) \cong \mathrm{Hom}_R(V_1^{b_1} \oplus \cdots \oplus V_s^{b_s}, V_i)$$

as $k$-vector spaces. Looking at the left-hand side, we have

$$\mathrm{Hom}_R(V_1^{a_1} \oplus \cdots \oplus V_s^{a_s}, V_i) \cong \prod_{j=1}^{s} \mathrm{Hom}_R(V_j, V_i) \cong \mathrm{Hom}_R(V_i, V_i)^{a_i} \cong k^{a_i},$$

where the first isomorphism is due to (1) of Remark 13.2, and the second isomorphism is because

$$\mathrm{Hom}_R(V_j, V_i) = \begin{cases} (0) & \text{if } j \neq i, \\ k & \text{if } j = i. \end{cases}$$

Similarly, we find that

$$\mathrm{Hom}_R(V_1^{b_1} \oplus \cdots \oplus V_s^{b_s}, V_i) \cong k^{b_i}.$$

This gives $k^{a_i} \cong k^{b_i}$, and hence $a_i = b_i$ for all $i = 1, \ldots, s$. □

Now, we're ready to move on to character theory. Recall that in our usual setting, we have a finite group $G$ and an algebraically closed field $k$ such that $\mathrm{char}(k) \nmid |G|$. Let $V$ be a finite-dimensional $k[G]$-module. Then $k[G]$ has $s$ pairwise non-isomorphic $k[G]$-modules $V_1, \ldots, V_s$, where $s$ is the number of conjugacy classes of $G$. Then $V$ gives us a group homomorphism

$$\rho_V : G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(k)$$

where $n = \dim_k(V)$, with the rule

$$\rho_V(g)(v) := g \cdot v.$$

Recall that linear maps $T : V \to V$ have a trace $\mathrm{Tr}(T)$.

**Remark 15.2**

If $\{v_1, \ldots, v_n\}$ is a basis for $V$, then we can write

$$Tv_j = \sum_{i=1}^{n} a_{ij} v_i, \qquad \mathrm{Tr}(T) = \sum_{i=1}^{n} a_{ii}.$$

**Definition 15.3**

We define the **character** of $V$ as the map $\chi_V : G \to k$ given the rule

$$\chi_V(g) := \mathrm{Tr}(\rho_V(g)).$$

**Example 15.4**

Let $G = S_3$, and let $V = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3$, which is a 3-dimensional vector space. We can give $V$ a structure as a $\mathbb{C}[S_3]$-module by the action

$$\sigma \cdot e_j = e_{\sigma(j)},$$

and hence

$$\sigma(\alpha e_1 + \beta e_2 + \gamma e_3) = \alpha e_{\sigma(1)} + \beta e_{\sigma(2)} + \gamma e_{\sigma(3)}.$$

In particular, we are taking the usual action of $S_3$ on $\{1, 2, 3\}$, and we're extending it to a vector space. Now, we'll determine the representation $\rho_V : G \to \mathrm{GL}_3(\mathbb{C}) \cong \mathrm{GL}(V)$. We have

$$\rho_V(\mathrm{id}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_V((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_V((13)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\rho_V((23)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \rho_V((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \rho_V((132)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Now, we can take a look at the character $\chi_V : G \to \mathbb{C}$; we see that

$$\begin{aligned} \chi_V(\mathrm{id}) &= 3, & \chi_V((12)) &= 1, & \chi_V((13)) &= 1, \\ \chi_V((23)) &= 1, & \chi_V((123)) &= 0, & \chi_V((132)) &= 0. \end{aligned}$$

Observe that $\chi_V(\sigma)$ gives us the number of fixed points of $\sigma \in S_3$. Moreover, if $\chi_V(\sigma) = \chi_V(\tau)$, then $\sigma$ and $\tau$ are in the same conjugacy class.

Recall that $f : G \to k$ is a class function if it is constant when restricted to conjugacy classes; that is, $f(xgx^{-1}) = f(g)$ for all $g, x \in G$.

**Theorem 15.5**

Let $V$ be a finite-dimensional $k[G]$-module. Then $\chi_V : G \to k$ is a class function.

Proof. Since $\rho_V : G \to \mathrm{GL}(V)$ is a group homomorphism, we have

$$\rho_V(xgx^{-1}) = \rho_V(x)\rho_V(g)\rho_V(x)^{-1}.$$

It follows that

$$\mathrm{Tr}(\rho_V(xgx^{-1})) = \mathrm{Tr}(\rho_V(x)\rho_V(g)\rho_V(x)^{-1}) = \mathrm{Tr}(\rho_V(g)),$$

where the last equality is because similar matrices preserve trace. In particular, we have $\chi_V(xgx^{-1}) = \chi_V(g)$ for all $g, x \in G$, so $\chi_V$ is a class function. □

**Remark 15.6**

(1) If $V \cong W$ as $k[G]$-modules, then $\chi_V = \chi_W$. (In fact, in the case that $V$ and $W$ are finite-dimensional, the converse is also true.)

(2) If $W_1$ and $W_2$ are $k[G]$-modules, then $\chi_{W_1 \oplus W_2} = \chi_{W_1} + \chi_{W_2}$. By induction, we also see that if $W_1, \ldots, W_r$ are $k[G]$-modules, then

$$\chi_{W_1 \oplus \cdots \oplus W_r} = \sum_{i=1}^{r} \chi_{W_i}.$$

Proof.

(1) Let $f : V \to W$ be a $k[G]$-module isomorphism. Let $\{v_1, \ldots, v_n\}$ be a basis for $V$ as a $k$-vector space. Then

$$\chi_V(g) = \mathrm{Tr}(a_{ij}) = a_{11} + a_{22} + \cdots + a_{nn},$$

where $g \cdot v_j = \sum_{i=1}^{n} a_{ij} v_i$. Notice that $\{f(v_1), \ldots, f(v_n)\}$ is a basis for $W$ as a $k$-vector space, and $f$ is $k[G]$-linear, so

$$g \cdot f(v_j) = f(g \cdot v_j) = f\left(\sum_{i=1}^{n} a_{ij} v_i\right) = \sum_{i=1}^{n} a_{ij} f(v_i).$$

Now, we see that $\chi_W(g) = \mathrm{Tr}(a_{ij}) = a_{11} + \cdots + a_{nn} = \chi_V(g)$.

(2) Write $W = W_1 \oplus W_2$. Let $\{v_1, \ldots, v_m\}$ be a basis for $W_1$, and let $\{v_{m+1}, \ldots, v_n\}$ be a basis for $W_2$. Observe that

$$\rho_W(g)(v_i) = \begin{cases} \rho_{W_1}(g)(v_i) & \text{if } i = 1, \ldots, m, \\ \rho_{W_2}(g)(v_i) & \text{if } i = m+1, \ldots, n. \end{cases}$$

Then with respect to the basis $\{v_1, \ldots, v_n\}$, we have

$$\rho_W(g) = \left(\begin{array}{c|c} \rho_{W_1}(g) & 0 \\ \hline 0 & \rho_{W_2}(g) \end{array}\right).$$

In particular, we find that $\chi_W(g) = \chi_{W_1}(g) + \chi_{W_2}(g)$. □

These results are important to us because if $V$ is a finite-dimensional $k[G]$-module, then $V$ decomposes as

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_s^{a_s},$$

where each $a_i \geq 0$, $V_1, \ldots, V_s$ are simple modules, and $s$ is the number of conjugacy classes of $G$. Then

$$\chi_V = a_1\chi_{V_1} + a_2\chi_{V_2} + \cdots + a_s\chi_{V_s}.$$

Moreover, if $V = {}_{k[G]}k[G]$, then we have seen that

$$V \cong V_1^{n_1} \oplus \cdots \oplus V_s^{n_s},$$

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

$$\chi_V(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{if } g \neq 1, \end{cases}$$

which gives us the nice fact that if $k[G] \cong M_{n_1}(k) \times \cdots \times M_{n_s}(k)$, then

$$\left(\sum_{i=1}^{s} n_i\chi_{V_i}\right)(g) = \sum_{i=1}^{s} n_i\chi_{V_i}(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{if } g \neq 1. \end{cases}$$

# 16 Character tables, an "inner product" of maps (10/20/2021)

Let $G$ be a finite group, and let $k$ be an algebraically closed field with $\mathrm{char}(k) \nmid |G|$. Then

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

as $k$-algebras, where $s$ is the number of conjugacy classes of $G$, and $\sum_{i=1}^{s} n_i^2 = |G|$. Moreover, $k[G]$ has $s$ pairwise non-isomorphic simple modules (or irreducible representations) $V_1, \ldots, V_s$, with $V_i \cong k^{n_i \times 1}$.

Moreover, every left $k[G]$-module $V$ decomposes as

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_s^{a_s},$$

and this decomposition is unique. We also have a representation

$$\rho_V : G \to \mathrm{GL}(V),$$

which gives rise to the character $\chi_V : G \to k$ of $V$, with the formula

$$\chi_V = \sum_{i=1}^{s} a_i\chi_{V_i}.$$

Notice that $\chi_V(1) = \mathrm{Tr}(\rho_V(1)) = \mathrm{Tr}(I_n) = n = \dim_k(V)$, so by taking the module $L = {}_{k[G]}k[G]$, we have

$$\chi_L = \sum_{i=1}^{s} n_i\chi_{V_i},$$

and for $g \in G$, we saw in the previous lecture that

$$\chi_L(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{if } g \neq 1. \end{cases}$$

What are the irreducible representations of a finite abelian group $G$? Assume that $|G| = n$, and $k$ is an algebraically closed field with $\text{char}(k) \nmid n$. We see that $k[G] \cong k^n$, which implies that there are $n$ inequivalent irreducible representations. Now, since $G$ is abelian, we can write

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r},$$

where $C_j$ denotes the cyclic group of order $j$. We can think of this as

$$G \cong \langle x_1 \mid x_1^{d_1} = 1 \rangle \times \cdots \times \langle x_r \mid x_r^{d_r} = 1 \rangle.$$

We know all simple $k[G]$-modules are one-dimensional as $k$-vector spaces. In particular, if $V$ is simple, then

$$\rho_V : G \to \text{GL}_1(k) \cong k^* = k \setminus \{0\}.$$

This means that if $\rho_V(x_i) = \omega_i \in k^*$, then

$$1 = \rho_V(1) = \rho_V(x_i^{d_i}) = \omega_i^{d_i}.$$

That is, each $\omega_i$ is a $d_i$-th root of unity, so there are $d_1 \cdots d_r = |G|$ choices for $\rho_V$. On the other hand, we already know that there are $d_1 \cdots d_r$ pairwise inequivalent irreducible representations, so these are in fact all of them. In this case, notice that $\chi_V = \rho_V$.

