Notes on Noncommutative Algebra

BY WHZECOMJM

Bar-Ilan University
July 5, 2015
Update: July 26, 2020

Abstract

This note is distributed to participants of the course on noncommutative algebra in July, 2015 given by Prof. Uzi Vishne at Bar-Ilan. The note is based on the lecture notes of the course and the book: *Graduate algebra: Noncommutative view* by Louis Rowen.

Table of contents

1 Basic concepts of rings

Whereas much of commutative theory stems from the polynomial algebra $F[x_1, \ldots, x_n]$ over a field F, the matrix algebra $M_n(F)$ is arguably the most important example of a noncommutative algebra, since the tools of matrix theory are available, including the trace, determinant, transpose, and so forth. Much of representation theory involves comparing a given algebraic structure to a such a matrix algebra, via suitable homomorphisms. In particular, any f.d. algebra can be embedded into a matrix algebra via the **regular representation**.

In commutative algebra, we encountered the ring $M_n(R)$ of $n \times n$ matrices over a commutative ring R. Familiar computations from linear algebra show that $M_n(R)$ is a ring, even when R is not commutative, although we shall also see this from a structural point of view.

Recall that by ideal we mean two-sided ideal. As we shall see, **the ideals of $\boldsymbol{R}$ and $\boldsymbol{M_n(R)}$ are in 1:1 correspondence**. Thus, when D is a division ring, the ring $M_n(D)$ has no proper nonzero ideals, and also is both left and right Artinian and Noetherian. A main theorem (Wedderburn-Artin-Hopkins-Levitzki) says that **any simple left Artinian ring has the form $\boldsymbol{M_n(D)}$ for a suitable division ring $\boldsymbol{D}$**. This implies that a simple ring is left Artinian if and only if it is right Artinian. Throughout this note, R-modules mean the left modules.

1.1 Simple modules

Every simple module (no submodules other than 0 and M) M is cyclic, that is it is generated by one element. But the inverse is not right, for example $4\mathbb{Z}$ is a cyclic module but not simple. An important proposition about the simple module is following:

Proposition 1.1. *An (left) R-module $M \neq 0$ is simple iff $M \cong R/L$, where L is a maximal left ideal of R. In particular, all rings have simple modules by Zorn's lemma.*

1.2 Matrix rings

Consider matrix ring $M_n(R)$, which is a free R-modules of rank n^2, with multiplication of any matrices given by usual operation. There is a ring injection $R \to M_n(R)$ via $r \mapsto \sum_{i=1}^{n} r\, e_{ii}$. Note that $M_{m,n}(R)$ doesn't have a natural ring structure for $m \neq n$, but can be viewed as a left module over $M_m(R)$ and as a right module over $M_n(R)$, via the usual matrix operations.

Definition 1.2. *A set of $n \times n$ matrix units of an arbitrary ring W is a set of elements $\{e_{ij} : 1 \leq i, j \leq n\}$ satisfying the following two basic properties:*

(MU1) $e_{ik}\, e_{lj} = \delta_{kl}\, e_{ij}$, where δ_{kl} denotes the Kronecker delta.

(MU2) $\sum_{i=1}^{n} e_{ii} = 1$.

It's easy to see that the usual units of matrix satisfy above conditions.

1.2.1 Idempotent

An idempotent of a ring R is an element e such that $e^2 = e$. The idempotents 0,1 are called the trivial idempotents of R. Idempotents e_i, $i \in I$, are called orthogonal if $e_i e_j = 0 = e_j e_i$ for all $i \neq j \in I$. We call $\{e_1, \ldots, e_n\}$ a 1-sum set of orthogonal idempotents if they are orthogonal and $\sum_{i=1}^{n} e_i = 1$. For any idempotent e, clearly $1 - e$ is an idempotent orthogonal to e, so $\{e, 1-e\}$ is a 1-sum set of orthogonal idempotents.

Proposition 1.3. *If e, f are orthogonal idempotents of the ring R, then as modules, $R(e+f) = Re \oplus Rf$. What's more, if $\{e_1,\ldots,e_n\}$ is a 1-sum set of orthogonal idempotents, then $R \cong Re_1 \oplus \cdots \oplus Re_n$.*

Proof. $Re = Re(e+f) \subset R(e+f)$, and likewise $Rf \subset R(e+f)$. Hence, $Re + Rf \subset Re(e+f)$, and the opposite direction is clear since $r(e+f) = re + rf$. Finally, we show that $Re \cap Rf = 0$: if $r_1 e = r_2 f$, then $r_1 e = r_1 e^2 = r_2 fe = 0$. By induction, we have $R = R(e_1 + \cdots + e_n) \cong Re_1 \oplus \cdots \oplus Re_n$. □

The diagonal matrix units $\{e_{11}, \ldots, e_{nn}\}$ comprise a 1-sum set of orthogonal idempotents of $M_n(R)$, so in particular

$$M_n(R) \cong \bigoplus_{i=1}^{n} M_n(R)\, e_{ii}.$$

Remark 1.4. For any ring R with an idempotent e, we define the *Peirce decomposition*

$$R = eRe \oplus eR(1-e) \oplus (1-e)Re \oplus (1-e)R(1-e)$$

as Abelian groups.

Remark 1.5. If e is an idempotent of ring W, then eWe is a ring with multiplicative unit e. R is isomorphic to the ring $e_{11} M_n(R) e_{11}$, via homomorphism $r \mapsto e_{11} r e_{11}$.

Proposition 1.6. *Suppose W is any ring having the set of matrix units $\{e_{ij}: 1 \leq i, j \leq n\}$ satisfying (MU1.) and (MU2.). Then $W \cong M_n(R)$, where $R = e_{11} W e_{11}$.*

Proof. Define $\varphi: W \to M_n(R)$ by $\varphi(w) = (r_{ij})$, where $r_{ij} = e_{1i} w e_{j1} = e_{11} e_{1i} w e_{j1} e_{11} \in R$. This is clearly a homomorphism of additive group structure, and noting that $\sum_{k=1}^{n} e_{k1} e_{1k} = 1$, we will see that i, j entry of $\varphi(ww')$ is

$$e_{1i} w w' e_{j1} = e_{1i} w \sum_{k=1}^{n} e_{k1} e_{1k} w' e_{j1} = \sum_{k=1}^{n} r_{ik} r'_{kj}.$$

Hence $\varphi(ww') = \varphi(w)\,\varphi(w')$, and φ is a homomorphism. To show that φ is onto, note that the matrix $(r_{ij}) = \varphi(\sum e_{i1} r_{ij} e_{1j})$, since $e_{1i}(e_{i1} r_{ij} e_{1j}) e_{j1} = e_{11} r_{ij} e_{11} = r_{ij}$. Finally, $w \in \ker\varphi$ iff each entry $r_{ij} = e_{1i} r_{ij} e_{j1} = 0$, implying that $e_{ii} w e_{jj} = e_{i1} e_{1i} r_{ij} e_{j1} e_{1j} = 0$, and thus

$$0 = \sum_{i,j=1}^{n} e_{ii} w e_{jj} = \sum_{i=1}^{n} e_{ii} w \sum_{j=1}^{n} e_{jj} = 1\, w\, 1 = w,$$

proving that $\ker\varphi = 0$. □

Corollary 1.7. *Suppose $W = M_n(R)$ and $\bar{W} = W/A$, where $A \lhd W$. Then $\bar{W} \cong M_n(\bar{R})$ for some ring $\bar{R}$, and the natural homomorphism $w \mapsto \bar{w}$ induces a ring surjection $R \to \bar{R}$.*

1.2.2 Lifting matrix units

A good point comes up later is whether we can reverse Coro 1.7, namely given $W/A \cong M_n(T)$, can we lift the matrix structure from T, and write W as a matrix ring?

We say a subset A of W is **nil** if every element of A is nilpotent. Let $A \subset W$ us nil, then it's easy to verify that the only idempotent $e \in A$ is 0. Moreover, $1-a$ is invertible in W for each $a \in A$. (Indeed if $a^k = 0$, then $(1-a)(1+a+a^2+\cdots+a^{k-1}) = 1-a^k = 1$.)

Proposition 1.8. *Suppose $A \subset W$ is nil. Then any set $\{f_1, \ldots, f_n\}$ of orthogonal idempotents of W/A can be lifted to a set $\{e_1, \ldots, e_n\}$ of orthogonal idempotents of W (i.e. $f_i = e_i + A$). If moreover $W/A \cong M_n(T)$, then W can be written as $M_n(R)$ for suitable ring R such that there is a surjection $R \to T$ including the given surjection $W = M_n(R) \to M_n(T)$.*

Proof is omitted.

1.2.3 Structure of matrix ring

The ideals of R and $M_n(R)$ are closed related:

Proposition 1.9. *There is a lattice isomorphism*

$$\{\text{Ideals of } R\} \to \{\text{Ideals of } M_n(R)\}$$

given by $A \mapsto M_n(A)$.

Recall a *division ring* (skew field) is a ring D in which every nonzero element is invertible. Thus, each division ring has no proper nonzero left or right ideals. To verify a ring D is a division ring, it suffices to prove that each nonzero element of D is left invertible. We will extend the *theory of vector spaces over field to modules over division rings*.

Remark 1.10. Any module M over a division ring D is free; indeed any maximal independent subset is a base. A *minimal left ideal* will mean minimal as a nonzero left ideal. A nonzero left ideal is simple as an R-module iff it's a minimal left ideal.

Proposition 1.11. *Suppose $R = M_n(D)$, where D is a division ring. Then the left ideal $L = R e_{jj}$ of R is minimal, for any $1 \le j \le n$. Moreover, R is a direct sum of minimal left ideals. Hence, R has composition length n as an R-module.*

1.3 Basic notions for noncommutative rings

1.3.1 The opposite ring

Definition 1.12. (opposite ring) *The opposite ring R^{op} has the same additive structure as original ring R, but with multiplication in the reverse order; i.e., the new product $a \cdot b$ is defined as the old product ba.*

It's easy to see that $(R^{op})^{op} = R$ and $R^{op} = R$ when R is commutative. Left R-modules are precisely right R^{op}-modules.

