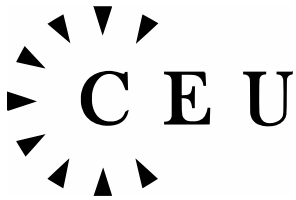
Topics in Algebra

Dorottya Sziráki
Gergő Nemes
Mohamed Khaled



Preface

These notes are based on the lectures of the course titled "Topics in Algebra", which were given by Mátyás Domokos in the fall trimester of 2012 as part of Central European University's mathematics Ph.D. program. The aim of these notes is to present the material of this course in a clear and easily understandable manner, and to help students in the preparation for the exam. We welcome any comments, suggestions and corrections.

Dorottya Sziráki, Gergő Nemes & Mohamed Khaled

Contents

Chapter 1

Noncommutative rings

Throughout this chapter, a ring will always mean a ring with unity. By an R-module, we always mean a left R-module unless otherwise stated.

The most important example of a noncommutative ring is the following. Let V be a vector space over a field K. Put

$$R = \mathrm{End}_K(V) \stackrel{\mathrm{def}}{=} \{\varphi \mid \varphi \text{ is a } K\text{-linear map from } V \text{ to } V\}.$$

Then R is a noncommutative ring, and V is naturally an R-module: for all $r \in R$ and $v \in V$, let $r \cdot v \stackrel{\mathrm{def}}{=} r(v)$.

Other examples are the subrings of a noncommutative ring. If M is an R-module, then M is also an S-module for any subring S of R.

If M is an abelian group (i.e., a $\mathbb{Z}$-module), then $R = \mathrm{End}_{\mathbb{Z}}(M)$ is a noncommutative ring, and M is naturally an R-module.

1.1 Primitive and prime rings

Definition 1.1.1. *The ring R is said to be **simple** if $\{0\}$ and R are the only two-sided ideals in R, i.e., R has no non-trivial two-sided ideals.*

Definition 1.1.2. *An R-module M is said to be **irreducible** (or **simple**) if $\{0\}$ and M are the only submodules of M. An R-module M is **faithful** if the action of each $R \ni r \neq 0$ on M is nontrivial (i.e., $rm \neq 0$ for some $m \in M$). Equivalently, the annihilator of M is the zero ideal (see Definition 1.1.5 below).*

Definition 1.1.3. *The ring R is **primitive** if there exists an irreducible, faithful R-module.*

Remark. *There exists a ring which is left-primitive but not right-primitive.*

Definition 1.1.4. *The ring R is said to be* ***prime*** *if for all ideals $A, B \lhd R$, $A \cdot B = \{0\}$ implies $A = \{0\}$ or $B = \{0\}$.*

Remark. *A commutative ring is prime if and only if it is a domain, i.e., it has no zero-divisors.*

Clearly, a simple ring is always prime.

Definition 1.1.5. *Let M be an R-module. The set*

$$\operatorname{ann}_R(M) \stackrel{\text{def}}{=} \{r \in R \mid rm = 0 \text{ for all } m \in M\}$$

is called the ***annihilator*** *of the module. It is not hard to show that the annihilator of an R-module is a two-sided ideal in R. Similarly let*

$$\operatorname{ann}_R(m) \stackrel{\text{def}}{=} \{r \in R \mid rm = 0\}, \quad m \in M.$$

Then $\operatorname{ann}_R(m)$ is a left ideal in R and

$$\operatorname{ann}_R(M) = \bigcap_{m \in M} \operatorname{ann}_R(m).$$

Proposition 1.1.1. *A ring R is primitive if and only if there exists a maximal left ideal I in R which contains no non-zero two-sided ideals.*

Proof. $\boxed{\Leftarrow}$ Consider the R-module R/I. This is irreducible (simple) because I was maximal. We show that it is a faithful module. We have

$$R \rhd \operatorname{ann}_R(R/I) = \bigcap_{s \in R/I} \operatorname{ann}_R(s) \subseteq \operatorname{ann}_R(1 + I) = I.$$

By assumption, I contains no non-zero two-sided ideals, hence $\operatorname{ann}_R(R/I) = \{0\}$. Thus, R/I is faithful. We showed an irreducible, faithful R-module (namely R/I), therefore R is primitive.