**Example 16.1**

Suppose that $G_1 = C_2 \times C_2 = \langle x \mid x^2 = 1 \rangle \times \langle y \mid y^2 = 1 \rangle$ and $G_2 = C_4 = \langle z \mid z^4 = 1 \rangle$. We compute the character tables of $G_1$ and $G_2$; namely, the characters of the representations.

| $G_1$ | 1 | $x$ | $y$ | $xy$ |
|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | $-1$ | $-1$ |
| $\chi_3$ | 1 | $-1$ | 1 | $-1$ |
| $\chi_4$ | 1 | $-1$ | $-1$ | 1 |

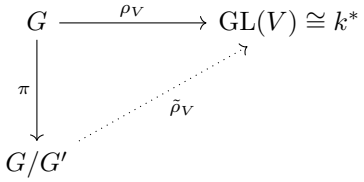
| $G_2$ | 1 | $z$ | $z^2$ | $z^3$ |
|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $i$ | $-1$ | $-i$ |
| $\chi_3$ | 1 | $-1$ | 1 | $-1$ |
| $\chi_4$ | 1 | $-i$ | $-1$ | $-i$ |

**Example 16.2**

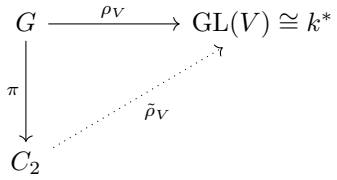
Let $G = S_3$ and $k = \mathbb{C}$. We recall that $\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. Then $S_3$ has three pairwise inequivalent irreducible representations, and these have dimensions 1, 1, and 2 respectively. Moreover, recall that for a finite-dimensional $k[G]$-module $V$, its character $\chi_V : G \to k$ is a class function. Therefore, to compute the character table of $S_3$, it suffices to consider the values of the characters on each conjugacy class.

First, the identity element is always sent to the dimension of the representation, so we obtain $\chi_1(\text{id}) = \chi_2(\text{id}) = 1$ and $\chi_3(\text{id}) = 2$. Since $(12)^2 = \text{id}$, we have $\chi_i((12))^2 = \chi_i(\text{id}) = 1$ for $i \in \{1, 2\}$, yielding $\chi_1((12)) = 1$ and $\chi_2((12)) = -1$.

Next, recall from Assignment 3 Question 1 that the one-dimensional irreducible representations come from $G/G'$. More precisely, if $V$ is a simple one-dimensional $k[G]$-module, then we obtain the following commutative diagram, where we note that $k^*$ is an abelian group.




In our case, we have $S_3' = A_3$ and $S_3/A_3 = C_2$, which gives us the following diagram.




In particular, everything in $A_3$ has to be in the kernel and gets sent to 1, so $\chi_1((123)) = \chi_2((123)) = 1$. The last row is more difficult to find directly. However, if we know everything in the character table except for the last row, then there's an easy way to compute it. Let

$$\chi_L = \chi_1 + \chi_2 + 2\chi_3.$$

We recall that $\chi_L(\sigma) = 0$ for all $\sigma \neq \mathrm{id}$; in particular, we have $\chi_L((12)) = \chi_L((123)) = 0$. This gives

$$\chi_1((12)) + \chi_2((12)) + 2\chi_3((12)) = 0,$$

and rearranging this, we obtain

$$\chi_3((12)) = -\frac{1}{2}(\chi_1((12)) + \chi_2((12)) = -\frac{1}{2}(1 + (-1)) = 0.$$

Similarly, we find that $\chi_3((123)) = -1$, so we have now completed the character table of $S_3$.

| $S_3$ | [id] | [(12)] | [(123)] |
|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 |
| $\chi_2$ | 1 | −1 | 1 |
| $\chi_3$ | 2 | 0 | −1 |

**Remark 16.3**

Notice that for the $\mathbb{C}[S_3]$-module $V = \mathbb{C}^{3\times 1}$ given the permutation representation, $\chi_V(\sigma)$ gives the number of fixed points of $\sigma \in S_3$. Then we have $\chi_V(\mathrm{id}) = 3$, $\chi_V((12)) = 1$, and $\chi_V((123)) = 0$, so we find that $\chi_V = \chi_1 + \chi_3$ simply from the character table.

**Example 16.4**

Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where $ij = k$ and $i^2 = j^2 = k^2 = -1$. Recall that

$$\mathbb{C}[Q_8] \cong \mathbb{C}^4 \times M_2(\mathbb{C}),$$

so $Q_8$ has five conjugacy classes; they are $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, and $\{k, -k\}$. Observe that

$Q_8' = \{\pm 1\}$, which implies that

$$Q_8/Q_8' = \langle i, j \mid i^2 = j^2 = 1,\, ij = ji \rangle \cong C_2 \times C_2.$$

Now, the first four rows of the character table are easy to compute, as well as the first column.

| $Q_8$ | $[1]$ | $[-1]$ | $[i]$ | $[j]$ | $[k] = [ij]$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | 1 | $-1$ | $-1$ |
| $\chi_3$ | 1 | 1 | $-1$ | 1 | $-1$ |
| $\chi_4$ | 1 | 1 | $-1$ | $-1$ | 1 |
| $\chi_5$ | 2 | | | | |

To obtain the last row, we apply the same trick as the previous example; we set

$$\chi_L = \chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5$$

and use the fact that $\chi_L(g) = 0$ when $g \neq 1$. This will finish the character table.

| $Q_8$ | $[1]$ | $[-1]$ | $[i]$ | $[j]$ | $[k] = [ij]$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | 1 | $-1$ | $-1$ |
| $\chi_3$ | 1 | 1 | $-1$ | 1 | $-1$ |
| $\chi_4$ | 1 | 1 | $-1$ | $-1$ | 1 |
| $\chi_5$ | 2 | $-2$ | 0 | 0 | 0 |

We will soon see the interesting fact that if $G$ is a group and $\Phi, \Psi : G \to \mathbb{C}$ are maps, then we can define an "inner product" by

$$\langle \Phi, \Psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \Phi(g)\Psi(g^{-1}).$$

Note that this is not actually an inner product, as it fails to satisfy some properties. However, we see that it is $\mathbb{C}$-bilinear; indeed, for $\lambda \in \mathbb{C}$, we have

$$\langle \Phi_1 + \lambda\Phi_2, \Psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} (\Phi_1(g) + \lambda\Phi_2(g))\Psi(g^{-1}) = \langle \Phi_1, \Psi \rangle_G + \lambda \langle \Phi_2, \Psi \rangle_G,$$

and the other direction can be checked similarly. Moreover, $\langle \cdot, \cdot \rangle_G$ is symmetric, since

$$\langle \Phi, \Psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \Phi(g)\Psi(g^{-1}) = \frac{1}{|G|} \sum_{x \in G} \Phi(x^{-1})\Psi(x) = \langle \Psi, \Phi \rangle_G,$$

where in the second equality, we used the substitution $x = g^{-1}$.

In the following lectures, we'll see that characters are orthonormal with respect to this "inner product".

# 17 Orthogonality of characters over "inner product" (10/22/2021)

For this part of the course, we'll be working over $\mathbb{C}$. Last time, for a pair of maps $\Phi, \Psi : G \to \mathbb{C}$, we defined the "inner product"

$$\langle \Phi, \Psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \Phi(g)\Psi(g^{-1}),$$

and saw that this was $\mathbb{C}$-bilinear and symmetric. We now make an important remark towards showing that $\langle \cdot, \cdot \rangle_G$ is a true inner product when working with characters.

**Remark 17.1**

If $\chi$ is a character, then $\chi(g^{-1}) = \overline{\chi(g)}$.

Proof. We have $\chi(g) = \mathrm{Tr}(\rho(g))$ where $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ is a representation. Let $g \in G$. Notice that $\rho(g)$ is triangularizable, so

$$S^{-1}\rho(g)S = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

where $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of $\rho(g)$. Since $G$ is finite, there exists an integer $d \geq 1$ such that $g^d = 1$. Then, we can write

$$\rho(g)^d = \rho(g^d) = \rho(1) = I,$$

which implies that

$$(S^{-1}\rho(g)S)^d = (S^{-1}\rho(g)S)(S^{-1}\rho(g)S)\cdots(S^{-1}\rho(g)S) = S^{-1}\rho(g)^d S = S^{-1}IS = I.$$

Therefore, we find that

$$\begin{pmatrix} \lambda_1^d & & * \\ & \ddots & \\ 0 & & \lambda_n^d \end{pmatrix} = I.$$

In particular, $\lambda_1, \ldots, \lambda_n$ are $d$-th roots of unity. Since $\rho(g^{-1})$ is the inverse of $\rho(g)$, we have

$$\rho(g^{-1}) = \begin{pmatrix} \lambda_1^{-1} & & * \\ & \ddots & \\ 0 & & \lambda_n^{-1} \end{pmatrix}.$$

Finally, it follows that

$$\chi(g^{-1}) = \mathrm{Tr}(\rho(g^{-1})) = \lambda_1^{-1} + \cdots + \lambda_n^{-1} = \overline{\lambda_1} + \cdots + \overline{\lambda_n} = \overline{\chi(g)}. \qquad \square$$

Let $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the conjugacy classes of $G$, and let $g_i$ be a representative of $\mathcal{C}_i$ for each $i = 1, \ldots, s$. If $\chi_1$ and $\chi_2$ are characters, then

$$\begin{aligned} \langle \chi_1, \chi_2 \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\chi_2(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} \\ &= \frac{1}{|G|} \sum_{i=1}^{s} \sum_{h \in \mathcal{C}_i} \chi_1(h)\overline{\chi_2(h)} \\ &= \frac{1}{|G|} \sum_{i=1}^{s} |\mathcal{C}_i| \chi_1(g_i)\overline{\chi_2(g_i)}, \end{aligned}$$

where the last equality follows since $\chi_1$ and $\chi_2$ are class functions.

We'll now show that if $V_1, \ldots, V_s$ are the inequivalent irreducible representations of $G$ with $\chi_i = \chi_{V_i}$, then $\langle \chi_i, \chi_j \rangle_G = \delta_{ij}$, where $\delta_{ij}$ denotes the Kronecker delta.

First, we will consider an averaging trick. Let $G$ be a finite group, and let $k$ be an algebraically closed field such that $\text{char}(k) \nmid |G|$. Let $V$ and $W$ be $k[G]$-modules. If $T : V \to W$ is a $k$-linear transformation, we can define a map $\hat{T} : V \to W$ where for $v \in V$, we have

$$\hat{T}(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot T(g^{-1} \cdot v).$$

This makes sense because $T(g^{-1} \cdot v) \in W$.

**Theorem 17.2**

If $T : V \to W$ is $k$-linear, then $\hat{T} : V \to W$ as above is $k[G]$-linear.

Proof. It suffices to show that $\hat{T}(h \cdot v) = h \cdot \hat{T}(v)$ for all $h, v \in V$, because every element in $k[G]$ is a linear combination of elements in $G$. By a direct computation, we have

$$\begin{aligned}
\hat{T}(h \cdot v) &= \frac{1}{|G|} \sum_{g \in G} g \cdot T(g^{-1} \cdot (h \cdot v)) \\
&= \frac{1}{|G|} \sum_{g \in G} g \cdot T((g^{-1} \cdot h) \cdot v) \\
&= \frac{1}{|G|} \sum_{x \in G} h \cdot x \cdot T(x^{-1} \cdot v) \quad \text{(substitute } x = h^{-1}g\text{)} \\
&= h \cdot \frac{1}{|G|} \sum_{x \in G} x \cdot T(x^{-1} \cdot v) = h \cdot \hat{T}(v).
\end{aligned}$$

□

.

We now return to working over $\mathbb{C}$, and look at some consequences of the previous result.