Remark 1.13. There is a natural isomorphism $M_n(R)^{op} \to M_n(R^{op})$, sending a matrix to its transpose. In particular, the right composition length of $M_n(D)$ equals the left composition length of $M_n(D^{op})$, which also is n.

1.3.2 Simple ring

Definition 1.14. *A ring R is simple if it has no proper nonzero ideals.*

Simple rings are building blocks of the structure theory of rings since any homomorphism from a simple ring to any ring is an injection. The commutative simple rings are just the fields. Note that, for noncommutative case, since the definition of simple rings involves lack of ideals, not left ideals, there are many simple rings that are not division rings. However, any division ring D is, of course, a simple ring. Then, by Proposition 1.9, $R = M_n(D)$ is simple. Then by Prop. 1.11, R is also left Artinian and left Noetherian.

1.3.3 Center of a ring

Definition 1.15. *The center of a ring R, denoted* $\mathrm{Cent}(R)$ *or* $Z(R)$*, is* $\{c \in R : cr = rc$ *for all r in $R\}$.*

It's easy to see that $Z(R)$ is a commutative ring. $Rc \lhd R$ for any $c \in Z(R)$. A well-known result is that is R is a simple ring, then $Z(R)$ is a field. Indeed, if $0 \neq c \in Z(R)$, then $1 \in Rc = R$ (from simplicity), which implies that $c^{-1} \in R$. Furthermore, $c^{-1}r = c^{-1}rcc^{-1} = c^{-1}crc^{-1} = rc^{-1}$, for all $r \in R$, proving that $c^{-1} \in Z(R)$.

1.4 The structure of $\mathrm{Hom}(M, N)$

Given two R-module M, N, define $\mathrm{Hom}_R(M, N)$ to be the set of R-module homos. from M to N. When understood, R may be deleted from the notation. $\mathrm{Hom}(M, M)$ is a ring whose multiplication is the composition of maps. To emphasize the ring structure, we write $\mathrm{End}_R(M)$ instead of $\mathrm{Hom}(M, M)$.

Given rings R, W, we say that M is an R, W-bimodule if M is both a left R-module and right W-module, satisfying the associative law $(ra)w = r(aw)$, for all $a \in M, r \in R, w \in W$.

Example 1.16. Any ring R itself is an R, R-bimodule. More generally, given a ring homomorphism $\phi : W \to R$, we can view R as an R, W-bimodule by taking $r_1 r_2 w$ to be $r_1 r_2 \phi(w)$. In particular, if R is a C-algebra, then we can view R as an R, C-bimodule. So any ring R is an $R, \mathbb{Z}$-bimodule.

Recall the definition of annihilator of module, $\mathrm{Ann}_R(M) = \{r \in R : rM = 0\}$. A module M is called *faithful* if $\mathrm{Ann}_R(M) = 0$. Note that for any nonzero R-module M, $\mathrm{Ann}_R(M) \lhd R$.

Remark 1.17. Every nonzero module M over a simple ring R is faithful. Indeed, $\mathrm{Ann}(M) \lhd R$ implies $\mathrm{Ann}(M) = 0$.

Proposition 1.18. *Suppose M is an R, W-bimodule,${}_RM_W$. There is a ring homomorphism $\phi\colon R \to \mathrm{End}M_W$ given by $\phi(r) = l_r$, where $l_r\colon M \to M$ with $a \to r\,a$. Furthermore,* $\ker\phi = \mathrm{Ann}_R M$.

Thus, ϕ is an *injection* if M is faithful as an R-module, which is true in particular if $M = R$.

1.5 Representations of rings and algebras

Definition 1.19. *A representation of a ring (resp. algebra) R is a homomorphism $\Phi\colon R \to \mathrm{End}M_W$, where M is a right module over the ring (resp. algebra) W. The representation Φ is faithful if* $\ker\Phi = 0$.

1.5.1 Schur's lemma

Proposition 1.20. (Schur's lemma)

1. *If $f\colon M \to N$ is a map of modules with M simple, then either $f = 0$ or f is monic.*
2. *If $f\colon M \to N$ is a map of modules with N simple, then either $f = 0$ or f is onto.*
3. *Every nonzero map $f\colon M \to N$ between simple modules is an isomorphism.*

Proposition 1.21. (another formulation of Schur's lemma) *If M is a simple module, then $\mathrm{End}_R M$ is a division ring. (Indeed, every nonzero element is invertible, by (3) in Prop. 1.20.)*

Example 1.22. Taking $R = M = W$, we have $R \cong \mathrm{End}R_R$. Similarly, $\mathrm{End}_R R \cong R^{op}$.

If M is free over W, we get matrix rings with following proposition.

Proposition 1.23. *The free right W-module $M = W^{(n)}$ is an $M_n(W), W$-bimodule, and the natural map $\phi\colon M_n(W) \to \mathrm{End}W_W^{(n)}$ is an isomorphism of rings. Similarly, $M_n(W) \cong (\mathrm{End}_W(W^{(n)}))^{op}$.*

By Remark 1.10, if M is a f.g. right module over a division ring D, then $\mathrm{End}M_D \cong M_n(D)$. Moreover, for simple modules, we have following theorem.

Theorem 1.24. *Suppose $M_i = S_i^{(n_i)}$ for $1 \le i \le t$, where S_i are simple pairwise nonisomorphic R-modules, and $M = M_1 \oplus \cdots \oplus M_t$. Then,*

$$\mathrm{End}_R(M) \cong \prod_{i=1}^{t} M_{n_i}(D_i),$$

where $D_i = \mathrm{End}S_i$.

We determined the structure of any ring R which is the direct sum of minimal left ideals.

Theorem 1.25. *A ring R is a finite direct sum of minimal left ideals i.f.f. $R \cong \prod_{i=1}^{t} M_{n_i}(D_i)$ for suitable t, suitable $n_i \in \mathbb{N}$, and division ring D_i. Furthermore, $R \cong L^{(n)}$ for a single minimal ideal L i.f.f. $t = 1$. In this case, $R \cong M_n(D)$ for the division algebra $D = \mathrm{End}_R L$.*

This result is used to prove the Wedderburn-Artin Theorem, which characterizes simple rings with a minimal left ideal as those of the form $M_n(D)$.

2 Semisimple modules and Wedderburn-Artin Theorem

2.1 Semisimple modules

Definition 2.1. (semisimple, completely reducible) *The scole* $\mathrm{soc}(M)$ *of a module M is the sum of simple submodules of M.*

$$\mathrm{soc}(M) = \sum \{N |\, N \text{ is a simple submodule of } M\}.$$

The module M is semisimple or completely reducible if $\mathrm{soc}(M) = M$.

For a ring R, $\mathrm{soc}(R)$ is the socle of R viewed as a module over itself. If M has no simple submodule, then define $\mathrm{soc}(M) = 0$. In fact, any integral domain that is not a field has socle 0.

The situation is straightforward when the underlying ring is a field F; then any module is a vector space V, which has a base B. For each $b \in B$, Fb has dimension 1, and thus must be a simple module. Furthermore, $V = \oplus_{b \in B} Fb$; so, in particular, $\mathrm{soc}(V) = V$, i.e., V is semisimple. Similarly, For any matrix ring $M_n(F)$ over a field F is also a semisimple ring.

Our first goal is to see that much of this vector space theory carries over to semisimple modules in general. Likewise, the sum of semisimple modules is semisimple. Any homomorphic image of a semisimple module is semisimple.

Proposition 2.2.

1. *If $N \subset M$, then* $\mathrm{soc}(N) \subset \mathrm{soc}(M)$.
2. *soc(soc(M))=soc(M).*
3. *If $M = \oplus M_i$ are R-modules, then* $\mathrm{soc}(M) = \oplus \mathrm{soc}(M_i)$.
4. *For $K \leq M$, $s\,o\,c(K) = s\,o\,c(M) \cap K$.*
5. *For any ring R, $s\,o\,c(R) \lhd R$.*
6. *For modules $K \leq M$, we have* $(\mathrm{soc}(M) + K)/K \leq \mathrm{soc}(M/K)$.

Proof. (1) Any homomorphic image of a simple module is simple or 0; hence for any map $f: N \to M$ of modules, $f(\mathrm{soc}(N)) \subset \mathrm{soc}(M)$. The embedding map here induces $f(\mathrm{soc}(N)) = \mathrm{soc}(N)$.

(2) Every simple submodule of M is a simple submodule of $\mathrm{soc}(M)$.

(3) $\mathrm{soc}(M_i) \subset \mathrm{soc}(M)$ by (1), so $\oplus \mathrm{soc}(M_i) \leq \mathrm{soc}(M)$. On the other hand, $\mathrm{soc}(M)_i \leq \mathrm{soc}(M_i)$ for the restriction map. Hence, $\mathrm{soc}(M) = \oplus \mathrm{soc}(M)_i \leq \mathrm{soc}(M_i)$. Thus, $\mathrm{soc}(M)$ is the unique largest semisimple submodule of M.

(4) $\mathrm{soc}(K) \subseteq K \cap \mathrm{soc}(M)$ is clear. On the other hand, because of the semisimplicity of $K \cap \mathrm{soc}(M)$, $K \cap \mathrm{soc}(M) \subseteq \mathrm{soc}(K)$.

(5) For any $r \in R$, L a minimal left ideal of R (and therefore $\mathrm{soc}(M) = \sum L$), clearly, we have $L\,r \leq L$ and then $L\,r$ is a minimal ideal or 0. Hence $L\,r \subset \mathrm{soc}(M)$ for any r, i.e., $\mathrm{soc}(R) \lhd R$.