$\boxed{\Rightarrow}$ Take a faithful, irreducible R-module M. Let $0 \neq x \in M$. Since M is irreducible, we have that $Rx = M$. By the Homomorphism Theorem,

$$M = Rx \cong R/\operatorname{ann}_R(x), \quad (\text{take } r \stackrel{\varphi}{\mapsto} rx).$$

Hence, $\mathrm{ann}_R(x)$ is a maximal left ideal in R (since M was irreducible). Suppose that $J \lhd R$ and $J \subseteq \mathrm{ann}_R(x)$. If we show that $J = \{0\}$, then we are done. For an arbitrary $m \in M$, there exists an $r \in R$ such that $m = rx$; (this is because $Rx = M$). Therefore, $Jm = Jrx = (Jr)x = Jx = \{0\}$. However, M is faithful, whence $J = \{0\}$. ■

Corollary 1.1.2. *A simple ring is always primitive.*

Proof. It can be shown that a ring R with unity always has a maximal left ideal (this is Krull's Theorem). If R is simple, there are no non-zero two-sided ideals of R, except for R. The statement now follows from the previous proposition. ■

Corollary 1.1.3. *A commutative ring is primitive if and only if it is a field.*

Proof. By the previous proposition, we have that a commutative ring R is primitive if and only if there exists a maximal two-sided ideal I in R which contains no non-zero two-sided ideals. Since I contains itself, the latter is equivalent to the statement that $\{0\}$ is the only maximal two-sided ideal in R. This is further equivalent to the statement that R is a field. ■

Example 1.1.1 (A ring which is primitive but not simple.)**.** *Let V be an infinite dimensional vector space over a field K. Put $R = \mathrm{End}_K(V)$. We claim that V is a faithful, irreducible R-module. This follows from the well-known fact that given any pair of $v, w \in V$, $v \neq 0$, there is a $\varphi \in \mathrm{End}_K(V)$ such that $\varphi(v) = w$. Thus, $Rv = V$ for any $0 \neq v \in V$. By definition, R is primitive. However, R is not simple as; the following is a non-trivial ideal of R:*

$$I = \{r \in R \mid \dim_K(\mathrm{Im}(r)) < \infty\}.$$

We know that a commutative ring is prime if and only if it is a domain. Comparing this with Corollary 1.1.3, we see that primeness does not imply primitivity. Nevertheless, we have the following proposition.

Proposition 1.1.4. *If a ring is primitive then it is prime.*

Proof. Let R be a primitive ring and let M be a faithful, irreducible R-module. Take $A, B \lhd R$ such that $A \neq 0, B \neq 0$. Take $0 \neq b \in B$. Since M is faithful, there

exists an x in M such that $bx \neq 0$. Then $\{0\} \neq Rbx \leq M$. Since M is irreducible, $Rbx = M$. For any $0 \neq a \in A$, we have $aRbx = aM \neq \{0\}$, whence $aRb \neq \{0\}$. This implies that $A \cdot B \neq \{0\}$. ■

Definition 1.1.6. *Let $\{R_\lambda \mid \lambda \in \Lambda\}$ be a family of rings. We say that the ring R is a **subdirect product** of this family, if there is an injective ring homomorphism*

$$\eta : R \hookrightarrow \prod_{\lambda \in \Lambda} R_\lambda,$$

such that $\pi_\lambda \circ \eta : R \twoheadrightarrow R_\lambda$ is surjective for all $\lambda \in \Lambda$. Here, π_λ is the projection $\pi_\lambda : \prod_{\mu \in \Lambda} R_\mu \twoheadrightarrow R_\lambda$.

Definition 1.1.7. *A ring R is **semisimple** if R is a subdirect product of simple rings. A ring R is **semiprimitive** if R is a subdirect product of primitive rings. A ring R is **semiprime** if R is a subdirect product of prime rings.*

Remark. *A ring R is semiprimitive if and only if for any $0 \neq r \in R$ there exists a faithful irreducible R-module which is not annihilated by r.*

Definition 1.1.8. *Let R be a ring. A two-sided ideal $I \lhd R$ is **maximal** if R/I is simple. A two-sided ideal $I \lhd R$ is **primitive** if R/I is primitive. A two-sided ideal $I \lhd R$ is **prime** if R/I is prime.*

Proposition 1.1.5. *Let R be a ring. The set of all primitive ideals in R is equal to the set of annihilator ideals of irreducible R-modules.*

Proof. $\boxed{\supseteq}$ Let S be an irreducible R-module and let $P = \operatorname{ann}_R(S)$. Then S is an irreducible, faithful R/P-module. Indeed, let $(r+P)s \stackrel{\text{def}}{=} rs$ for all $r \in R$ and $s \in S$. Since S is irreducible R-module, we have that $(r+P)S = rS = S$ for $r \notin P$. Thus, the ideal P of R is, by definition, primitive.