If $V$ and $W$ are non-isomorphic simple $\mathbb{C}[G]$-modules and $T : V \to W$ is $\mathbb{C}$-linear, then $\hat{T} \equiv 0$ since $\text{Hom}_{\mathbb{C}[G]}(V, W) = (0)$. On the other hand, recall that

$$\text{Hom}_{\mathbb{C}[G]}(V, V) = \text{End}_{\mathbb{C}[G]}(V) = \mathbb{C}$$

by Schur's lemma. This implies that if $T : V \to V$ is $\mathbb{C}$-linear, then $\hat{T} : V \to V$ is just scalar multiplication by some $\lambda \in \mathbb{C}$. That is, for all $v \in V$, we have

$$\hat{T}(v) = \lambda v.$$

We now determine what $\lambda$ is. Let $L_g : V \to V$ be the map given by $L_g(v) = g \cdot v$. Then

$$\begin{aligned}
\text{Tr}(\hat{T}) &= \text{Tr}\left( \frac{1}{|G|} \sum_{g \in G} L_g \circ T \circ L_g^{-1} \right) \\
&= \frac{1}{|G|} \sum_{g \in G} \text{Tr}(L_g \circ T \circ L_g^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \text{Tr}(T) = \text{Tr}(T).
\end{aligned}$$

On the other hand, we already know that $\text{Tr}(\hat{T}) = \lambda \cdot \dim V$, so

$$\lambda = \frac{\text{Tr}(T)}{\dim V}.$$

Let $V$ and $W$ be two simple non-isomorphic $\mathbb{C}[G]$-modules with bases $\{v_1, \dots, v_m\}$ and $\{w_1, \dots, w_n\}$ respectively. Then, we obtain representations

$$\rho_1 : G \to \mathrm{GL}_m(\mathbb{C}) \cong \mathrm{GL}(V),$$
$$\rho_2 : G \to \mathrm{GL}_n(\mathbb{C}) \cong \mathrm{GL}(W).$$

Note that if we want to find the matrix of a linear transformation, we pick our basis, and to get the $j$-th column, we apply the transformation to the $j$-th element of our basis. In particular, we find that

$$\rho_1(g) \cdot v_j = \sum_{i=1}^{m} \rho_1(g)_{ij} \cdot v_i, \qquad \rho_2(g) \cdot w_j = \sum_{i=1}^{n} \rho_2(g)_{ij} \cdot w_i.$$

Notice that we can view $\rho_1(g) = (\rho_1(g))_{ij}$ and $\rho_2(g) = (\rho_2(g))_{ij}$ as functions from $G$ to $\mathbb{C}$ by looking at their $(i,j)$-th entries.

**Theorem 17.3**

For all $1 \le i, j \le m$ and $1 \le p, q \le n$, we have $\langle (\rho_1)_{ij}, (\rho_2)_{pq} \rangle_G = 0$.

Proof. Fix some $1 \le i \le m$ and $1 \le q \le n$. Define a linear transformation $T : V \to W$ by $T(v_i) = w_q$, and $T(v_k) = 0$ whenever $k \neq i$. Then $\hat{T} \equiv 0$ since $V$ and $W$ are non-isomorphic simple modules. For all $1 \le j \le m$, we have

$$0 = \hat{T}(v_j) = \frac{1}{|G|} \sum_{g \in G} g \cdot T(g^{-1} \cdot v_j) = \frac{1}{|G|} \sum_{g \in G} \rho_2(g) \cdot T(\rho_1(g^{-1}) \cdot v_j).$$

By definition, we have

$$\rho_1(g^{-1}) \cdot v_j = \sum_{k=1}^{m} \rho_1(g^{-1})_{kj} \cdot v_k,$$

which gives us

$$T(\rho_1(g^{-1}) \cdot v_j) = T\left( \sum_{k=1}^{m} \rho_1(g^{-1})_{kj} \cdot v_k \right) = \rho_1(g^{-1})_{ij} \cdot T(v_i) = \rho_1(g^{-1})_{ij} \cdot w_q,$$

where the second equality comes from throwing everything away except when $k = i$. Finally, we obtain

$$\begin{aligned} 0 &= \frac{1}{|G|} \sum_{g \in G} \rho_2(g) \cdot T(\rho_1(g) \cdot v_j) \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_1(g^{-1})_{ij} \cdot \rho_2(g) \cdot w_q \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_1(g^{-1})_{ij} \left[ \sum_{k=1}^{n} \rho_2(g)_{kq} \cdot w_k \right] \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_1(g^{-1})_{ij} \cdot \rho_2(g)_{pq} \\ &= \langle (\rho_2)_{pq}, (\rho_1)_{ij} \rangle_G = \langle (\rho_1)_{ij}, (\rho_2)_{pq} \rangle_G. \end{aligned}$$

Since $1 \le i, j \le m$ and $1 \le p, q \le n$ were arbitrary, we are done. □

Now, we can show that the characters are orthonormal.

**Corollary 17.4**

If $V$ and $W$ are non-isomorphic simple $\mathbb{C}[G]$-modules, then $\langle \chi_V, \chi_W \rangle = 0$.

Proof. Suppose that $\dim V = m$ and $\dim W = n$. Then we obtain representations

$$\rho_1 : G \to \mathrm{GL}(V) \cong \mathrm{GL}_m(\mathbb{C}),$$
$$\rho_2 : G \to \mathrm{GL}(W) \cong \mathrm{GL}_n(\mathbb{C}).$$

We can write these in matrix form as

$$\rho_1(g) = ((\rho_1)_{ij}(g))_{1 \le i,j \le m},$$
$$\rho_2(g) = ((\rho_2)_{ij}(g))_{1 \le i,j \le n}.$$

By Theorem 17.3, we have $\langle (\rho_1)_{ij}, (\rho_2)_{pq} \rangle = 0$ for all $1 \le i, j \le m$ and $1 \le p, q \le n$. Notice that

$$\chi_V(g) = \mathrm{Tr}(\rho_1(g)) = \sum_{i=1}^{m} (\rho_1)_{ii}(g),$$
$$\chi_W(g) = \mathrm{Tr}(\rho_2(g)) = \sum_{j=1}^{n} (\rho_2)_{jj}(g),$$

and it follows from the bilinearity of our "inner product" that

$$\langle \chi_V, \chi_W \rangle_G = \left\langle \sum_{i=1}^{m} (\rho_1)_{ii}, \sum_{j=1}^{n} (\rho_2)_{jj} \right\rangle_G = 0. \qquad \square$$

# 18 Orthonormality of characters over "inner product" (10/25/2021)

Let $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the conjugacy classes of $G$, and let $g_i, \ldots, g_s$ be representatives of the conjugacy classes. We showed that for characters $\chi$ and $\chi'$, we have

$$\langle \chi, \chi' \rangle_G = \frac{1}{|G|} \sum_{i=1}^{s} |\mathcal{C}_i| \chi(g_i) \overline{\chi'(g_i)}.$$

Now, for general class functions $\Theta, \Omega : G \to \mathbb{C}$, we define

$$\langle \Theta, \Omega \rangle_G = \frac{1}{|G|} \sum_{i=1}^{s} |\mathcal{C}_i| \Theta(g_i) \overline{\Omega(g_i)}.$$

This definition turns the space of $\mathbb{C}$-valued class functions into a complex inner product space; we notice that

$$\langle \Theta, \Theta \rangle_G = \frac{1}{|G|} \sum_{i=1}^{s} |\mathcal{C}_i| |\Theta(g_i)|^2 \ge 0.$$

We'll show that if $\chi_1, \ldots, \chi_s$ are the inequivalent irreducible characters, then $\chi_1, \ldots, \chi_s$ forms an orthonormal basis for the $\mathbb{C}$-valued class functions.

First, we observe that given a class function $\Theta : G \to \mathbb{C}$, we have an element given by $(\Theta(g_1), \ldots, \Theta(g_s)) \in \mathbb{C}^s$. In particular, this gives us a bijection between the $\mathbb{C}$-valued class functions and $\mathbb{C}^s$, since we can define a class function $\Theta : G \to \mathbb{C}$ by picking $s$ values in $\mathbb{C}$ and assigning them to the representatives $g_1, \ldots, g_s$. Therefore, the space of $\mathbb{C}$-valued class functions is $s$-dimensional.

Notice that Corollary 17.4 already shows orthogonality. Let $V$ be a simple $\mathbb{C}[G]$-module with a representation

$$\rho : G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{C}),$$

where $V$ has basis $\{v_1, \dots, v_n\}$. Then we have $\rho(g) \cdot v_j = \sum_{i=1}^n \rho_{ij}(g) \cdot v_i$, where

$$\rho(g) = \begin{pmatrix} \rho_{11}(g) & \cdots & \rho_{1n}(g) \\ \vdots & \ddots & \vdots \\ \rho_{n1}(g) & \cdots & \rho_{nn}(g) \end{pmatrix}.$$

**Lemma 18.1**

For all $1 \leq i, j, s, t \leq n$, we have

$$\langle \rho_{ij}, \rho_{st} \rangle_G = \frac{1}{\dim V} \delta_{it} \delta_{js} = \frac{1}{n} \delta_{it} \delta_{js},$$

where $\delta_{ij}$ denotes the Kronecker delta.

With the lemma, we can immediately prove orthonormality! Let $\chi = \mathrm{Tr}(\rho)$, so $\chi(g) = \rho_{11}(g) + \cdots + \rho_{nn}(g)$. Then we find that

$$\langle \chi, \chi \rangle_G = \langle \rho_{11} + \cdots + \rho_{nn}, \rho_{11} + \cdots + \rho_{nn} \rangle_G = \sum_{i=1}^n \sum_{j=1}^n \langle \rho_{ii}, \rho_{jj} \rangle_G.$$

Lemma 18.1 tells us that

$$\langle \rho_{ii}, \rho_{jj} \rangle_G = \begin{cases} 0 & \text{if } i \neq j, \\ 1/n & \text{if } i = j. \end{cases}$$

It follows that

$$\langle \chi, \chi \rangle_G = \sum_{i=1}^n \langle \rho_{ii}, \rho_{ii} \rangle_G = \sum_{i=1}^n \frac{1}{n} = 1.$$

Recall that if $T : V \to V$ is $\mathbb{C}$-linear, then we defined

$$\hat{T}(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot T(g^{-1} \cdot v),$$

which we showed was $\mathbb{C}[G]$-linear. Moreover, when $V$ is simple, we showed that $\hat{T}(v) = \lambda v$, where $\lambda = \mathrm{Tr}(T)/\dim V$. We now prove Lemma 18.1.