(6) Consider an element $0 \neq a \in (\mathrm{soc}(M) + K)/K$, $a + K \subseteq \mathrm{soc}(M) + K$, then there exists an element $k \in K$, such that $a + k \in \mathrm{soc}(M)$. Consider the module homomorphism f: $M \to M/K$ given by $m \mapsto \bar{m}$ and we already know $f(\mathrm{soc}(M)) \subseteq \mathrm{soc}(M/K)$. Hence, $f(a + k) = a \in \mathrm{soc}(M/K)$. This may be strictly inequality. Consider $M = \mathbb{Z}$ and $K = 2\,\mathbb{Z}$, then since Z has no simple submodules, i.e. $\mathrm{soc}(\mathbb{Z}) = 0$, then we have $2\,\mathbb{Z}/2\,\mathbb{Z} = 1 < \mathrm{soc}(\mathbb{Z}/2\,\mathbb{Z}) = \mathbb{Z}/2\,\mathbb{Z}$. □

2.1.1 Complements of modules

Definition 2.3. (complement) *A complement of a submodule $N \leq M$ is a submodule $N' \leq M$ such that $N + N' = M$ and $N \cap N' = 0$. Thus $M = N \oplus N'$. The module M is complemented if every submodule of M has a complement.*

The complement (if it exists) need not be unique. Indeed, the x-axis is a one-dimensional subspace of $\mathbb{R}^{(2)}$; any other line passing through the origin is a complement.

Proposition 2.4. *Any submodule of a complemented module is complemented. More precisely, if $K \leq N \leq M$ and K has a complement K' in M, then K has the complement $K' \cap N$ in N.*

Unfortunately, complements need not exist. Indeed, for $M = \mathbb{Z}$, every two nonzero submodules intersect nontrivially, so no submodule has a complement.

Definition 2.5. *$N \leq M$ is a large, or essential, submodule of M if $N \cap K \neq 0$ for all $0 \neq K \leq M$.*

Obviously, a large submodule cannot have a complement. An *essential complement* for N (in M) is a submodule N' of M, for which $N \cap N' = 0$ and $N + N'$ is a large submodule of M.

Proposition 2.6. *Every submodule N of M has an essential complement.*

Proof. By Zorn's lemma, we can find $K \leq M$ maximal with respect to $N \cap K = 0$. We claim that $N + K$ is large in M. Indeed, suppose $T \leq M$ with $(N + K) \cap T = 0$. Suppose $a = b + c \in N \cap (K + T)$, then $a - b = c \in (N + K) \cap T = 0$, implying $a = b \in N \cap K = 0$. Hence $N \cap (K + T) = 0$. Hence, by our maximality assumption, we see that $K + T = K$; i.e. $T \subset K$, so $T = 0$. □

Remark 2.7. If $S \neq 0$ is a simple submodule of M and $N \leq M$, then $S \cap N \neq 0$ iff $S \subset N$.

Lemma 2.8. $\mathrm{soc}(M)$ *is contained in every large submodule of* M.

Proof. *It suffices to show that every large submodule contains every simple submodules* S *of* M*, which is true by the last Remark.* □

Theorem 2.9. *The following conditions are equivalent for a module* M*:*

(i) M *is semisimple.*

(ii) M *is complemented.*

(iii) M *has no proper large submodule.*

Proof. (i)⇒(iii) By lemma 2.8 any large submodule of M contains $\mathrm{soc}(M) = M$.

(iii)⇒(ii) By Prop. 2.6. Every submodule has an essential complement, then by (iii) the essential complement must be complement. Hence, M is complemented.

(ii)⇒(i) Suppose $\mathrm{soc}(M) \neq M$. By (ii) $\mathrm{soc}(M)$ has a complement $N \neq 0$. We want to find a simple submodule of N, since this would be a simple submodule of M not in $\mathrm{soc}(M)$, a contradiction. Take $0 \neq a \in N$, and take $K \leq N$ maximal with respect to $a \notin K$. By Prop. 2.4, K has a complement S in N. We claim that S is the desired simple submodule of N. Otherwise S has a proper nonzero submodule P. P has a complement $P' \neq 0$ in S, so $S = P \oplus P'$. Since $S \cap K = 0$, our assumption on K implies that both $a \in K + P$ and $a \in K + P'$. Write $a = k_1 + p = k_2 + p'$ for suitable $k_i \in K$, $p \in P$ and $p' \in P'$. Then $k_1 - k_2 = p' - p \in K \cap S = 0$. So $p' = p \in P' \cap P = 0$, implying that $a = k_1 \in K$, a contradiction. □

Remark 2.10. (1) A stronger version of this theorem says that for any module M,

$$\mathrm{soc}(M) = \cap\{\text{Large submodules of M}\}.$$

Note that $\cap\{\text{Large submodules of M}\}$ is complemented, since any submodule has an essential complement in M.

(2) Every submodule of a semisimple module is semisimple.

(3) Another method to prove (ii)⇒(i) relying on induction that every submodule of complemented module is complemented.

Example 2.11. (1) Any infinite-dimensional vector space over a field is semisimple but has infinite length.

(2) For any $n > 0$, the $\mathbb{Z}$-module $\mathbb{Z}/n$ is a finite set, and thus has finite length, but is not semisimple unless n is a product of distinct primes (square free).

Lemma 2.12. *If* $N_1 \subset N_2$ *in a semisimple module* M*, then any given complement* N_1' *of* N_1 *(in* M*) contains a complement of* N_2*.*

Theorem 2.13. *Suppose* M *is a semisimple module. The following conditions are equivalent:*

(1) M *has finite composition length.*

(2) M is Artinian.

(3) M is Noetherian.

(4) M is a finite direct sum of simple submodules.

Proof. (Sketch of Proof) (4)⇒(1)⇒(2) By definition. (2)⇒(3) By reductio ad absurdum with complements of decreasing chain. (3)⇒(4) By reductio ad absurdum, take maximal submodule of M with respect to being a direct sum of simple submodules. Then consider its complement which will contains a nonzero simple submodule. □

More generally, a module is semisimple if it is the direct sum of simple modules (not necessary of finite number).

2.2 Semisimple rings

Definition 2.14. (semisimple ring) *A ring R is a semisimple ring if R is semisimple as an R-module.*

We have a serious difficulty here: **A simple ring need not be semisimple**. Indeed, the full matrix ring over a field does not have any nontrivial ideals (since any ideal of $M(n, R)$ is of the form $M(n, I)$ with I an ideal of R), but has nontrivial left ideals (namely, the sets of matrices which have some fixed zero columns).

Proposition 2.15. *A ring R is semisimple i.f.f. it is a finite direct sum of minimal left ideals.*

Theorem 2.16. *A ring R is semisimple i.f.f. $R \cong \prod_{i=1}^{t} M_{n_i}(D_i)$ for suitable t, suitable $n_i \in \mathbb{N}$, and suitable division rings D_i.*

Proof. By Theorem 1.25 and Proposition 2.15. □

Remark 2.17. Given a semisimple ring $R = R_1 \times \cdots \times R_t$, where each $R_i = M_{n_i}(D_i)$, the left ideals of R are precisely $L = L_1 \times \cdots \times L_t$, where each $L_i < R_i$. Thus the maximal left ideals have the form

$$R_1 \times \cdots \times R_{i-1} \times L_i \times R_{i+1} \times \cdots \times R_t,$$

where L_i is a maximal ideal of R_i. Likewise, each (two-sided) ideal A of R is of form $A_1 \times \cdots \times A_t$, where $A_i = 0$ or $A_i = R_i$ (since R_i is simple). In particular, R/A is isomorphic to a direct product of some of the R_i, and thus also is a semisimple ring. Hence, R has precisely t maximal ideals.

2.2.1 Modules over semisimple rings

Proposition 2.18. *Any module M over a semisimple ring R is semisimple.*

Proof. Writing $R = \sum L$ as a sum of minimal left ideals, we have $M = \sum_{a \in M} R\, a = \sum_L \sum_{a \in M} L\, a$, a sum of simple modules by Remark 14.22 in p34 of the book. □

2.3 The Wedderburn-Artin Theorem

We bring in left Artinian rings, which clearly have minimal left ideals.

Theorem 2.19. (Wedderburn-Artin) *The following properties are equivalent for a ring R:*

1. $R \cong M_n(D)$;
2. *R is simple and left Artinian.*
3. *R is simple with a minimal left ideal.*
4. *R is simple and semisimple*

Proof. (1)⇒(2) By Prop. 1.11. (2)⇒(3) Clear. (3)⇒(4) $0 \neq \mathrm{soc}(R) \lhd R$, so $\mathrm{soc}(R) = R$. (4)⇒(1) By Theorem 2.16 we know that $R \cong \prod_{i=1}^{t} M_{n_i}(D_i)$ for suitable t. But if $t > 1$, then R cannot be simple. □

2.3.1 Preliminaries about division algebras

Suppose D is a division ring with center F. F is a field, and we often view D as an algebra over F; to emphasize this perspective, we call D a division algebra. For any $d \in D$, the subalgebra $F[d]$ is an integral domain.

Proposition 2.20. *The only finite dimensional division algebra D over an algebraically closed field F is F itself.*

Combining this proposition wit Theorem 2.16, we have

Theorem 2.21. *If R is a f.d. semisimple algebra over an algebraically closed field F, then R is isomorphic to a direct product of matrix algebras, i.e.,*

$$R \cong M_{n_1}(F) \times \cdots \times M_{n_t}(F).$$

There is also an appropriate formulation of Schur's Lemma in this case:

Proposition 2.22. (Schur's lemma) *Suppose for F an algebraically closed field, $R \subset M_n(F)$ such that $M = F^{(n)}$, viewed naturally as an R-module, is simple. If $f \in \mathrm{End}_R M$, then f is given by scalar multiplication. (Indeed, $\mathrm{End}_R M$ is a f.d. division algebra over F, hence is isomorphic to F.)*

Example 2.23. (A noncommutative f.d. division algebra over $\mathbb{R}$) We define Hamilton's algebra of quaternions $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}\, i \oplus \mathbb{R}\, j \oplus \mathbb{R}\, k$, where $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $ki = -ik = j$, and $jk = -kj = i$. These rules can be written more concisely as

$$i^2 = j^2 = k^2 = ijk = -1.$$

$\mathbb{H}$ is an $\mathbb{R}$-algebra, and in fact is a division algebra since $\forall a \in H, a^{-1} = \bar{a}/N(a)$. Frobenius showed that any noncommutative f.d. division algebra D over $\mathbb{R}$ is isomorphic to $\mathbb{H}$.