$\boxed{\subseteq}$ Suppose that P is a primitive two-sided ideal in R. Then, by definition, there exists an irreducible, faithful R/P-module M. Then M is also an irreducible R-module with $P = \operatorname{ann}_R(M)$. Indeed, let $rm \stackrel{\text{def}}{=} (r+P)m$ for all $r \in R$ and $m \in M$. If $r \in R$, then

$$rM = (r+P)M = \begin{cases} 0 & \text{if } r \in P, \\ M & \text{if } r \notin P. \end{cases}$$

■

Lemma 1.1.6. *A two-sided ideal P of R is prime if and only if for every $A, B \lhd R$, $A \cdot B \subseteq P$ implies that $A \subseteq P$ or $B \subseteq P$.*

Proof. By definition $P \lhd R$ is prime if and only if R/P is prime. This is equivalent to the statement that for every $\overline{A}, \overline{B} \lhd R/P$, $\overline{A} \cdot \overline{B} = \{0\}$ implies $\overline{A} = \{0\}$ or $\overline{B} = \{0\}$. This is equivalent to the statement that for every $A, B \lhd R$, $A \cdot B \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$. ■

Lemma 1.1.7. *A ring R is semiprime if and only if $\bigcap_{P \lhd R \atop P \text{ is prime}} P = \{0\}$. A ring R is semiprimitive if and only if $\bigcap_{I \lhd R \atop I \text{ is primitive}} I = \{0\}$. A ring R is semisimple if and only if $\bigcap_{L \lhd R \atop L \text{ is maximal}} L = \{0\}$.*

Proof. The three statements are proven almost the same way, so we only prove the first statement. $\boxed{\Rightarrow}$ Suppose that

$$\eta : R \hookrightarrow \prod_{\lambda \in \Lambda} R_\lambda,$$

where R_λ is prime. By the Homomorphism Theorem

$$R_\lambda \cong R/\mathrm{Ker}\,(\pi_\lambda \circ \eta)$$

where π_λ is the projection $\pi_\lambda : \prod_{\mu \in \Lambda} R_\mu \twoheadrightarrow R_\lambda$. Since R_λ is prime, by definition, $\mathrm{Ker}\,(\pi_\lambda \circ \eta) \lhd R$ is a prime ideal. By the definition of a direct product, $R \ni r = 0$ if and only if for all $\lambda \in \Lambda$, $(\pi_\lambda \circ \eta)(r) = 0$. Hence,

$$\bigcap_{\lambda \in \Lambda} \mathrm{Ker}\,(\pi_\lambda \circ \eta) = \{0\}\,.$$

Since the members of this intersection are prime ideals of R, it contains the intersection of all prime ideals of R. Thus, $\bigcap_{P \lhd R \atop P \text{ is prime}} P = \{0\}$.

$\boxed{\Leftarrow}$ Assume that $\bigcap_{P \lhd R \atop P \text{ is prime}} P = \{0\}$. We have

$$\eta : R \hookrightarrow \prod_{P \lhd R \atop P \text{ is prime}} R/P,$$

with $r \overset{\eta}{\mapsto} (r + P)_{P \lhd R \atop P \text{ is prime}}$. By definition, R/P is prime for all prime ideals P of R. Thus, R is the direct product of prime ideals. To complete the proof, we need to show that $\pi_P \circ \eta : R \to R/P$ is a surjection for all prime ideals P of R. Naturally it is, since $r \overset{\eta}{\mapsto} (r + P)_{P \lhd R \atop P \text{ is prime}} \overset{\pi_P}{\mapsto} r + P$. ■

Proposition 1.1.8. *A ring R is semiprime if and only if there is no $\{0\} \neq I \lhd R$ two-sided ideal such that $I \cdot I = I^2 = \{0\}$.*

Proof. $\boxed{\Rightarrow}$ Suppose that $I \lhd R$ such that $I^2 = \{0\}$. Then, by Lemma 1.1.6, $I \subseteq P$ for any prime ideal in R, that is

$$I \subseteq \bigcap_{\substack{P \lhd R \\ P \text{ is prime}}} P.$$

By Lemma 1.1.7, this intersection is $\{0\}$. Hence, $I = \{0\}$.