Proof of Lemma 18.1. Fix a basis $\{v_1, \dots, v_n\}$ for $V$. By definition, we know that

$$\rho(g) \cdot v_j = \sum_{i=1}^n \rho_{ij}(g) \cdot v_i,$$

where $\rho(g)$ denotes the linear transformation, and $\rho_{ij}(g) \in \mathbb{C}$ is an entry of the matrix. Let $T : V \to V$ be the $\mathbb{C}$-linear transformation defined by

$$T(v_k) = \begin{cases} v_t & \text{if } k = i, \\ 0 & \text{if } k \neq i. \end{cases}$$

Note that $\mathrm{Tr}(T) = \delta_{it}$, which means that

$$\hat{T}(v) = \frac{\delta_{it}}{n}$$

for all $v \in V$, where $n = \dim V$. In particular, notice that

$$\frac{\delta_{it}}{n} \cdot v_j = \hat{T}(v_j) = \frac{1}{|G|} \sum_{g \in G} \rho(g) \cdot T(\rho(g^{-1}) \cdot v_j). \tag{18.1}$$

We can write

$$T(\rho(g^{-1}) \cdot v_j) = T\left( \sum_{k=1}^{n} \rho(g^{-1})_{kj} \cdot v_k \right) = T(\rho(g^{-1})_{ij} \cdot v_i) = \rho(g^{-1})_{ij} \cdot v_t,$$

since we can throw out the terms where $k \neq i$. Following from equation (18.1), we get

$$\begin{aligned}
\frac{\delta_{it}}{n} \cdot v_j &= \frac{1}{|G|} \sum_{g \in G} \rho(g) \cdot T(\rho(g^{-1}) \cdot v_j) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(g) \cdot (\rho(g^{-1})_{ij} \cdot v_t) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1}_{ij} \cdot (\rho(g) \cdot v_t) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1}_{ij} \left( \sum_{\ell=1}^{n} \rho(g)_{\ell t} \cdot v_\ell \right) \\
&= \sum_{\ell=1}^{n} \left( \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1}_{ij} \cdot \rho(g)_{\ell t} \right) \cdot v_\ell \\
&= \sum_{\ell=1}^{n} \langle \rho_{\ell t}, \rho_{ij} \rangle_G \cdot v_\ell.
\end{aligned}$$

Now, we compare the coefficients. When $\ell \neq j$, the coefficient of $v_\ell$ on the left-hand side is 0, whereas it is $\langle \rho_{\ell t}, \rho_{ij} \rangle_G$ on the right-hand side. When $\ell = j$, the coefficients of $v_\ell$ are $\delta_{it}/n$ and $\langle \rho_{jt}, \rho_{ij} \rangle_G$ on the left-hand side and right-hand side, respectively. We conclude that

$$\langle \rho_{ij}, \rho_{\ell t} \rangle_G = \langle \rho_{\ell t}, \rho_{ij} \rangle_G = \delta_{\ell j} \cdot \frac{\delta_{it}}{n},$$

which completes the proof of the lemma. □

**Theorem 18.2**

If $\chi_1, \ldots, \chi_s$ are the inequivalent irreducible characters, then $\chi_1, \ldots, \chi_s$ forms an orthonormal basis for the space of $\mathbb{C}$-valued class functions.

Proof. Notice that $\langle \chi_i, \chi_j \rangle_G = \delta_{ij}$ for all $1 \leq i, j \leq s$. Therefore, $\chi_1, \ldots, \chi_s$ are linearly independent as the space of $\mathbb{C}$-valued class functions is $s$-dimensional. Moreover, $\chi_1, \ldots, \chi_s$ spans, so they form an orthonormal basis. □

What is the significance of this result? Recall that if $V$ is a representation of $G$, then it can be decomposed as

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_s^{a_s},$$

where $V_1, \ldots, V_s$ are simples. Letting $\chi_i = \chi_{V_i}$, we have the formula

$$\chi_V = a_1 \chi_1 + \cdots + a_s \chi_s.$$

In particular, notice that by orthonormality, we have

$$\langle \chi_V, \chi_i \rangle_G = \langle a_1 \chi_1 + \cdots + a_s \chi_s, \chi_i \rangle_G = \langle a_i \chi_i, \chi_i \rangle_G = a_i \|\chi_i\|^2 = a_i.$$

# 19 Character tables of $S_4$ and $S_5$ (10/27/2021)

Recall that we can write $\mathbb{C}[G] \cong M_{n_i}(\mathbb{C}) \times \cdots \times M_{n_s}(\mathbb{C})$, where $s$ is the number of conjugacy classes of $G$. Then, we obtain $s$ irreducible characters $\chi_1, \ldots, \chi_s$, with

$$\chi_i(1) = n_i,$$

where we call $n_i$ the degree of $\chi_i$ for each $i = 1, \ldots, s$. We also saw that

$$\delta_{ij} = \langle \chi_i, \chi_j \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)}.$$

For a $\mathbb{C}[G]$-module $V \cong V_1^{a_1} \oplus \cdots \oplus V_s^{a_s}$, we have the formula

$$\chi_V = a_1\chi_i + \cdots + a_s\chi_s,$$

where $\chi_i = \chi_{V_i}$ for all $i = 1, \ldots, s$. We saw that this gives $a_i = \langle \chi_V, \chi_i \rangle_G$ by orthonormality. In particular, we find that

$$\langle \chi_V, \chi_V \rangle_G = \sum_{i=1}^{s} a_i^2 \|\chi_i\|^2 = \sum_{i=1}^{s} a_i^2.$$

Let's use our results to find the character tables of $S_4$ and $S_5$.

**Example 19.1**

To find the character table of $S_4$, we first recall that $\mathbb{C}[S_4] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}) \times M_3(\mathbb{C}) \times M_3(\mathbb{C})$, which we determined in Example 11.3. We also saw that the 5 conjugacy classes and their sizes were

$$\begin{aligned} \#[\mathrm{id}] &= 1, \\ \#[(12)] &= 6, \\ \#[(123)] &= 8, \\ \#[(1234)] &= 6, \\ \#[(12)(34)] &= 3. \end{aligned}$$

Since $S_4' = A_4$, we have $S_4/S_4' = S_4/A_4 \cong C_2$, so we can immediately determine the degree 1 characters, as well as the first column as we know the degrees of all the characters.

| $S_4$ | 1 [id] | 6 [(12)] | 8 [(123)] | 6 [(1234)] | 3 [(12)(34)] |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi_3$ | 2 | | | | |
| $\chi_4$ | 3 | | | | |
| $\chi_5$ | 3 | | | | |

To compute the rest of the character table, we'll usually find a nice representation of the group in practice. Consider the permutation representation $P : S_4 \to \mathrm{GL}_4(\mathbb{C})$ given by

$$P(\sigma)e_j = e_{\sigma(j)}.$$

Recall that $\chi_P(\sigma)$ is the number of fixed points of $\sigma \in S_4$. For now, let's add $\chi_P$ to the character table.

| $S_4$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{6}{[(12)]}$ | $\overset{8}{[(123)]}$ | $\overset{6}{[(1234)]}$ | $\overset{3}{[(12)(34)]}$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi_3$ | 2 | | | | |
| $\chi_4$ | 3 | | | | |
| $\chi_5$ | 3 | | | | |
| $\chi_P$ | 4 | 2 | 1 | 0 | 0 |

By Exercise 5 in Homework 3, we find that

$$\langle \chi_P, \chi_P \rangle = \frac{1}{4!} \sum_{\sigma \in S_4} \mathrm{fix}(\sigma)^2 = \frac{1}{24}(1 \cdot 4^2 + 6 \cdot 2^2 + 8 \cdot 1^2 + 6 \cdot 0^2 + 3 \cdot 0^2) = 2,$$

where $\mathrm{fix}(\sigma)$ denotes the number of fixed points of $\sigma$. In particular, we see that $\chi_P$ is not an irreducible character, but recalling the formula

$$\langle \chi_V, \chi_V \rangle = \sum_{i=1}^{s} a_i^2,$$

we see that $\chi_P$ can be decomposed as the sum of two irreducible components. Now, looking at $\langle \chi_P, \chi_1 \rangle$, we obtain

$$\langle \chi_P, \chi_1 \rangle = \frac{1}{24}(4 \cdot 1 \cdot 1 + 2 \cdot 1 \cdot 6 + 1 \cdot 1 \cdot 8) = 1.$$

This means that $\chi_P = \chi_1 + \chi$, where $\chi$ is some irreducible character. In other words, $\chi_P - \chi_1$ is an irreducible character. Notice that $\chi_P(\mathrm{id}) - \chi_1(\mathrm{id}) = 4 - 1 = 3$, so this character is one of $\chi_4$ or $\chi_5$. Let's say we have $\chi_4 = \chi_P - \chi_1$, since we can just flip the rows if necessary. This allows us to fill out another row in the character table.

| $S_4$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{6}{[(12)]}$ | $\overset{8}{[(123)]}$ | $\overset{6}{[(1234)]}$ | $\overset{3}{[(12)(34)]}$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi_3$ | 2 | | | | |
| $\chi_4$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_5$ | 3 | | | | |
| $\chi_P$ | 4 | 2 | 1 | 0 | 0 |

On Question 1 of Homework 4, we will show that if $\chi$ is a degree 1 character and for each $d \geq 1$, we let $X_d$ be the set of irreducible characters of degree $d$, then multiplication by $\chi$ permutes $X_d$ for all $d \geq 1$.

In particular, since $\chi_2$ is a degree 1 character, we can multiply $\chi_4$ with $\chi_2$ to obtain the other degree 3 character $\chi_5 = \chi_4 \cdot \chi_2$, as multiplication by $\chi_2$ permutes $X_3 = \{\chi_4, \chi_5\}$. Similarly, if we multiply $\chi_5$ with $\chi_2$, we again obtain $\chi_4$.

| $S_4$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{6}{[(12)]}$ | $\overset{8}{[(123)]}$ | $\overset{6}{[(1234)]}$ | $\overset{3}{[(12)(34)]}$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi_3$ | 2 | | | | |
| $\chi_4$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_5$ | 3 | $-1$ | 0 | 1 | $-1$ |
| $\chi_P$ | 4 | 2 | 1 | 0 | 0 |

What happens if we do this with $\chi_3$? We have $X_2 = \{\chi_3\}$, and we know that multiplication by $\chi_2$ must permute $X_2$, so that $\chi_3 \cdot \chi_2 = \chi_3$. This tells us that $\chi_3((12)) = \chi_3((1234)) = 0$, since $\chi_2((12)) = \chi_2((1234)) = -1$. Let's now try to find the remaining entries in the row.

| $S_4$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{6}{[(12)]}$ | $\overset{8}{[(123)]}$ | $\overset{6}{[(1234)]}$ | $\overset{3}{[(12)(34)]}$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi_3$ | 2 | 0 | $a$ | 0 | $b$ |
| $\chi_4$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_5$ | 3 | $-1$ | 0 | 1 | $-1$ |
| $\chi_P$ | 4 | 2 | 1 | 0 | 0 |

We take the inner product of $\chi_3$ with some of the other irreducible characters. Observe that

$$0 = \langle \chi_3, \chi_1 \rangle = \frac{1}{24}(2 \cdot 1 \cdot 1 + a \cdot 1 \cdot 8 + b \cdot 1 \cdot 3) = \frac{1}{24}(2 + 8a + 3b),$$
$$0 = \langle \chi_3, \chi_4 \rangle = \frac{1}{24}(2 \cdot 3 \cdot 1 + a \cdot 0 \cdot 8 + b \cdot (-1) \cdot 3) = \frac{1}{24}(6 - 3b).$$

Solving this yields $a = -1$ and $b = 2$, so we have now completed the character table of $S_4$.

| $S_4$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{6}{[(12)]}$ | $\overset{8}{[(123)]}$ | $\overset{6}{[(1234)]}$ | $\overset{3}{[(12)(34)]}$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi_3$ | 2 | 0 | $-1$ | 0 | 2 |
| $\chi_4$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_5$ | 3 | $-1$ | 0 | 1 | $-1$ |