3 Jacobson's theory and Left Artinian Rings

In this chapter, we introduce the structure theory of rings, in order to yield decisive results about Artinian rings that strengthen parts of Theorem 2.19. In particular, we show that any Artinian ring R has a nilpotent ideal N such that R/N is semisimple Artinian. In this chapter, we use Jacobson's theory to describe Artinian rings.

3.1 Primitive rings and ideals

Definition 3.1. (primitive) *An ideal P is primitive if $P = \mathrm{Ann}_R M$ for some simple module M. A ring R is primitive if 0 is a primitive ideal, i.e., if R has a faithful simple module.*

Primitivity is the foundation stone of Jacobson's theory. To help remember the definition, recall Wedderburn-Artin Theorem, we have already deal with simple Artinian ring. Now, we focus on Artin, so we should define something more general than simplicity, but related to simplicity, and this is primitivity.

Remark 3.2. (1) Every simple ring R is primitive. Since every ring R has nonzero simple modules, which are faithful since R is simple.

(2) A commutative ring is primitive iff it is a field. Indeed, let R be primitive and let M be a faithful simple left R-module. Then $M \cong R/m$ for some maximal ideal m in R. Since $m \cdot M = 0$, it follows that $m = 0$. This clearly implies that R is a field. However, there are examples of noncommutative primitive rings that are not simple. For example, For D a division ring, if M is infinite-dimensional over D. Then the primitive ring $W = \mathrm{End}M_D$ is not simple. Since the set of finite rank linear transformations is a proper two-sided ideal of M, and hence it is not simple.

(3) An ideal is P is primitive iff R/P is primitive.

Remark 3.3. Here is a cute way of generating primitive ideals, which strengthens Nakayama's Lemma. Suppose M is any nonzero f.g. R-module. Writing $M = \sum_{i=1}^{t} R\, a_i$ with t minimal, take a submodule $N \supset \sum_{i=1}^{t-1} R\, a_i$ maximal with respect to $a_t \notin N$. Clearly N is a maximal submodule of N; hence, M/N is a simple module, and its annihilator P is a primitive ideal.

$\mathrm{Ann}_R M = \cap_{a \in M} \mathrm{Ann}_R a$. But, $\mathrm{Ann}_R a$ is a maximal left ideal of R when the module M is simple, hence we have

Proposition 3.4. *Every primitive ideal is the intersection of maximal left ideals.*

Every maximal left ideal L of a ring R contains a primitive ideal. Indeed, R/L is a simple R-module, so $\mathrm{Ann}_R R/L$ is a primitive ideal contained in $\mathrm{Ann}_R(1 + L) = L$.

Our main interest here lies in the following example.

Example 3.5. Suppose a ring $R = R_1 \times \cdots \times R_t$ is semisimple, where each R_i is simple Artinian. Any primitive ideal of R has the form $\mathrm{Ann} R/L$ for a suitable maximal left ideal L. Since the maximal left ideal L has the form

$$R_1 \times \cdots \times R_{i-1} \times L_i \times R_{i+1} \times \cdots \times R_t,$$

we see that $R/L \cong 0 \times \cdots \times 0 \times R_i/L_i \times 0 \times \cdots \times 0$. But $\mathrm{Ann}_{R_i}(R_i/L_i) = 0$ since R_i is simple, so

$$\mathrm{Ann}_R(R/L) = R_1 \times \cdots \times R_{i-1} \times 0 \times R_{i+1} \times \cdots \times R_t =: P_i,$$

which describes the maximal ideals. Thus, every primitive ideal of R is one of $P_1, \ldots, P_t$, and is thus a maximal ideal. In particular, if the ring R is primitive semisimple, then some $P_i = 0$, i.e., $R = R_i$ is simple Artinian.

3.1.1 Isomorphism classes of simple modules

The isomorphism classes of simple modules of a given ring is a very fundamental question in module theory.

Proposition 3.6. *Suppose a primitive ring R has a minimal nonzero left ideal L. Then every faithful simple R-module M is isomorphic to L.*

Corollary 3.7. *(1)If R is a simple ring with nonzero socle, then any two simple R-modules are isomorphic.*

(2) The Wedderburn-Artin decomposition $R = M_n(D)$ of a simple Artinian ring R is unique.

3.1.2 Prime and semiprime rings

Definition 3.8. (prime) *A ring R is prime if the product of any two nonzero ideals is nonzero.*

Thus a commutative prime ring is just an integral domain. Prime rings often are the "correct" generalization of integral domains in the noncommutative theory. In a prime ring R, the product $A_1 \cdots A_m$, of any finite number of nonzero ideals is nonzero. If L is a left ideal and I is a right ideal of R, then $L\,I \lhd R$.

$\mathbb{Z}$ is an example of a prime ring that is not primitive (Since it is not a field). A noncommutative example is $M_2(\mathbb{Z})$.

Remark 3.9. (1) Any primitive ring R is prime. Indeed, take a faithful simple module M, suppose $A, B \lhd R$ with $A\,B = 0$ but $B \neq 0$. Then $0 \neq B\,M \leq M$, implying that $B\,M = M$. But then $0 = (A\,B)\,M = A\,(B\,M) = A\,M$, implying that $A = 0$.

(2) Conversely, if a prime ring R has a minimal nonzero left ideal L, then $\mathrm{Ann}_R L = 0$; thus, L is a faithful simple module, so R is primitive.

Definition 3.10. (semiprime) *A ring R is semiprime if $A^2 \neq 0$ for any $0 \neq A \lhd R$.*

Remark 3.11. A semiprime ring R has no nonzero nilpotent ideals.

3.2 The Jacobson radical

Definition 3.12. (Jacobson radical) *The Jacobson radical* $\mathrm{Jac}(R)$ *is the intersection of the primitive ideals of R.*

Proposition 3.13. *Let $J = \mathrm{Jac}(R)$, then*

1. J is also the intersection of the maximal left ideals of R.

2. If $a \in J$, then $1 - a$ is left invertible.

3.3 The structure of left Artinian rings

We apply these results to develop the structure theory for left Artinian rings, which we recall are rings that satisfy the descending chain condition (DCC) on left ideals. Since any left Artinian ring must have minimal nonzero left ideals, which implies that "prime" and "primitive" coincide in the class of left Artinian rings.

Theorem 3.14. *Suppose R is left Artinian, and let $J = \mathrm{Jac}(R)$. Then*

(1) J is the intersection of finitely many maximal left ideals of R.

(2) R/J is a semisimple ring.

(3) There are only finitely many primitive ideals of R, and each primitive ideal is maximal.

(4) J is a nilpotent ideal.

Proof omitted. One immediate consequence of this theorem (3) is the following improvement of the Wedderburn-Artin Theorem:

Theorem 3.15. *Any prime left Artinian ring is simple.*

Let us summarize our results characterizing semisimple rings:

Theorem 3.16. *The following are equivalent for a ring R:*

1. *R is semisimple.*
2. *R is a finite direct sum of simple right R-module.*
3. *R is left Artinian and semiprime.*

4. *R is right Artinian and semiprime.*

5. *R is a finite direct product of matrix rings over division rings.*

Here is one more striking application.

Theorem 3.17. (Hopkins-Levitzki) *Any left Artinian ring R is also left Noetherian.*

Proof. We show that R has finite composition length. Let $J = \mathrm{Jac}(R)$. By Theorem 3.14(4), $J^t = 0$ for some t. Consider the chain of modules

$$R \supset J \supset J^2 \supset \cdots \supset J^t = 0.$$

Each factor module $M_i = J^{i-1}/J^i$ is Artinian, and is naturally a module over the semisimple ring R/J and thus is semisimple. Since, any semisimple Artinian module has finite composition length, so $l(R) = \sum_{i=1}^{t} l(M_i)$, as desired □

3.3.1 Finite-dimensional algebras

Definition 3.18. (split) *A semisimple F-algebra R is split if*

$$R \cong M_{n_1}(F) \times \cdots \times M_{n_t}(F)$$

for suitable t and suitable n_i, $1 \leq i \leq t$.

Theorem 3.19. *Suppose R is a f.d. algebraic over field F. Then $\mathrm{Jac}(R)$ is a nilpotent ideal and $R/\mathrm{Jac}(R)$ is a direct product $R_1 \times \cdots \times R_t$ of f.d. simple F-algebras. If F is algebraically closed, then $R/\mathrm{Jac}(R)$ is split.*

The theorem is far from the end of the story for f.d. algebras. Wedderburn proved the amazing result that R/J is actually isomorphic to a subalgebra of R.

Theorem 3.20. (Wedderburn's principal theorem) *Suppose R is f.d. algebra over a field F and R/J is split, where $J = \mathrm{Jac}(R)$. Then the semisimple algebra $S = R/J$ is isomorphic to a subalgebra $\tilde{S}$ of R, which is a vector space complement of J in R; i.e., $R = \tilde{S} \oplus J$. This decomposition is so called Wedderburn decomposition of R.*

3.4 Jacobson's program

We call a ring R semiprimitive if $\mathrm{Jac}(R) = 0$; then R is a subdirect product of primitive rings. The Jacobson program in the structure of rings studies R in terms of $\mathrm{Jac}(R)$ and the semiprimitive ring $R/\mathrm{Jac}(R)$. This program is particularly useful for those rings whose primitive homomorphic images are simple.

We turn to the general structure theory, featuring Jacobson's general theory of primitive rings and the Jacobson radical, for rings not necessarily satisfying chain conditions.

3.4.1 Chevalley-Jacobson Density Theorem

Suppose M is a given R-module, and let $W = (\mathrm{End}_R M)^{op}$. Clearly M is also a right W-module, under the scalar multiplication $a\,f = f(a)$ for $a \in M$ and $f \in W$, since $a\,(f\,g) = f\,g(a) = (a\,g)\,f$ for all $a \in M$ and $f, g \in W$. M thereby becomes an R, W-bimodule, which is faithful as a right W-module (since $f(M) = 0$ iff $f = 0$).

Taking $\hat{R} = \mathrm{End}M_W$, we have a natural homomorphism $\Phi\colon R \to \hat{R}$ given by $r \mapsto l_r$; Φ is an injection whenever the R-module M is faithful. Although it is too much to expect that Φ is onto, one has the celebrated **Density Theorem** that, for M semisimple, the image $\Phi(R)$ is dense in $\hat{R}$ with respect to the following topology:

Given a finite set $a_1, \ldots, a_n \in M$ and $f_0 \in \hat{R}$, define

$$B(a_1, \ldots, a_n; f_0) = \{ f \in \hat{R} \colon f(a_i) = f_0(a_i), 1 \le i \le n \}.$$

The $\{B(a_1,\ldots,a_n; f_0) \colon n \in \mathbb{N}, a_i \in M, f_0 \in \hat{R}\}$ comprise a sub-base of a topology on $\hat{R}$, called the finite topology.

Theorem 3.21. (General Density Theorem) *If M is a semisimple R-module, then $\Phi(R)$ is dense in $\hat{R}$ under the finite topology.*

Now suppose the module M is simple. By Schur's Lemma, $(\mathrm{End}_R M)^{op}$ is a division ring D over which M is viewed as a vector space (on the right).

Theorem 3.22. (Jacobson Density Theorem for Simple Modules) *Suppose M is a simple R-module, and $D = \mathrm{End}_R M$. For any $n \in \mathbb{N}$, any D-independent elements $a_1, \ldots, a_n \in M$, and any elements $b_1, \ldots, b_n$ of M, there is $r \in R$ such that $r\,a_i = b_i$ for $1 \le i \le n$.*

Corollary 3.23. *If M is a faithful simple R-module and M has dimension $n < \infty$ as a right vector space over $D = \mathrm{End}_R M$, then R has the form $M_n(D)$ and thus is simple Artinian.*

4 Tensor Product

The direct sum of two vector spaces A and B over a field F has the property that the dimension $\dim_F(A \oplus B) = \dim_F A + \dim_F B$, since the union of bases of $A \times \{0\}$ and $\{0\} \times B$ is a base of $A \oplus B$. Analogously, we already have noted that the vector space $A \otimes B$, called the tensor product, has dimension $\dim_F A \cdot \dim_F B$.

When A and B are algebras, just as $A \times B$ turns out to be an algebra, also $A \otimes B$ has a natural structure as an algebra.

Definition 4.1. *Suppose A, B are vector spaces over a field F, with respectively bases $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_n\}$. $A \otimes B$ is defined as the vector space of dimension $m\,n$ over F with base labeled $\{a_i \otimes b_j \colon 1 \le i \le m, 1 \le j \le n\}$.*

When A and B are algebras, we introduce a multiplication on $A \otimes B$, starting with the simple tensors:

$$(a \otimes b)\,(a' \otimes b') = a\,a' \otimes b\,b'.$$

This extends to a product on all of $A \otimes B$.

Before proceeding, let us record some basic properties of tensor products:

$$\begin{aligned}(a_1 + a_2) \otimes b &= a_1 \otimes b + a_2 \otimes b;\\ a \otimes (b_1 + b_2) &= a \otimes b_1 + a \otimes b_2;\\ \alpha\, a \otimes b &= a \otimes \alpha\, b\end{aligned}$$

For all $a \in A, b \in B, \alpha \in F$. Hence, the map $(a, b) \mapsto a \otimes b$ resembles a bilinear form.

4.1 Basic construction

Suppose R is any ring, not necessarily commutative. Given a right R-module M and an R-module N, we want to produce an Abelian group $M \otimes_R N$ spanned by "simple tensors" $a \otimes b$ for $a \in M, b \in N$, satisfying the following properties:

$$\begin{aligned}(a_1 + a_2) \otimes b &= a_1 \otimes b + a_2 \otimes b;\\ a \otimes (b_1 + b_2) &= a \otimes b_1 + a \otimes b_2;\\ r\, a \otimes b &= a \otimes r\, b\end{aligned}$$

for all $a \in A, b \in B, r \in F$.

These properties form the foundation of our construction, which is to be universal as so-called a balanced map.

Proposition 4.2. *Suppose $f\colon M \to M'$ is a map of right R-modules and $g\colon N \to N'$ is a map of R-module. Then, there is a group homomorphism denoted*

$$f \otimes g\colon M \otimes N \to M' \otimes N'$$

given by $(f \otimes g)\,(a \otimes b) = f(a) \otimes g(b)$.

Remark 4.3. If, in above Proposition, f, g are isomorphisms, then $f \otimes g$ is also an isomorphism, which inverse is given by $f^{-1} \otimes g^{-1}$. In other words, if $M \cong M', N \cong N'$, then $M \otimes N \cong M' \otimes N'$.

4.1.1 Tensor product of bimodules

Proposition 4.4. *Suppose R and T are arbitrary rings, M is a T, R-bimodule, and N is an R-module. Then $M \otimes_R N$ is a T-module under the multiplication $t\,(a \otimes b) = t\,a \otimes b$ for $t \in T, a \in M, b \in N$.*

Remark 4.5. (1) When T is a ring containing R and $M = T$, the T-module $T \otimes_R N$ is called the T-module extended from N.

(2) The last proposition also has a right-handed version.

4.1.2 Isomorphisms of tensor products

Proposition 4.6. *$R \otimes_R N \cong N$ for any R-module N.*

Example 4.7. If V is a vector space over a field F and V^* is the dual space, then

$$V \otimes_F V^* \cong \mathrm{End}_F V \cong M_n(F).$$

Proposition 4.8. *For any modules A, B over a commutative ring C, there is a twist isomorphism $\tau: A \otimes_C B \to B \otimes_C A$ given by $\tau(a \otimes b) = b \otimes a$.*

5 Group Representations and Group Algebras

In this chapter we define group representations over a field F, and study their basic properties in terms of the structure of the group algebra, featuring Maschke's Theorem. We focus on finite groups, with emphasis at the end on the symmetric group S_n.

5.1 Group representations

Definition 5.1. *A **representation** of a (multiplicative) group G is a group homomorphism $\rho: G \to \mathrm{GL}(V)$ for a suitable vector space V over F. We consider only the case when $\dim_F V = n \leq \infty$ in the next two chapters, then we say that the representation ρ is finite-dimensional (f.d.) of degree n. The representation ρ is called complex if $F = \mathbb{C}$; is called real if $F = \mathbb{R}$.*

Representations of groups are among the most important tools in mathematics. They enable us to study elements of the groups in terms of matrix techniques. The case when the base field F is algebraically closed is especially important, since F then contains the eigenvalues of the matrices.

The kernel of the group representation ρ, denoted $\ker\rho$, measures the amount of information lost in passing to $\mathrm{GL}_n(F)$. A representation with kernel $\{1\}$ is called faithful.

Example 5.2. (regular representation) The symmetric group S_n has a faithful representation sending the permutation π to the permutation matrix $\sum e_{\pi(i),i} \in \mathrm{GL}(n, F)$. Combined with Cayley's Theorem, which injects any group G of order n into S_n, this shows that any group G of order n has a faithful representation ρ into $\mathrm{GL}(n, F)$ (For S_n, it has a regular representation with order $n!$), called the regular representation ρ_{reg}, sending an element $g \in G$ to the permutation matrix corresponding to the left multiplication map l_g. All the diagonal entries of the permutation matrix ρ_{reg} are 0 unless $g = 1$, and $\rho(1) = 1$.

More generally, a **permutation representation** is a representation ρ for which $\rho(g)$ is a permutation matrix, $\forall g \in G$.

5.1.1 Degree 1 representations

The degree representations are just the group homomorphisms $G \to \mathrm{GL}(1, F) = F^\times$. The unit representation, or trivial representation, denoted as 1, is the degree 1 representation given by $\rho(g) = 1$ for all $g \in G$. All other representations are called nontrivial.

We can already determine all degree 1 representations of finite Abelian groups.

Lemma 5.3. *(1) The number of degree 1 representations of cyclic group C_n equals the number of distinct n-th roots of 1 contained in F, which is n precisely when F contains a primitive n-th root of 1.*

(2) Suppose $A = C_1 \times \cdots \times C_m$ is a finite Abelian group, written as a direct product of cyclic groups C_i of order n_i. If F contains primitive n_i-th roots of 1 for $1 \le i \le m$, then A has precisely $n_1 \cdots n_m = |A|$ distinct degree 1 representations.

Thus, we usually want to work in a field that contains "enough" roots of unity. A famous example if the Klein group $K_4 = \langle a, b : a^2 = b^2 = (a\,b)^2 = 1 \rangle$. Any degree 1 representation ρ of K_4 must satisfy $\rho(a) = \pm 1$ and $\rho(b) = \pm 1$, and each of these four possibilities yields a representation, so K_4 has exactly four degree 1 representations, including the trivial representation.