### Example 19.2

Let's now find the character table of $S_5$. Note that $S_5$ has 7 conjugacy classes; their sizes are

$$\begin{aligned} \#[\mathrm{id}] &= 1, \\ \#[(12)] &= 10, \\ \#[(123)] &= 20, \\ \#[(1234)] &= 30, \\ \#[(12345)] &= 24, \\ \#[(12)(34)] &= 15, \\ \#[(12)(345)] &= 20. \end{aligned}$$

These sizes can be determined using Exercise 6 of Homework 3. This states that if $\sigma \in S_n$ has disjoint cycle structure with $\lambda_i \geq 0$ $i$-cycles for $i = 1, \ldots, n$ (so that $\sum_{i=1}^n i\lambda_i = n$), then the conjugacy class of $\sigma$ has size

$$\frac{n!}{\prod_{i=1}^n \lambda_i! i^{\lambda_i}}.$$

Now, we recall that $S_5' = A_5$, so $S_5/S_5' = S_5/A_5 \cong C_2$. Then the odd cycles get sent to $-1$ and the even cycles get sent to 1, so we obtain the first two rows of the character table.

| $S_5$ | $^{1}$[id] | $^{10}$[(12)] | $^{20}$[(123)] | $^{30}$[(1234)] | $^{24}$[(12345)] | $^{15}$[(12)(34)] | $^{20}$[(12)(345)] |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | | | | | | | |
| $\chi_4$ | | | | | | | |
| $\chi_5$ | | | | | | | |
| $\chi_6$ | | | | | | | |
| $\chi_7$ | | | | | | | |

Take the permutation representation $P : S_5 \to \mathrm{GL}_5(\mathbb{C})$ given by

$$P(\sigma)e_j = e_{\sigma(j)}.$$

Again, $\chi_P(\sigma)$ gives the number of fixed points of $\sigma$, so let's add $\chi_P$ to the character table for now.

| $S_5$ | $^{1}$[id] | $^{10}$[(12)] | $^{20}$[(123)] | $^{30}$[(1234)] | $^{24}$[(12345)] | $^{15}$[(12)(34)] | $^{20}$[(12)(345)] |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | | | | | | | |
| $\chi_4$ | | | | | | | |
| $\chi_5$ | | | | | | | |
| $\chi_6$ | | | | | | | |
| $\chi_7$ | | | | | | | |
| $\chi_P$ | 5 | 3 | 2 | 1 | 0 | 1 | 0 |

By Exercise 5 of Homework 3, we have

$$\langle \chi_P, \chi_P \rangle = \frac{1}{5!} \sum_{\sigma \in S_5} \mathrm{fix}(\sigma)^2 = 2.$$

We compute that

$$\langle \chi_P, \chi_1 \rangle = \frac{1}{5!}(5 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot 10 + 2 \cdot 1 \cdot 20 + 1 \cdot 1 \cdot 30 + 1 \cdot 1 \cdot 15) = 1.$$

As in the previous example, this tells us that $\chi_P - \chi_1$ is an irreducible character. Since $\chi_P(\mathrm{id}) - \chi_1(\mathrm{id}) = 5 - 1 = 4$, we obtain an irreducible character $\chi_3 = \chi_P - \chi_1$ of degree 4.

| $S_5$ | $^{1}$[id] | $^{10}$[(12)] | $^{20}$[(123)] | $^{30}$[(1234)] | $^{24}$[(12345)] | $^{15}$[(12)(34)] | $^{20}$[(12)(345)] |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 4 | 2 | 1 | 0 | $-1$ | 0 | $-1$ |
| $\chi_4$ | | | | | | | |
| $\chi_5$ | | | | | | | |
| $\chi_6$ | | | | | | | |
| $\chi_7$ | | | | | | | |
| $\chi_P$ | 5 | 3 | 2 | 1 | 0 | 1 | 0 |

We can also take $\chi_4 = \chi_3 \cdot \chi_2$ to get another irreducible character.

| $S_5$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{10}{[(12)]}$ | $\overset{20}{[(123)]}$ | $\overset{30}{[(1234)]}$ | $\overset{24}{[(12345)]}$ | $\overset{15}{[(12)(34)]}$ | $\overset{20}{[(12)(345)]}$ |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 4 | 2 | 1 | 0 | $-1$ | 0 | $-1$ |
| $\chi_4$ | 4 | $-2$ | 1 | 0 | $-1$ | 0 | 1 |
| $\chi_5$ | | | | | | | |
| $\chi_6$ | | | | | | | |
| $\chi_7$ | | | | | | | |
| $\chi_P$ | 5 | 3 | 2 | 1 | 0 | 1 | 0 |

Now, let $a = \chi_5(\mathrm{id})$, $b = \chi_6(\mathrm{id})$, and $c = \chi_7(\mathrm{id})$. Then we know that

$$1^2 + 1^2 + 4^2 + 4^2 + a^2 + b^2 + c^2 = 120,$$

or equivalently,

$$a^2 + b^2 + c^2 = 86.$$

Therefore, we have $2 \leq a, b, c \leq 9$, and we can deduce that $(a, b, c) = (5, 5, 6)$. We have $X_6 = \{\chi_7\}$, and since $\chi_2$ is of degree 1, we have $\chi_7 \cdot \chi_2 = \chi_7$, which tells us that $\chi_7((12)) = \chi((1234)) = \chi((12)(345)) = 0$, since their counterparts in $\chi_2$ are equal to $-1$. We can now fill out the first column and some of the entries of $\chi_7$.

| $S_5$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{10}{[(12)]}$ | $\overset{20}{[(123)]}$ | $\overset{30}{[(1234)]}$ | $\overset{24}{[(12345)]}$ | $\overset{15}{[(12)(34)]}$ | $\overset{20}{[(12)(345)]}$ |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 4 | 2 | 1 | 0 | $-1$ | 0 | $-1$ |
| $\chi_4$ | 4 | $-2$ | 1 | 0 | $-1$ | 0 | 1 |
| $\chi_5$ | 5 | | | | | | |
| $\chi_6$ | 5 | | | | | | |
| $\chi_7$ | 6 | 0 | | 0 | | | 0 |
| $\chi_P$ | 5 | 3 | 2 | 1 | 0 | 1 | 0 |

Observe that $S_5$ acts on the subsets of size 2; namely $\{\{i, j\} : i, j \in \{1, 2, 3, 4, 5\}\}$. There are $\binom{5}{2} = 10$ such subsets. Instead of considering the permutation representation $P : S_5 \to \mathrm{GL}_5(\mathbb{C})$, we have another representation $Q : S_5 \to \mathrm{GL}_{10}(\mathbb{C})$ where from the basis $\{e_{\{i,j\}} : i, j \in \{1, 2, 3, 4, 5\}\}$, we define

$$\sigma \cdot e_{\{i,j\}} = e_{\sigma(i)\sigma(j)}.$$

Let's now determine $\chi_Q$. This time, $\chi_Q(\sigma)$ is the number of sets of size two that are fixed by $\sigma$.

| $S_5$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{10}{[(12)]}$ | $\overset{20}{[(123)]}$ | $\overset{30}{[(1234)]}$ | $\overset{24}{[(12345)]}$ | $\overset{15}{[(12)(34)]}$ | $\overset{20}{[(12)(345)]}$ |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 4 | 2 | 1 | 0 | $-1$ | 0 | $-1$ |
| $\chi_4$ | 4 | $-2$ | 1 | 0 | $-1$ | 0 | 1 |
| $\chi_5$ | 5 | | | | | | |
| $\chi_6$ | 5 | | | | | | |
| $\chi_7$ | 6 | 0 | | 0 | | | 0 |
| $\chi_Q$ | 10 | 4 | 1 | 0 | 0 | 2 | 1 |

For example, note that $(12) \cdot e_{\{1,2\}} = e_{\{1,2\}}$, because the set $\{2,1\}$ is the same as the set $\{1,2\}$. Then, we see that the basis elements fixed by $(12)$ are $e_{\{1,2\}}$, $e_{\{3,4\}}$, $e_{\{3,5\}}$, and $e_{\{4,5\}}$, so $\chi_Q((12)) = 4$. The other values of $\chi_Q$ can be found similarly. We now compute that

$$\langle \chi_Q, \chi_Q \rangle = \frac{1}{5!}(1 \cdot 10^2 + 10 \cdot 4^2 + 20 \cdot 1^2 + 15 \cdot 2^2 + 20 \cdot 1^2) = 3.$$

Therefore, $\chi_Q$ is the sum of 3 distinct irreducible characters. We find that

$$\langle \chi_Q, \chi_1 \rangle = \frac{1}{5!}(10 \cdot 1 \cdot 1 + 4 \cdot 1 \cdot 10 + 1 \cdot 1 \cdot 20 + 2 \cdot 1 \cdot 15 + 1 \cdot 1 \cdot 20) = 1,$$
$$\langle \chi_Q, \chi_3 \rangle = \frac{1}{5!}(10 \cdot 4 \cdot 1 + 4 \cdot 2 \cdot 10 + 1 \cdot 1 \cdot 20 + 1 \cdot (-1) \cdot 20) = 1.$$

Hence, $\chi_Q - \chi_1 - \chi_3$ is an irreducible character. Note that $\chi_Q(\mathrm{id}) - \chi_1(\mathrm{id}) - \chi_3(\mathrm{id}) = 10 - 1 - 4 = 5$, and since $\chi_5(\mathrm{id}) = 5$, we can set $\chi_5 = \chi_Q - \chi_1 - \chi_3$. Then, $X_5 = \{\chi_5, \chi_6\}$, and since $\chi_2$ is a degree 1 character, it must permute $X_5$, so we can set $\chi_6 = \chi_5 \cdot \chi_2$. This completes two more rows of the character table.

| $S_5$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{10}{[(12)]}$ | $\overset{20}{[(123)]}$ | $\overset{30}{[(1234)]}$ | $\overset{24}{[(12345)]}$ | $\overset{15}{[(12)(34)]}$ | $\overset{20}{[(12)(345)]}$ |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 4 | 2 | 1 | 0 | $-1$ | 0 | $-1$ |
| $\chi_4$ | 4 | $-2$ | 1 | 0 | $-1$ | 0 | 1 |
| $\chi_5$ | 5 | 1 | $-1$ | $-1$ | 0 | 1 | 1 |
| $\chi_6$ | 5 | $-1$ | $-1$ | 1 | 0 | 1 | $-1$ |
| $\chi_7$ | 6 | 0 | $d$ | 0 | $e$ | $f$ | 0 |
| $\chi_Q$ | 10 | 4 | 1 | 0 | 0 | 2 | 1 |

Finally, let's compute $\chi_7$ by determining $d = \chi_7((123))$, $e = \chi_7((12345))$, and $f = \chi_7((12)(34))$. We have

$$0 = \langle \chi_7, \chi_5 \rangle = \frac{1}{5!}(30 - 20d + 15f),$$
$$0 = \langle \chi_7, \chi_3 \rangle = \frac{1}{5!}(24 + 20d - 24e),$$
$$0 = \langle \chi_7, \chi_1 \rangle = \frac{1}{5!}(6 + 20d + 24e + 15f).$$

This is a system of 3 equations and 3 unknowns; solving it yields $(d, e, f) = (0, 1, -2)$, completing the character table of $S_5$.