Remark 5.4. For any representation $\rho : G/N \to \mathrm{GL}(V)$ of G/N, where $N \lhd G$, the composite $G \to G/N \to^{\rho} \mathrm{GL}(V)$ defines a representation $\hat{\rho}$ of G, given explicitly by $\hat{\rho}(g) = \rho(Ng)$. We say that the representation ρ lifts to $\hat{\rho}$. Note that $\ker\rho = \ker\hat{\rho}/N$. Conversely, given a representation $\rho : G \to \mathrm{GL}(V)$ and $N \subset \ker\rho$, we have a natural representation $\bar{\rho}$: $G/N \to \mathrm{GL}(V)$ by Noether's first isomorphism theorem. In particular, any representation ρ of G is lifted from a faithful representation of the group $G/\ker\rho$.

When the representation ρ has degree 1, the group $G/\ker\rho$ is injected into $F^\times$ and thus is Abelian; in fact $G/\ker\rho$ is cyclic (Finite subgroups of the multiplicative group of a field are cyclic). Thus, the degree 1 representations of any finite group G can be obtained by finding those normal subgroups such that G/N is cyclic, and then lifting their faithful representations.

Hence, we can extend Lemma 5.3 to arbitrary groups by means of the commutator subgroup G' ($G' \lhd G, G/G'$ is Abelian and G' is contained in every $N \lhd G$ such that G/N is Abelian.)

Proposition 5.5. *Suppose m is the exponent (the exponent of a group is defined as the least common multiple of the orders of all elements of the group) of the group G/G', and F contains a primitive m-th root of 1. Then the number of distinct complex degree 1 representations of G is $[G : G']$.*

Proof. Let $n = [G : G']$. G/G', being Abelian, has n complex degree 1 representations, each of which provides a degree 1 representation of G by Remark 5.4. Conversely, for ρ of degree 1, clearly $G/\ker\rho$ is abelian even cyclic, implying that $\ker(\rho) \supseteq G'$, and thus ρ is lifted from a degree 1 representation of G/G'. □

Example 5.6. (1) 1 and sgn are the only degree 1 representations of S_n.

(2) $|G| = 8$, there are two nonabelian examples: $G = D_4$ or $G = Q_8$. For $G = D_4 = \langle a, b : a^4 = b^2 = 1, b\,a\,b^{-1} = a^{-1}\rangle$, the dihedral group. Then $N = \langle a^2\rangle \lhd G$, then $G/N \cong K_4$ has four degree 1 representations, which lift to four degree 1 representations of G. For $G = Q_8 = \langle a, b : a^4 = b^4 = 1, a^2 = b^2, b\,a\,b^{-1} = a^{-1}\rangle$. Again, $N = \langle a^2\rangle \lhd G$ and $G/N \cong K_4$ has four degree 1 representations, which lift to four degree 1 representations of G. (Commutator subgroups of D_n and Q_8 are both $\langle a^2\rangle$.)

5.1.2 Finite dimensional representations of degree greater than 1

Definition 5.7. *Given two representations ρ, φ of respective degree m, n, we define their direct sum $\rho \oplus \varphi$ of degree $m + n$, by*

$$(\rho \oplus \varphi)(g) = \operatorname{diag}\{\rho(g), \varphi(g)\}.$$

Remark 5.8. (1) If $a, b \in G$ are conjugate, then $\rho(a)$ and $\rho(b)$ have the same minimal polynomial, eigenvalues and also the same characteristic polynomial.

(2)Suppose $g \in G$ with $g^m = 1$ and $F \subseteq \mathbb{C}$ contains a primitive m-th root of I. Then $\rho(g)^m = I$ for any representation ρ of G. Hence, the matrix $\rho(g)$ is diagonalizable, and with respect to a suitable base, we may assume that

$$\rho(g) = \operatorname{diag}\{\zeta_1, \ldots, \zeta_n\},$$

where $n = \deg(\rho)$. Furthermore,

$$\rho(g^{-1}) = \rho(g)^{-1} = \operatorname{diag}\{\zeta_1^{-1}, \ldots, \zeta_n^{-1}\} = \operatorname{diag}\{\bar{\zeta_1}, \ldots, \bar{\zeta_n}\}.$$

Example 5.9. (1) A faithful complex representation ρ of S_3 having degree 2. Clearly, $\rho((12))$ must have order 2 and $\rho((123))$ must have order 3. We may assume that $\rho((123))$ is diagonal, with $\{1, \zeta, \zeta^2\}$. But $(123)^{-1} = (132) = (12)(123)(12)^{-1}$ Hence $\rho((123)) = \operatorname{diag}\{\zeta, \zeta^2\}$ or $\operatorname{diag}\{\zeta^2, \zeta\}$. We take $\rho(12) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, since the conjugation equality. Clearly, ρ is faithful. Actually, we obtain this representation by viewing S_3 as the dihedral group D_3 of order 6, and this example can be generalized easily to any dihedral group.

(2) A faithful representation ρ of S_3 over $\mathbb{Q}$, having degree 2, with $\rho((123)) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ and $\rho((12)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(3) A faithful representation of the dihedral group D_4, having degree 2: $a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $b \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

5.2 Modules and vector spaces over groups

Although historically the theory of group representations preceded the theory of modules, we motivate our study with the structure of modules, since it gives us a ready framework on which to build the theory.

Remark 5.10. If $G \to M$ is a homomorphism of monoids and G is a group, then $f(G)$ is also a group.

Definition 5.11. (G-module, G-space) *A module over a monoid G, or G-module, is an Abelian group V together with an action $G \times V \to V$ satisfy the following laws for all g, $h \in G, v, w \in V$:*

(1) $1\,v = v$;

(2) $(g\,h)\,v = g\,(h\,v)$;

(3) $g\,(v+w) = g\,v + g\,w$.

A G-module map is a group homomorphism: $f: V \to W$ such that $f\,(g\,v) = g\,f(v), \forall g \in G$, $v \in V$. When a G-module V is a vector space over a given field F, we say that V is a G-space if it also satisfies the condition

(4) $f\,(\alpha\,v) = \alpha\,(g\,v), \forall \alpha \in F$.

Remark. Any Abelian group V becomes a G-module via the trivial action $gv = v$.

We get the following basic correspondence.

Proposition 5.12. *For any group G, there is a 1:1 correspondence (explicitly) between group representations $G \to \mathrm{GL}(V)$ and G-space structures on V.*

5.3 Group algebras

Now we work over any arbitrary commutative ring C.

Definition 5.13. (group algebra) *For any set X, we define the free C-module $C\,X$ with base indexed by the elements of X. A typical element of $C\,X$ is $\sum_{g \in X} \alpha_g\,g$, where $\alpha_g \in C$ and almost all $\alpha_g = 0$. Now suppose X is a group G. The group algebra $C[G]$ is defined to be the free C-module $C\,G$, also endowed with multiplication given by*

$$\left(\sum_{g \in G} \alpha_g\,g\right)\left(\sum_{h \in G} \beta_h\,h\right) = \sum_{s \in G}\left(\sum_{gh=s} \alpha_g\,\beta_h\right)s,$$

which makes $C[G]$ an algebra over C.

We can view G as a multiplicative subgroup of $C[G]$ via a natural monoid homomorphism $g \mapsto 1_C\,g$.

Lemma 5.14. *Suppose $U = \mathrm{Unit}(R)$ of a C-algebra R.*

(1) Any C-algebra homomorphism $f: C[G] \to R$ restricts to a group homomorphism $f|_G$: $G \to U$.

(2) Conversely, for any group homomorphism $f: G \to U$, there is a unique C-algebra homomorphism $\hat{f}: C[G] \to R$ whose restriction to G is f.

(3) Parts (1) and (2) are inverse correspondences, thereby yielding a 1:1 correspondence between group homomorphism $G \to U$ and algebra homomorphisms $C[G] \to R$.

Thus, for any field F, the theory of group representations of a group G corresponds precisely to the theory of algebra representations of the group algebra $F[G]$.

Let us summarize the connections among the various structures.

Proposition 5.15. *Given a vector space V over a field F, we have a 1:1 correspondence between:*

(1) group representations $\rho: G \to \mathrm{GL}(V)$;

(2) algebra representations $F[G] \to \mathrm{End}_F V$;

(3) G-space structures on the vector space V;

(4) $F[G]$-module structures on V.

Remark 5.16. $F[G]$ is a commutative ring i.f.f. G is an Abelian group.

Definition 5.17. *Two representations ρ and τ of G over F are equivalent if their corresponding $F[G]$-modules are isomorphic.*

Suppose representations ρ and τ provide isomorphic $F[G]$-module structures on $V = F^{(n)}$. Thus, there is a linear transformation $T: V \to V$ that also is a G-module map, i.e.,

$$T(\rho(g)\, v) = \tau(g)\, T(v)$$

for all $g \in G, v \in V$. Writing A (called intertwining map) for the matrix corresponding to the linear transformation T, then we will get $A\,\rho(g) = \tau(g)\, A$, implying

$$\tau(g) = A\,\rho(g)\, A^{-1}.$$

Definition 5.18. (irreducible representation) *A representation is irreducible i.f.f. it corresponds to a simple $F[G]$-module. A representation is reducible if it is not irreducible.*

Let us see what reducibility means in matrix terms. Suppose a representation $\rho: G \to \mathrm{GL}(n, F)$ is reducible. In other words, $V = F^{(n)}$ has a proper nonzero G-subspace W. Let $m = \dim_F W < n$ and extend an F-base $b_1, \ldots b_m$ of W to a F- base $b_1, \ldots, b_n$ of V. Taking the equivalent representation τ with respect to this new base, we can partition any $n \times n$ matrix as $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, with A is $m \times m$ and D is $(n-m) \times (n-m)$. Thus , writing

$$\tau(g) = \begin{pmatrix} A(g) & B(g) \\ C(g) & D(g) \end{pmatrix},$$

we have $\tau(g)(w) \in W$ for all w in W; i.e., $C(g)\, W = 0$, so $C(g) = 0$. We conclude that for all $g \in G$ that $\tau(g)$ is of the form

$$\tau(g) = \begin{pmatrix} A(g) & B(g) \\ 0 & D(g) \end{pmatrix}.$$

From $\tau(gh) = \tau(g)\,\tau(h)$, we can get $A(gh) = A(g)\,A(h)$ and $D(gh) = D(g)\,D(h)$.