| $S_5$ | $\overset{1}{[\mathrm{id}]}$ | $\overset{10}{[(12)]}$ | $\overset{20}{[(123)]}$ | $\overset{30}{[(1234)]}$ | $\overset{24}{[(12345)]}$ | $\overset{15}{[(12)(34)]}$ | $\overset{20}{[(12)(345)]}$ |
|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 4 | 2 | 1 | 0 | $-1$ | 0 | $-1$ |
| $\chi_4$ | 4 | $-2$ | 1 | 0 | $-1$ | 0 | 1 |
| $\chi_5$ | 5 | 1 | $-1$ | $-1$ | 0 | 1 | 1 |
| $\chi_6$ | 5 | $-1$ | $-1$ | 1 | 0 | 1 | $-1$ |
| $\chi_7$ | 6 | 0 | 0 | 0 | 1 | $-2$ | 0 |

# 20 Algebraic numbers and algebraic integers (10/29/2021)

Write $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_s}(\mathbb{C})$, and let $\chi_1, \ldots, \chi_s$ be the irreducible characters. We have $\chi_i(1_G) = n_i$, which is the degree of $\chi_i$. Moreover, since $\langle \chi_i, \chi_j \rangle = \delta_{ij}$, we know that $\|\chi\|^2 = 1$ if and only if $\chi$ is irreducible. In particular, if the character $\chi = a_1\chi_1 + \cdots + a_s\chi_s$ is irreducible, then

$$\|\chi\|^2 = a_1^2 + \cdots + a_s^2 = 1$$

implies that there is a unique $1 \leq j \leq s$ such that $a_j = 1$ and $a_i = 0$ for all $i \neq j$. Hence, $\|\chi\|^2 = 1$ if and only if $\chi = \chi_j$ for some $1 \leq j \leq s$. Today, we'll introduce the algebraic integers, which will help us to prove the last part of the big theorem, which states that $n_i \mid |G|$ for all $1 \leq i \leq s$.

**Definition 20.1**

We define the **algebraic numbers** $\mathbb{A} \subseteq \mathbb{C}$ to be the set

$$\mathbb{A} = \{\alpha \in \mathbb{C} : P(\alpha) = 0 \text{ for some monic polynomial } P(x) \in \mathbb{Z}[x]\}.$$

**Example 20.2**

(1) Observe that $\mathbb{Z} \subseteq \mathbb{A}$, since for any $n \in \mathbb{Z}$, the polynomial $P(x) = x - n$ has $n$ as a root.

(2) If $\alpha \in \mathbb{Q}$, then $\beta = e^{\pi i \alpha} \in \mathbb{A}$. Indeed, write $\alpha = a/b$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Taking the polynomial $P(x) = x^{2b-1}$, we have $P(\beta) = (e^{\pi i a/b})^{2b} - 1 = e^{2\pi i a} - 1 = 0$.

(3) Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. Then $\alpha = \sqrt[b]{a} \in \mathbb{A}$ by taking $P(x) = x^b - a \in \mathbb{Z}[x]$.

**Lemma 20.3**

We have $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Exercise 1 of Homework 4 shows that $\mathbb{Z} \subseteq \mathbb{A} \cap \mathbb{Q}$. Next, we clearly have $\alpha = 0 \in \mathbb{Z}$. Suppose that we have a nonzero $\alpha = a/b$ with $\gcd(a, b) = 1$ and $b > 0$ which is a root of the monic polynomial

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x].$$

Moreover, we can assume that $c_0 \neq 0$, for otherwise we could just reduce the degree of the polynomial. Then by the rational roots theorem, we obtain $b \mid 1$ and $a \mid c_0$, which implies that $\alpha = a/b \in \mathbb{Z}$. Therefore, we conclude that $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. □

This statement is very simple, but it has some very powerful consequences. Recall that a finitely generated $\mathbb{Z}$-submodule of $(\mathbb{C}, +)$ is given by all elements of the form

$$\{n_1\lambda_1 + \cdots + n_p\lambda_p : n_1, \ldots, n_p \in \mathbb{Z}\}$$

for some fixed $\lambda_1, \ldots, \lambda_p \in \mathbb{C}$. For example, we have $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ by choosing $\lambda_1 = 1$ and $\lambda_2 = i$. We'll now prove some characterizations of algebraic numbers.

**Theorem 20.4**

Let $\alpha \in \mathbb{C}$. The following are equivalent:

(1) $\alpha \in \mathbb{A}$.

(2) There exists a nonzero finitely generated $\mathbb{Z}$-submodule $M$ of $\mathbb{C}$ such that $\alpha M \subseteq M$.

(3) There exists $p \geq 1$ and $\lambda_1, \ldots, \lambda_p \in \mathbb{C} \setminus \{0\}$ such that $\alpha\lambda_i \in \mathbb{Z}\lambda_1 + \cdots + \mathbb{Z}\lambda_p$ for all $i = 1, \ldots, p$.

Proof. (1) $\Rightarrow$ (2). If $\alpha \in \mathbb{A}$, then there exists $n \geq 1$ and $c_0, \ldots, c_{n-1} \in \mathbb{Z}$ such that

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0. \tag{20.1}$$

Let $M = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \cdots + \mathbb{Z}\alpha^{n-1}$. This is a finitely generated $\mathbb{Z}$-submodule, and $M \neq (0)$ since $1 \in M$. Now, we claim that $\alpha M \subseteq M$. To this end, suppose that $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in M$. Then we have

$$\begin{aligned}\alpha(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) &= a_0\alpha + a_1\alpha^2 + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1}\alpha^n \\ &= a_0\alpha + a_1\alpha^2 + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1}(-c_{n-1}\alpha^{n-1} - \cdots - c_1\alpha - c_0) \\ &= -a_{n-1}c_0 + (a_0 - a_{n-1}c_1)\alpha + \cdots + (a_{n-2} - a_{n-1}c_{n-1})\alpha^{n-1},\end{aligned}$$

where the second last equality follows from (20.1). We see that $\alpha(a_0 + a_1\alpha + \cdots + a_{n-1}) \in M$, so $\alpha M \subseteq M$.

(2) $\Rightarrow$ (3). Suppose there exists a nonzero finitely generated $\mathbb{Z}$-submodule $M$ of $\mathbb{C}$ such that $\alpha M \subseteq M$. Then we can pick $\lambda_1, \ldots, \lambda_p \in \mathbb{C} \setminus \{0\}$ such that $M = \mathbb{Z}\lambda_1 + \cdots + \mathbb{Z}\lambda_p$. Since $\alpha M \subseteq M$, this implies that $\alpha\lambda_i \in M$ for each $i = 1, \ldots, p$.

(3) $\Rightarrow$ (1). Suppose there exists $p \geq 1$ and $\lambda_1, \ldots, \lambda_p \in \mathbb{C} \setminus \{0\}$ such that $\alpha\lambda_i \in \mathbb{Z}\lambda_i + \cdots + \mathbb{Z}\lambda_p$ for all $i = 1, \ldots, p$. Then for $j = 1, \ldots, p$, we can pick $a_{j1}, \ldots, a_{jp} \in \mathbb{Z}$ such that

$$\alpha\lambda_i = a_{j1}\lambda_1 + \cdots + a_{jp}\lambda_p.$$

We can write this as a matrix equation to get

$$\alpha \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_p \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \cdots & a_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1} & a_{p2} & \cdots & a_{pp} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_p \end{pmatrix}.$$

Set $v = (\lambda_1, \ldots, \lambda_p)^T$, and notice that $v \neq 0$ since $\lambda_1, \ldots, \lambda_p \in \mathbb{C} \setminus \{0\}$. Moreover, set $A$ to be the matrix above, and observe that $A \in M_p(\mathbb{Z})$. Now, we have $\alpha v = Av$, so $\alpha$ is an eigenvalue of $A$. Hence, $\alpha$ is a root of the characteristic polynomial of $A$. That is, for

$$P_A(x) = \det(xI - A) = \det \begin{pmatrix} x - a_{11} & \cdots & -a_{1p} \\ \vdots & \ddots & \vdots \\ -a_{p1} & \cdots & x - a_{pp} \end{pmatrix},$$

we have $P_A(\alpha) = 0$. Note that $A \in M_p(\mathbb{Z})$, so $P_A(x)$ is a monic polynomial in $\mathbb{Z}[x]$. It follows that $\alpha \in \mathbb{A}$. $\square$

**Theorem 20.5**

The algebraic numbers $\mathbb{A}$ form a subring of $\mathbb{C}$.

PROOF. It suffices to show that $\mathbb{A}$ is closed under addition and multiplication, and that $-1 \in \mathbb{A}$; this last condition assures that we have additive inverses.

We have already seen that $\mathbb{Z} \subseteq \mathbb{A}$, so $-1 \in \mathbb{A}$. Let $\alpha, \beta \in \mathbb{A}$. We assume that $\alpha$ and $\beta$ are both nonzero, as the result is trivial otherwise. We want to show that $\alpha + \beta$ and $\alpha\beta$ are in $\mathbb{A}$. By definition, we have

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0,$$
$$\beta^m + d_{m-1}\beta^{m-1} + \cdots + d_1\beta + d_0 = 0,$$

for some $c_0, \ldots, c_{n-1}, d_0, \ldots, d_{n-1} \in \mathbb{Z}$. Let

$$M = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \mathbb{Z}\alpha^i\beta^j,$$

which is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$, and $M \neq (0)$ since $1 \in M$. Now, we claim that $\alpha M \subseteq M$ and $\beta M \subseteq M$. It suffices to show that $\beta(\alpha^i\beta^j)$ and $\alpha(\alpha^i\beta^j)$ are in $M$ for all $0 \leq i \leq n-1$ and $0 \leq j \leq m-1$.

We will consider $\alpha(\alpha^i\beta^j)$. When $0 \leq i \leq n-2$, we have $\alpha(\alpha^i\beta^j) = \alpha^{i+1}\beta^j \in M$, since $0 \leq i+1 \leq n-1$. Otherwise, we have $i = n-1$, in which case

$$\alpha(\alpha^{n-1}\beta^j) = \alpha^n\beta^j = (-c_{n-1}\alpha^{n-1} - \cdots - c_1\alpha - c_0)\beta^j \in M.$$

This implies that $\alpha M \subseteq M$, and a similar argument shows that $\beta M \subseteq M$. Now, observe that

$$(\alpha + \beta)M \subseteq \alpha M + \beta M \subseteq M + M = M,$$

and similarly, we know from our work above that

$$(\alpha\beta)M = \alpha(\beta M) \subseteq \alpha M \subseteq M.$$

It follows from Theorem 20.4 that $\alpha + \beta$ and $\alpha\beta$ are in $\mathbb{A}$. □

REMARK 20.6

Note that $\mathbb{A}$ is not a field, since $2 \in \mathbb{A}$ but $1/2 \notin \mathbb{A}$.

Now, we'll prove an interesting corollary of the fact that $\mathbb{A}$ is a subring of $\mathbb{C}$.

COROLLARY 20.7

If $\alpha \in \mathbb{Q}$ and $\tan(\pi\alpha) \in \mathbb{Q}$, then $\tan(\pi\alpha) \in \{0, 1, -1\}$.