In this manner, our setup gives rise to two more representations: (1) τ restricts to a representation $\tau|_W$ sending $g \mapsto A(g)$, which has degree m and corresponding to the G-subspace W; (2) The representation $g \mapsto D(g)$ has degree $n-m$ and corresponding to the factor space V/W.

Conversely, if $\tau(g)$ has this form $\begin{pmatrix} A(g) & B(g) \\ 0 & D(g) \end{pmatrix}$ for all $g \in G$, then the subspace W generated by the first m elements of the bases of V satisfies $\tau(g)\,W \subseteq W$ for all $g \in G$, implying that τ is reducible.

Proposition 5.19. *A group representation ρ of degree n is reducible, i.f.f. there is an equivalent representation τ for which each matrix $\tau(g), g \in G$ has the form $\begin{pmatrix} A(g) & B(g) \\ 0 & D(g) \end{pmatrix}$ for suitable $1 \leq m < n$.*

Corollary 5.20. *If $\rho: G \to \mathrm{GL}(n, F)$ is a representation such that the corresponding algebra homomorphism $\hat{\rho}: F[G] \to M_n(F)$ is **onto**, then ρ is irreducible.*

Proof. Otherwise, replacing ρ by a suitable equivalent representation, we could assume that $\rho(g)$ has quasi-triangle form as above. But then $\hat{\rho}(\sum \alpha_g g) = \sum \alpha_g \rho(g)$ also has this form, contrary to $\hat{\rho}$ being onto. □

Definition 5.21. *A representation is called* ***completely reducible*** *if it is the direct sum of irreducible representations.*

Remark 5.22. A representation is completely reducible i.f.f. its corresponding module is **semisimple**.

5.4 Maschke's Theorem

Lemma 5.23. *Let M_i be $F[G]$-modules for a finite group G, and suppose $\psi: M_1 \to M_2$ is an arbitrary linear transformation over F. Then we have an $F[G]$-module map $\bar{\psi}: M_1 \to M_2$ defined by*

$$\bar{\psi}(v) = \sum_{g \in G} g^{-1}\,\psi\,(g\,v), \forall v \in M_1.$$

Proof. Clearly $\bar{\psi}$ is an F-linear transformation. Furthermore, for any element $h \in G$, we have

$$\begin{aligned}
\bar{\psi}(h\,v) &= \sum_{g \in G} g^{-1}\,\psi\,(g\,(h\,v)) \\
&= \sum_{g \in G} g^{-1}\,\psi\,((g\,h)\,v) \\
&= \sum_{gh \in G} h\,(g\,h)^{-1}\,\psi\,((g\,h)\,v) \\
&= h\,\bar{\psi}(v).
\end{aligned}$$

□

The map $\Phi\colon \mathrm{Hom}_F(M_1, M_2) \to \mathrm{Hom}_{F[G]}(M_1, M_2)$ given by $\psi \to \bar{\psi}$ is called the **averaging procedure**. Note that if ψ is already an $F[G]$-module map, then

$$\bar{\psi}(v) = \sum_{g \in G} g^{-1}\, \psi\,(g\, v) = \sum_{g \in G} \psi\,(g^{-1}\, g\, v) = |G|\, \psi(v),$$

so we see that Φ is onto when $|G|^{-1} \in F$.

Theorem 5.24. (Maschke's Theorem) *$F[G]$ is a semisimple ring, for any finite group G whose order is not divisible by* $\mathrm{char}(F)$*. (This condition is automatic when* $\mathrm{char}(F) = 0$*.)*

Proof. From the equivalent theorem of semisimple ring, it suffices to show that any left ideal L of $F[G]$ has a complement as an $F[G]$-module. Certainly L has a complement as a vector space over F, so define the corresponding projection $\pi\colon F[G] \to L$ and take $\bar{\pi}$ as in Lemma 5.23. Clearly, $\bar{\pi}(F[G]) \subseteq L$, so $g\,\bar{\pi}(a) \in g\,L \subseteq L$, implying $\pi\,(g\,\bar{\pi}(a)) = g\,\bar{\pi}(a)$ for all $g \in G$ and $a \in F[G]$. Consequently, we have the $F[G]$-module map $\hat{\pi} = \frac{1}{|G|}\,\bar{\pi}\colon F[G] \to L$. For each $a \in L$, we have $g\,a \in L$; hence, $\pi\,(g\,a) = g\,a$ and

$$\hat{\pi}(a) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\, \pi\,(g\,a) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\,(g\,a) = a.$$

Hence, $\hat{\pi}(F[G]) = L$, and $\hat{\pi}$ is a projection as $F[G]$-modules. □

Corollary 5.25. *Under the hypotheses of Maschke's Theorem, every representation of G is completely reducible.*

5.5 Group algebras over splitting fields

Maschke's Theorem leads us to the following variant of Definition 3.18.

Theorem 5.26. *A field F is a splitting field of a group G if*

$$F[G] \cong M_{n_1}(F) \times \cdots \times M_{n_t}(F),$$

for suitable n_i, where $n_1 = 1$.

It follows that $F[G]$ is split semisimple, with each simple component having center F.

Remark 5.27. If K/F is a field extension and G is a group, then

$$K[G] \cong K \otimes_F F[G].$$

Indeed, the balanced map $K \times F[G] \to K[G]$ given by $(k, a) \mapsto k\,a$ yields an algebra homomorphism $\Phi\colon K \otimes_F F[G] \to K[G]$. But $K \otimes_F F[G]$ and $k[G]$ are both free K-modules with base G, which is fixed by Φ, so Φ is an isomorphism.

Proposition 5.28. *Any finite group G has a splitting field that is a finite extension of $\mathbb{Q}$.*

Remark 5.29. By Theorem 2.21 and Maschke's Theorem, any algebraically closed field of characteristic 0 is a splitting field of every finite group. Surprisingly, when $|F|$ is finite and relatively prime to $|G|$, $F[G]$ must be split, because of another theorem of Wedderburn. (But F may not be a splitting field of G.) For arbitrary fields, by a theorem of Brauer, if $\exp(G) = m$, then any field F containing a primitive m-th root of 1 is a splitting field of G.

Proposition 5.30. *For any splitting field F of the group G, a representation ρ of degree n is irreducible i.f.f. $\{\rho(g) : g \in G\}$ spans $M_n(F)$.*

For example, for ρ irreducible, if $g \in Z(G)$, then $\rho(g)$ commutes with all of $M_n(F)$ and thus is a scalar matrix.

Remark 5.31. The number of components of $F[G]$ which is isomorphic to F is precisely $[G : G']$.

We can summarize the situation quite concisely for Abelian groups:

Proposition 5.32. *The following are equivalent for F a splitting field of a finite group G:*

(1) G is Abelian;

(2) The group algebra $F[G]$ is commutative;

(3) $F[G] \cong F \times F \times \cdots \times F$;

(4) Every irreducible representation of G has degree 1.

Remark 5.33. We have the following formula:

$$|G| = \dim_F F[G] = \sum_{i=1}^{t} \dim_F M_{n_i}(F) = \sum_{i=1}^{t} n_i^2 = 1 + \sum_{i=2}^{t} n_i^2.$$

For low values of n, this formula often enables us to determine t with hardly any other prior knowledge of the group structure of G. For example, it is well known that any nonabelian group of order 6 (resp. 8) is isomorphic to the symmetric group S_3 (resp. the dihedral group or the quaternion group of order 8). Indeed, for $n = 6$, note that $6 = 1 + 1 + 2^2$ is the only way of writing such sum (not all 1), so G is nonabelian i.f.f. $t = 3$, in which case $F[G] \cong F \times F \times M_2(F)$. For $n = 8$, likewise $8 = 1 + 1 + 1 + 1 + 2^2$, so G is nonabelian i.f.f. $t = 5$. In this case G has precisely one complex representation of degree 2 (up to equivalent) to go along with the four complex representation of degree 1, so $\mathbb{C}[G] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.

5.5.1 The center of the group algebra

There is another important description of this number t inside the formula through the center $\mathrm{Cent}(F[G])$, which is $F \times \cdots \times F$, taking t times, so $\dim_F \mathrm{Cent}(F[G]) = t$.

We would like a base of Cent$F[G]$ that is given explicitly in terms of the elements of G. For future reference, let us consider $C[G]$. If G is Abelian, then $C[G]$ is commutative, $t = |G|$, and G itself is the base. For G nonabelian, we want to enlarge $Z(G)$ to a base of Cent$(C[G])$.

Theorem 5.34. *For any commutative ring C,* Cent$(C[G])$ *is free as a C-module having base $\{z_{\mathcal{C}}: \mathcal{C}$ is a conjugacy class of $G\}$, where $z_{\mathcal{C}} := \sum_{g \in \mathcal{C}} g \in$* Cent$(C[G])$.

Corollary 5.35. *Suppose F is a splitting field for a finite group G. The following numbers are equal (denoted as t):*

(1) The number of conjugacy classes of G;

(2) The number of inequivalent irreducible representations of G;

(3) The number of simple components of $F[G]$;

(4) $\dim_F$Cent$(F[G])$.

Example 5.36. Let us determine t for $G = S_n$. Since two permutations are conjugate if they can be written as products of disjoint cycles of the same respective lengths. Thus, S_3 has three conjugacy classes, $(1), (12), (123)$. Hence, S_3 has precisely three inequivalent irreducible representations, two of which are degree 1 and the third (of degree 2) given in Example 5.9(2). Likewise, S_4 has five conjugacy classes, represented by $(1), (12), (123)$, $(1234), (12)(34)$, so S_4 has five inequivalent irreducible representations. In general, The structure of $\mathbb{Q}[S_n]$ was determined independently by Young and Frobenius, who showed in particular that $\mathbb{Q}$ is a splitting field of S_n for all n.