PROOF. Recall that $\tan^2(x) + 1 = 1/\cos^2(x)$. Therefore, if $\tan(\pi\alpha) \in \mathbb{Q}$, then we have $\tan^2(\pi\alpha) + 1 = 1/\cos^2(\pi\alpha) \in \mathbb{Q}$ as well. This implies that $4\cos^2(\pi\alpha) \in \mathbb{Q}$. Now, notice that

$$4\cos^2(\pi\alpha) = (2\cos(\pi\alpha))^2 = (e^{i\pi\alpha} + e^{-i\pi\alpha})^2.$$

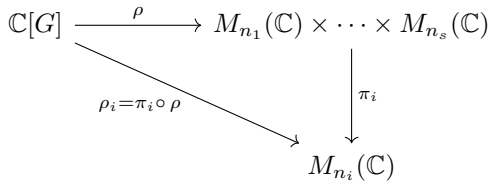
In particular, since $e^{i\pi\alpha}$ and $e^{-i\pi\alpha}$ are both algebraic numbers (as we saw in Example 20.2), this shows that $4\cos^2(\pi\alpha) \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$. Now, we know that $4\cos^2(\pi\alpha) \in \{0, 1, 2, 3, 4\}$. Taking the inverses and multiplying by 4, we find that $1/\cos^2(\pi\alpha) \in \{4, 2, 4/3, 1\}$. Finally, we have

$$\tan^2(\pi\alpha) = \frac{1}{\cos^2(\pi\alpha)} - 1 \in \left\{3, 1, \frac{1}{3}, 0\right\}.$$

But we assumed that $\tan(\pi\alpha) \in \mathbb{Q}$, so the only possibilities are $\tan(\pi\alpha) \in \{0, 1, -1\}$, as desired. □

# 21 Degree of irreps divide order of the group (11/01/2021)

Let $G$ be a finite group. Let $\rho : \mathbb{C}[G] \to M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_s}(\mathbb{C})$ be a $\mathbb{C}$-algebra isomorphism. Then, we have the following commutative diagram.




Then, we obtain characters $\chi_i(g) = \mathrm{Tr}(\rho_i(g))$. We also have $\mathbb{C}[G]$-modules $V_i = \mathbb{C}^{n_i \times 1}$ with the action $g \cdot v = \rho_i(g) \cdot v$. Our goal in this lecture is to prove that $n_i \mid |G|$ for each $i = 1, \ldots, s$, where $\chi_i(1_G) = n_i$ is the degree of the character. Note that $\rho_i(1_G) = I_{n_i}$.

**Lemma 21.1**

Let $\mathcal{C}$ be a conjugacy class of $G$, and let $g \in \mathcal{C}$. Then for all $i = 1, \ldots, s$, we have

$$\frac{|\mathcal{C}|\chi_i(g)}{n_i} \in \mathbb{A}.$$

Proof. Let $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the conjugacy classes of $G$. Recall from Proposition 10.7 that a basis for $Z(\mathbb{C}[G])$ is given by $z_1, \ldots, z_s$, where

$$z_p = \sum_{h \in \mathcal{C}_p} h.$$

Let $M = \mathbb{Z}z_1 + \cdots + \mathbb{Z}z_s \subseteq Z(\mathbb{C}[G])$. We claim that $z_p M \subseteq M$ for all $p = 1, \ldots, s$.

It suffices to show that $z_p z_j \in M$ for all $p = 1, \ldots, s$ and $j = 1, \ldots, s$, as every element in $M$ can be written as a linear combination of $z_1, \ldots, z_s$. In particular, notice that

$$z_p(c_1 z_1 + \cdots + c_s z_s) = c_1 z_p z_1 + \cdots + c_s z_p z_s \in M.$$

Notice that $z_p z_j \in Z(\mathbb{C}[G])$, so we have

$$z_p z_j = \sum_{k=1}^{s} \lambda_{p,j,k} z_k \tag{21.1}$$

for some $\lambda_{p,j,k} \in \mathbb{C}$. In order to show that $z_p z_j \in M$, we require that $\lambda_{p,j,k} \in \mathbb{Z}$ for all $k = 1, \ldots, s$. Pick $h \in \mathcal{C}_k$ and consider the coefficient of $h$ in (21.1). On the right hand side, it is simply $\lambda_{p,j,k}$. On the left hand side, note that

$$z_p z_j = \left( \sum_{h' \in \mathcal{C}_p} h' \right) \left( \sum_{h'' \in \mathcal{C}_j} h'' \right),$$

so the coefficient of $h$ is $\#\{(h', h'') \in \mathcal{C}_p \times \mathcal{C}_j : h' \cdot h'' = h\} \in \mathbb{Z}_{\geq 0}$. This proves the claim.

Now, consider the diagram above, and note that $\rho_i$ is surjective. Since $z_j$ is central in $\mathbb{C}[G]$, we see that $\rho_i(z_j) \in Z(M_{n_i}(\mathbb{C}))$. By surjectivity of $\rho_i$, it follows that $\rho_i(z_j) = \gamma_{i,j} I_{n_i}$ with $\gamma_{i,j} \in \mathbb{C}$; that is, $\rho_i(z_j)$ is a scalar matrix. Next, define

$$M_i = \mathbb{Z}\gamma_{i,1} + \cdots \mathbb{Z}\gamma_{i,s} \subseteq \mathbb{C},$$

which is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$ with $M_i \neq (0)$. Notice that $M_i = \rho_i(M)$ by construction after identifying the scalar matrices $\mathbb{C} \cdot I_{n_i}$ with $\mathbb{C}$. Now, since $z_j M \subseteq M$ by our claim, we obtain $\rho_i(z_j)\rho_i(M) \subseteq \rho_i(M)$, so

$$\gamma_{i,j} M_i \subseteq M_i$$

after identification. Hence, for all $1 \leq i, j \leq s$, we get $\gamma_{i,j} \in \mathbb{A}$. Next, let $\mathcal{C} = \mathcal{C}_j$ be a conjugacy class and $g \in \mathcal{C}$. Note that

$$\gamma_{i,j} I_{n_i} = \rho_i(z_j) = \rho_i \left( \sum_{h \in \mathcal{C}_j} h \right) = \sum_{h \in \mathcal{C}_j} \rho_i(h).$$

Taking the trace of both sides yields

$$\gamma_{i,j} \cdot n_i = \operatorname{Tr}(\gamma_{i,j} I_{n_i}) = \operatorname{Tr} \left( \sum_{h \in \mathcal{C}_j} \rho_i(h) \right) = \sum_{h \in \mathcal{C}_j} \chi_i(h) = |\mathcal{C}| \chi_i(g),$$

where the last equality is because $\chi_i$ is a class function. It follows that

$$\frac{|\mathcal{C}| \chi_i(g)}{n_i} = \gamma_{i,j} \in \mathbb{A}. \qquad \square$$

**Theorem 21.2**

Let $G$ be a finite group. If $\chi_i$ is an irreducible character with degree $n_i$, then $n_i \mid |G|$.

Proof. We always have a trivial irreducible character with $\chi(h) = 1$ for all $h \in G$. Without loss of generality, suppose that $\chi_1$ is the trivial representation, which has degree $n_1 = 1$, in which case the result clearly holds.

It suffices to consider the case where $i > 1$. Let $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the conjugacy classes of $G$. For each $j = 1, \ldots, s$, pick a representative $g_j \in \mathcal{C}_j$. Then we have

$$1 = \langle \chi_i, \chi_i \rangle = \frac{1}{|G|} \sum_{j=1}^{s} |\mathcal{C}_j| \chi_i(g_j) \overline{\chi_i(g_j)} = \frac{n_i}{|G|} \sum_{j=1}^{s} \frac{|\mathcal{C}_j| \chi_i(g_j)}{n_i} \cdot \overline{\chi_i(g_j)}.$$

By Lemma 21.1, each $|\mathcal{C}_j| \chi_i(g_j)/n_i$ is in $\mathbb{A}$. Moreover, we have shown that $\rho_i(g)$ is triangularizable with roots of unity $\omega_1, \ldots, \omega_{n_i}$ along the diagonal, so

$$\overline{\chi_i(g_j)} = \overline{\omega_1} + \cdots + \overline{\omega_{n_i}} \in \mathbb{A}.$$

In particular, we see that

$$1 = \frac{n_i}{|G|} \cdot \alpha$$

where $\alpha \in \mathbb{A}$. Rearranging gives $|G|/n_i = \alpha$. Observe that $|G|/n_i \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$, so $n_i \mid |G|$. $\square$

# 22 Burnside's theorem (11/03/2021)

The fact that the degrees of the irreducible characters divide the order of the group has some very powerful consequences. The Feit-Thompson theorem states that every group of odd order is solvable. We'll focus on Burnside's theorem, which gives the weaker statement that every group of order $p^a q^b$ is solvable, where $p$ and $q$ are distinct primes and $a, b \in \mathbb{Z}^+$. The proofs of these theorems are very difficult (if not impossible) without using character theory, and we'll use it to make our lives easier. First, let's recall what it means for a group to be solvable.

**Definition 22.1**

A group $G$ is **solvable** if there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{1\}$$

such that $G_{i+1} \trianglelefteq G_i$ and $G_i/G_{i+1}$ is abelian for all $0 \leq i \leq m-1$.

Towards the proof of Burnside's theorem, we'll first prove some intermediate results.

**Lemma 22.2**

Let $\chi$ be an irreducible character of degree $n \geq 2$. If $\chi(g)/n \in \mathbb{A}$ for some $g \in G$, then $\chi(g) = 0$.

We leave the proof of this lemma for the next lecture. For the moment, we will use this lemma to prove the following theorem.

**Theorem 22.3**

Let $G$ be a non-abelian finite group. Suppose that $G$ has a conjugacy class of size $p^a$ where $p$ is a prime and $a \in \mathbb{Z}^+$. Then $G$ is not simple.

Proof. Suppose by way of contradiction that there exists a non-abelian finite simple group $G$ with an element $g \in G$ such that the conjugacy class $\mathcal{C} = \mathcal{C}(g)$ containing $g$ has size $p^a$, where $p$ is prime and $a \in \mathbb{Z}^+$. Since $G$ is non-abelian and simple, we have $G' = G$. Indeed, note that $G' \trianglelefteq G$. By simplicity, we either have $G' = G$ or $G' = \{1\}$. But $G$ is non-abelian, so we must be in the first case. This means that $G$ has one inequivalent irreducible representation of degree 1 since $|G/G'| = |G/G| = 1$. The only irreducible character of degree 1 is the trivial character $\chi$ with $\chi(h) = 1$ for all $h \in G$.

Let $\chi_1, \ldots, \chi_s$ be the irreducible characters of $G$. Without loss of generality, we may assume that $\chi_1$ is the trivial character. Notice that if $n_1, \ldots, n_s$ are the degrees of $\chi_1, \ldots, \chi_s$ respectively, then $n_1 = 1$ and $n_i > 1$ for $i = 2, \ldots, s$. Recall that we have $g \in G$ such that $|\mathcal{C}| = |\mathcal{C}(g)| = p^a$, where $p$ is prime and $a \in \mathbb{Z}^+$. This implies that $g \neq 1$, for otherwise its conjugacy class would have size 1. Now, if $L$ is the left regular representation of $G$, then $\chi_L(g) = 0$. This implies that

$$0 = \chi_L(g) = \sum_{i=1}^{s} n_i \chi_i(g) = \chi_1(g) + \sum_{\substack{i \geq 2 \\ p \mid n_i}} n_i \chi_i(g) + \sum_{\substack{i \geq 2 \\ p \nmid n_i}} n_i \chi_i(g).$$

Claim. For $i \geq 2$, if $p \nmid n_i$, then $\chi_i(g) = 0$.