6 Characters of Finite Groups

In this chapter we introduce group characters, the key notion in group representations. Various structural tools, such as bilinear forms and tensor products, enhance their role. Group characters have a wide range of applications, including Burnside's celebrated theorem that every group of order $p^i q^j$ (p, q prime) is solvable.

Assume throughout that G is a group, $F \subseteq C$ is a splitting field for G, and $\rho: G \to \mathrm{GL}(n, F)$ is a representation.

Definition 6.1. (character) *The character afforded by the representation ρ is the function $\chi_\rho: G \to F$ given by*

$$\chi_\rho(g) = \mathrm{tr}(\rho(g));$$

by definition, $\deg\chi_\rho = \deg\rho$.

Remark 6.2. (1) $\chi_\rho(1) = \mathrm{tr}(I) = n = \deg\rho$.

(2) $\chi_\rho(a\, g\, a^{-1}) = \mathrm{tr}(\rho(a\, g\, a^{-1})) = \chi_\rho(g)$ for all $g \in G$. Thus, χ_ρ depends only on the conjugacy class of g, and likewise, $\chi_\rho = \chi_{\rho'}$ for any equivalent representations ρ and ρ'.

(3) Taking the sum of characters as functions, we have $\chi_\rho + \chi_\tau = \chi_{\rho\oplus\tau}$ for all representations ρ and τ. Thus the sum of characters is a character. We write m_χ for $\chi + \cdots + \chi$, taken m times.

(4) Any character χ extends a linear transformation $\hat{\chi}: F[G] \to F$ given by $\hat{\chi}(\sum \alpha_g g) = \sum \alpha_g \chi(g)$.

Each character actually is afforded by an equivalence class of representations. Fortunately, Corollary 6.6 below shows that inequivalent representations always afford distinct characters.

Example 6.3. (1) The unit character χ_1, the character of the unit representation 1, satisfies $\chi_1(g) = 1$ for all $g \in G$.

(2) More generally, if $\deg\rho = 1$, then $\chi_\rho = \rho(g)$.

(3) Suppose $\chi = \chi_{\rho_{reg}}$. Then $\chi(g) = 0$ unless $g = 1$, in which case $\chi(1) = \mathrm{tr}(I) = \deg\rho_{reg} = |G|$. It follows that $\hat{\chi}(\sum \alpha_g g) = |G|\,\alpha_1$.

We also need some basic arithmetic properties of characters.

Proposition 6.4. *(1) If the element $g \in G$ has order m, then $\chi_\rho(g)$ is a sum of m-roots of unity and thus is integral over $\mathbb{Z}$.*

(2) $|\chi_\rho(g)| \leq \deg\rho$, equality holding iff $\rho(g)$ is a scalar matrix.

(3) $\chi_\rho(g) = \deg\rho$ iff $g \in \ker\rho$

(4) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

(5) If g is conjugate to g^{-1}, then $\chi_\rho(g)$ is real.

(6) If $g^2 = 1$, then $\chi_\rho(g)$ is an integer of the same parity as $\deg(\rho)$.

One could verify all properties above.

6.1 Schur's orthogonality relations

The character χ_ρ is called irreducible if the representation ρ is irreducible. Fixing a set $\rho_1 = 1, \rho_2, \ldots, \rho_t$ of inequivalent irreducible representations of G of respective degrees n_i, we write χ_i for χ_{ρ_i}. These are all the irreducible characters of G. Since any linear representation is a finite direct sum of irreducible representations, any character χ is a finite sum $u_1\chi_1 + \cdots + u_t\chi_t$ of irreducible characters for suitable $u_1, \ldots, u_t \in \mathbb{N}$, where u_j is called the multiplicity of χ_j in χ.

Recall that t is also the number of conjugacy classes of our given finite group G. We write R for $F^{(t)}$, viewed as an F-algebra where addition and multiplication are taken componentwise. Writing the conjugacy classes of G as $\mathcal{C}_1, \ldots, \mathcal{C}_t$, we define a **class function** to be a function $\{\mathcal{C}_1, \ldots, \mathcal{C}_t\} \to F$. The set of class functions is identified with R, by sending componentwise.

We want a base of R that reflects the structure of G, any character is a class function and thus belongs to R. The natural candidate for our base is $\{\chi_1, \ldots, \chi_t\}$.

Theorem 6.5. *The characters $\chi_1, \ldots, \chi_t$ comprise an orthonormal base of R with respect to the Hermitian inner product $\langle , \rangle$ given by*

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{1 \leq k \leq t} |\mathcal{C}_k| \, \phi(\mathcal{C}_k) \overline{\psi(\mathcal{C}_k)}.$$

In particular, the characters $\chi_1, \ldots, \chi_t$ are distinct.

Hence, t is also the number of distinct irreducible characters of G. We call this inner product the *Schur inner product*. Viewing a class function ϕ as a function $\phi: G \to F$ for which $\phi(a) = \phi(b)$ whenever a, b belong to the same conjugacy class, one could rewrite the formula as

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{1 \leq k \leq t} \sum_{g \in \mathcal{C}_k} \phi(g) \overline{\psi(g)} = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}$$

Saying $\chi_1, \ldots, \chi_t$ is an orthonormal base thus means:

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

Corollary 6.6. *(1) Writing an arbitrary class function ϕ as $\sum_{i=1}^{t} u_i \chi_i$ for suitable $u_i \in F$, we have $u_i = \langle \phi, \chi_i \rangle$. Thus, a class function is a character if the multiplicity $\langle \phi, \chi_i \rangle \in \mathbb{N}$, for each $1 \leq i \leq t$.*

(2) Two inequivalent irreducible representations cannot afford the same character.

(3) If $\chi = \sum_{i=1}^{t} u_i \chi_i$, for $u_i \in \mathbb{N}$, then $\langle \chi, \chi \rangle = \sum u_i^2 \in \mathbb{N}$. Conversely, $\langle \chi, \chi \rangle = 1$ iff $\chi = \chi_i$ for some i; i.e., iff the character χ is irreducible.

Example 6.7. Recall that $n_i = \deg \rho_i = \chi_i(1)$. If $\chi = \chi_{reg}$, then $\langle \chi, \chi_i \rangle = \frac{|G| \, n_i}{|G|} = n_i$ by Example 6.3(3), so

$$\chi = \sum n_i \chi_i.$$

For example, for S_3, we have three representations, namely $\rho_1 = 1, \rho_2 = \text{sgn}, \rho_3$ with $\chi_1(123) = 1 = \chi_2(123)$ and $\chi_3(123) = -1$. Hence, the regular character $\chi(123) = 1 + 1 + 2\,(-1) = 0$ which is true. From this vantage point, the regular representation yields all the character theory of G.

6.2 The character table

Let $n_i = \deg \rho_i = \chi_i(1)$, also $\mathcal{C}_1, \ldots, \mathcal{C}_k$ denote the conjugacy classes of G, and put $m_j = |\mathcal{C}_j|$. We pick a conjugacy representative g_j from $\mathcal{C}_j$ for each j, taking $g_1 = 1$. Recall some group theory, the centralizer of g in G is denoted by $C(g)$, then $m_j = \frac{|G|}{|C(g_j)|}$. In particular, each m_j divides $|G|$.

Definition 6.8. *The character table is $t \times t$ matrix $X = (\chi_{ij})$, where $\chi_{ij} = \chi_i(g_j)$.*

Thus, rows correspond to the irreducible characters $\chi_1 = 1, \ldots, \chi_t$, and columns correspond to the conjugacy representatives. First note that $\chi_{1j} = \chi_1(g_i) = 1$ for all j, and $\chi_{i1} = \chi_i(1) = n_i$ for all j. Hence, we have first column and row immediately.

Remark 6.9. Let us interpret Proposition 6.4 as information about the character table: (1) **If order$(g_j) = m$, then χ_{ij} is a sum of m-th roots of 1, and thus is integral over $\mathbb{Z}$. ** (2) $|\chi_{ij}| \leq n_i$, equality holding iff $\rho_i(g_j)$ is a scalar matrix. (3) $\chi_{ij} = n_i$ iff $g_j \in \ker \rho_i$. (4) The column corresponding to the class of g is the complex conjugate of the column corresponding to the class of g^{-1}, and is in $\mathbb{Z}$ if $g^2 = 1$.

Example 6.10. (1) Suppose $G = C_n$. There are n conjugacy class, so there are n irreducible characters, each of degree 1, determined in Lemma 5.3.

(2) The Klein group $G = \{1, a, b, a\,b\}$. Again, there are four irreducible characters, all of degree 1. There are also four possibilities for choosing χ_{i2} and χ_{i3} from ± 1.

(3) $G = S_3$, thus $t = 3$, with $n_1 = n_2 = 1, n_3 = 2$. We can easily determine the first two row since S_n has 2 specific representations of degree 1, namely 1 and sgn. The last row could be filled by the property of regular representation.

(4) If $\mathbb{Q}$ is a splitting field for G, then the entries of the character table of G are all in $\mathbb{Z}$.

(5) For any n, the entries of the complex character table of Sn are all in $\mathbb{Z}$, since $\mathbb{Q}$ is a splitting field.

6.2.1 Schur's orthogonality relations applied to the character table

Remark 6.11. (Schur I) Theorem 6.5 also can be viewed as a weighted orthogonality relationship between any two rows of character table:

$$\delta_{ik}|G| = \sum_{j=1}^{t} m_j \chi_{ij} \bar{\chi}_{kj}.$$

In matrix algebra, if $A\,B = \alpha\, I$, then $B = \alpha\, A^{-1}$, hence $B\,A = \alpha\, I$. This basic observation enables us to switch from rows to columns and prove another relation.

Remark 6.12. (Schur II)

$$\delta_{jk}|G| = m_k \sum_{i=1}^{t} \chi_{ij} \bar{\chi}_{ik}.$$