Proof of Claim. We know that $\chi_i(g) \in \mathbb{A}$. We have also showed in Lemma 21.1 that

$$\frac{p^a \chi_i(g)}{n_i} = \frac{|\mathcal{C}(g)| \chi_i(g)}{n_i} \in \mathbb{A}.$$

Since $p \nmid n_i$, we have $\gcd(p^a, n_i) = 1$. Therefore, there exist $c, d \in \mathbb{Z}$ such that $cp^a + dn_i = 1$. We find that

$$\frac{\chi_i(g)}{n_i} = \frac{cp^a + dn_i}{n_i} \chi_i(g) = \frac{cp^a \chi_i(g)}{n_i} + d\chi_i(g) \in \mathbb{A}.$$

By Lemma 22.2, we obtain $\chi_i(g) = 0$. ∎

Now, writing $n_i = pn_i'$ for each $i \geq 2$ with $p \mid n_i$, we have

$$0 = \chi_1(g) + \sum_{\substack{i \geq 2 \\ p \mid n_i}} n_i \chi_i(g) + \sum_{\substack{i \geq 2 \\ p \nmid n_i}} n_i \chi_i(g) = \chi_1(g) + p \sum_{\substack{i \geq 2 \\ p \mid n_i}} n_i' \chi_i(g).$$

Let $\alpha$ denote the sum in the above equation, and note that $\alpha \in \mathbb{A}$. Then $1 + p\alpha = 0$, which implies that $\alpha = -1/p$. But this is a contradiction since $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$, but $-1/p \notin \mathbb{Z}$. □

We can now prove Burnside's theorem. First, we'll recall some facts from group theory.

(1) Let $N \trianglelefteq G$. Then $G$ is solvable if and only if $N$ and $G/N$ are both solvable.

(2) Let $G$ be a group of order $q^b c$ where $q$ is prime, $b \in \mathbb{Z}^+$, and $q \nmid c$. Then by the first Sylow theorem, $G$ has a subgroup $Q$ of order $q^b$.

(3) If $G$ is a group of order $q^b$ where $q$ is prime and $b \in \mathbb{Z}^+$, then $G$ has a non-trivial center by the class equation.

(4) If $g \in G$ and $\mathcal{C}(g)$ is the conjugacy class of $g$, then $|\mathcal{C}(g)| = |G|/|C(g)|$, where $C(g) = \{h \in G : hg = gh\}$ is the centralizer of $g$.

**Theorem 22.4: Burnside's theorem**

Let $G$ be a group of order $p^a q^b$ where $p$ and $q$ are distinct primes and $a, b \in \mathbb{Z}^+$. Then $G$ is solvable.

Proof. Suppose the result is not true. Let $G$ be a minimal counterexample; that is, $G$ is a group of order $p^a q^b$ where $p$ and $q$ are distinct primes and $a, b \in \mathbb{Z}^+$, and $G$ has minimal size with respect to this property.

Claim. $G$ is a non-abelian simple group.

Proof of Claim. Note that $G$ is non-abelian since if $G$ were abelian, then it would be solvable. Assume that $G$ is not simple. Then there exists a non-trivial proper normal subgroup $N$ of $G$. Then $G/N$ and $N$ are both smaller than $G$ and their sizes divide $p^a q^b$. By minimality, $N$ and $G/N$ are solvable, so $G$ is also solvable by (1), a contradiction. ■

Pick a subgroup $Q \leq G$ with $|Q| = q^b$, which exists by (2). Moreover, we can choose $z \neq 1$ such that $z \in Z(Q)$, which exists since $Q$ has non-trivial center by (3). Then $Q \subseteq C(z) \subseteq G$, so $|C(z)| = p^c q^b$ where $c \in \{0, \ldots, a\}$. By (4), it follows that

$$|\mathcal{C}(z)| = \frac{|G|}{|C(z)|} = \frac{p^a q^b}{p^c q^b} = p^{a-c}.$$

If $c < a$, then $G$ is not simple by Theorem 22.3 since $G$ is non-abelian and $|\mathcal{C}(z)|$ is a conjugacy class with size which is a prime power, contradicting our claim. So $c = a$, which gives $|\mathcal{C}(z)| = 1$. But this means that $C(z) = G$. Moreover, $z$ is central, which gives $\{1\} \neq Z(G) \trianglelefteq G$. Since $G$ is simple, we must have $Z(G) = G$. This would mean that $G$ is abelian, once again contradicting our claim. Therefore, no counterexample exists, so the result holds. □

# 23 Galois theory (11/05/2021)

Let $F$ be a field of characteristic 0, and let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ be a monic polynomial with roots $\alpha_1, \ldots, \alpha_n \in \overline{F}$. Let $K = \{p(\alpha_1, \ldots, \alpha_n) : p(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]\}$. Notice that $K$ is a subring of $\overline{F}$, because we may consider the surjective $F$-algebra homomorphism

$$\begin{aligned} \varphi : F[x_1, \ldots, x_n] &\mapsto \overline{F}, \\ p(x_1, \ldots, x_n) &\mapsto p(\alpha_1, \ldots, \alpha_n), \end{aligned}$$

whose image is $K$ by definition. Note that $\dim_F K < \infty$ since $K$ is spanned by $S = \{\alpha_1^{i_1} \cdots \alpha_n^{i_n} : 0 \leq i_1, \ldots, i_n \leq n\}$. To see this, let $V$ be the $F$-vector subspace of $K$ spanned by $S$. If $V \subsetneq K$, then there exists a polynomial $p(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ such that $p(\alpha_1, \ldots, \alpha_n) \notin V$. Pick such a $p$ of smallest degree lexicographically; that is, $x_1^{i_1} \cdots x_n^{i_n} <_{\text{lex}} x_1^{j_1} \cdots x_n^{j_n}$ if for some $1 \leq m \leq n$, we have $i_k = j_k$ for all $0 \leq k < m$, and $i_m < j_m$. Note that this is a total ordering.

We claim that all monomials of $p$ have degree less than $n$. Suppose we had some $x_1^{i_1} \cdots x_s^{i_s} \cdots x_n^{i_n}$ with $i_s \geq n$. Recall that $\alpha_s$ is a root of $p$, so we have

$$\alpha_s^n + a_{n-1}\alpha_s^{n-1} + \cdots + a_1\alpha_s + a_0 = 0.$$

Rearranging the above equation and multiplying by $\alpha_s^{i_n - n}$ gives

$$\alpha_s^{i_n} = -a_{n-1}\alpha_s^{i_n - 1} - \cdots - a_0\alpha_s^{i_n - n}.$$

From this, it follows that

$$\alpha_1^{i_1} \cdots \alpha_s^{i_s} \cdots \alpha_n^{i_n} = -a_{n-1}\alpha_1^{i_1} \cdots \alpha_s^{i_n - 1} \cdots \alpha_n^{i_n} - \cdots - a_0\alpha_1^{i_1} \cdots \alpha_s^{i_n - n} \cdots \alpha_n^{i_n}.$$

We can repeat this with all other monomials to reach a contradiction.

Note that $K$ is a field. Indeed, we have $K \subseteq \overline{F}$, so $K$ is an integral domain. Moreover, we showed that $\dim_F K < \infty$. Therefore, if $a \in K \setminus \{0\}$, then the map $L_a : K \to K$ given by $L_a(x) = ax$ is $K$-linear and onto. Since $L_a$ is onto, there exists $b \in K$ such that $L_a(b) = 1$, so $ab = ba = 1$. We call $K$ the splitting field of $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - \alpha_1) \cdots (x - \alpha_n)$. By construction, it is the smallest field extension of $F$ containing all the roots of $p(x) \in F[x]$.

Recall that the Galois group $\text{Gal}(K/F)$ is the set of all $F$-algebra automorphisms $\sigma : K \to K$ with $\sigma|_F = \text{id}_F$ together with the operation of composition.

**Remark 23.1**

$\text{Gal}(K/F)$ embeds into $S_n$. To see why, if $\sigma \in \text{Gal}(K/F)$, then $\sigma$ is uniquely determined by the values $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. Now, we see that $\sigma$ permutes $\alpha_1, \ldots, \alpha_n$ because if $p(\alpha) = 0$ for some $\alpha \in K$, then

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Since $\sigma$ is $F$-linear, we obtain

$$\begin{aligned} p(\sigma(\alpha)) &= \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\ &= \sigma(0) = 0. \end{aligned}$$

Now, let $G = \text{Gal}(K/F)$. The fundamental theorem of Galois theory tells us that if we are given a subgroup $\{\text{id}\} \subseteq H \subseteq G$, then $K^H = \{a \in K : \tau(a) = a \text{ for all } \tau \in H\}$ forms a field, and the converse is also true. Moreover, we have $H_1 \subseteq H_2$ if and only if $K^{H_1} \supseteq K^{H_2}$; that is, this correspondence is inclusion-reversing. In particular, notice that $K^G = \{a \in K : \sigma(a) = a \text{ for all } \sigma \in \text{Gal}(K/F)\} = F$.

**Theorem 23.2**

Consider the polynomial

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - \alpha_1) \cdots (x - \alpha_n) \in \mathbb{Z}[x].$$

If $|\alpha_i| \leq 1$ for all $i = 1, \ldots, n$, then each $\alpha_i$ is either 0 or a root of unity.

PROOF. First, note that $\alpha_1, \ldots, \alpha_n \in \mathbb{A}$. Let $K$ be the splitting field of $p(x) \in F[x]$, and let $G = \mathrm{Gal}(K/\mathbb{Q})$. For $j \in \mathbb{Z}^+$, define the polynomial

$$p_j(x) = (x - \alpha_1^j) \cdots (x - \alpha_n^j).$$

Note that $p_j(x) \in \mathbb{Q}[x]$. Indeed, if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then by $K$-linearity, we obtain

$$\sigma(p_j(x)) = \sigma((x - \alpha_1^j) \cdots (x - \alpha_n^j)) = (x - \sigma(\alpha_1^j)) \cdots (x - \sigma(\alpha_n^j)) = p_j(x).$$

This holds for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. The coefficients of $p_j(x)$ are all in $K^G = \mathbb{Q}$ (where this equality holds by the fundamental theorem of Galois theory). It follows that $p_j(x) \in \mathbb{Z}[x]$ since $\alpha_1, \ldots, \alpha_n \in \mathbb{A}$, and so the coefficients are in $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Now, write

$$p_j(x) = x^n + a_{n-1,j} x^{n-1} + \cdots + a_{1,j} x + a_{0,j} \in \mathbb{Z}[x].$$

We claim that $|a_{n,j}| \leq \binom{n}{k}$. Indeed, by expanding out our original definition of $p_j(x)$, we have

$$p_j(x) = x^n - (\alpha_1^j + \cdots + \alpha_n^j) x^{n-1} + \cdots + (-1)^k \left( \sum_{1 \leq i_1 < \cdots < i_k \leq n} \alpha_{i_1}^j \cdots \alpha_{i_k}^j \right) x^{n-k} + \cdots .$$

Then we have

$$a_{n-k,j} = (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} \alpha_{i_1}^j \cdots \alpha_{i_k}^j,$$

and since $|\alpha_i| \leq 1$ for all $i = 1, \ldots, n$, it follows that $|a_{n-k,j}| \leq \binom{n}{k}$. □