$\boxed{\Leftarrow}$ Let b_0 be any non-zero element of R. We should show that there exists a prime ideal in R that does not contain b_0. By assumption $(Rb_0R)^2 \neq \{0\}$, i.e., there is a non-zero $b_1 = b_0x_0b_0$ for some $x_0 \in R$. Similarly, there is a non-zero $b_2 = b_1x_1b_1$ for some $x_1 \in R$. In this way, we obtain a sequence of non-zero elements of R: $b_0, b_1, b_2, \ldots$. From the construction, it follows that there are $x, y \in R$ such that $b_j = b_ix = yb_i$ for any $i < j$.

Let S be the family of ideals that are disjoint from the set $\{b_0, b_1, b_2, \ldots\}$. The S is not empty, since $\{0\} \in S$. It can be verified that the conditions of Zorn's Lemma are satisfied for S. Therefore there is a maximal element M in S.

We claim that M is a prime ideal. Indeed, assume in the contrary that for some ideals A, B, we have $M \subsetneq A$ and $M \subsetneq B$, but $AB \subseteq M$. By the maximality of M we have $b_i \in A$ and $b_j \in B$ for some i, j. Take any $k > i, j$. By the construction, we have that for some $z \in R$, $b_k = b_izb_j \in AB \subseteq M$. This is a contradiction, since M is disjoint from the set $\{b_0, b_1, b_2, \ldots\}$. ■

1.2 The Jacobson radical

Definition 1.2.1. *The **Jacobson radical** (or simply the **radical**) of a ring R is*

$$\begin{aligned} \operatorname{rad}(R) &\overset{\text{def}}{=} \{r \in R \mid r \in \operatorname{ann}_R(M) \text{ for all irreducible } R\text{-module } M\} \\ &= \bigcap_{\substack{M \text{ is an irreducible} \\ R\text{-module}}} \operatorname{ann}_R(M). \end{aligned}$$

Remark. *Note that the **radical of a module** M is*

$$\operatorname{rad}(M) \overset{\text{def}}{=} \bigcap_{\substack{N \leq M \\ N \text{ is maximal}}} N.$$

Because of the following proposition, this definition is a generalization of the concept of the radical of a ring.

Proposition 1.2.1. *For a ring R it holds that*

$$\operatorname{rad}(R) = \bigcap_{\substack{I \lhd R \\ I \text{ is primitive}}} I = \bigcap_{\substack{L \lhd R \\ L \text{ is a maximal} \\ \text{left ideal}}} L.$$

Proof. The first equality follows from Proposition 1.1.5. For the second equality we use

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

We shall prove that the set of maximal left ideals in R and the set of annihilators of non-zero elements in irreducible R-modules are equal. Indeed, let L be a maximal left R-module. Then, R/L is an irreducible R-module. It is clear that the annihilator $\operatorname{ann}_R(1+L)$ of the element $1+L \in R/L$ is L. Conversely, start with $0 \neq x \in M$, where M is an irreducible R-module. By the irreducibility and the Homomorphism Theorem

$$M = Rx \cong R/\operatorname{ann}_R(x),$$

hence, $R/\operatorname{ann}_R(x)$ is an irreducible R-module. Consequently, $\operatorname{ann}_R(x)$ is a maximal left ideal in R. ■

Corollary 1.2.2. *A ring R is semiprimitive if and only if* $\operatorname{rad}(R) = \{0\}$.

Proof. By Lemma 1.1.7, a ring R is semiprimitive if and only if

$$\bigcap_{\substack{I \lhd R \\ I \text{ is primitive}}} I = \{0\}.$$

By the previous proposition, this intersection is the radical of R. ■

Proposition 1.2.3. *Let R be a ring. We have the following:*

(i) $R/\operatorname{rad}(R)$ *is semiprimitive;*

(ii) if $I \lhd R$ *and* R/I *is semiprimitive then* $\operatorname{rad}(R) \subseteq I$.

Proof. $\boxed{(i)}$ Use the previous corollary and the fact that

$$\operatorname{rad}(R/\operatorname{rad}(R)) = \operatorname{rad}(R)/\operatorname{rad}(R) = \{0\}.$$

$\boxed{(ii)}$ An irreducible R/I-module can be viewed as an irreducible R-module which is annihilated by I. So if R/I is semiprimitive, then for all $a \in R \setminus I$ there exist an irreducible R/I module M that is not annihilated by $a + I$. This follows from the previous corollary and the definition of the radical. Thus, M – when it is viewed as an R-module – is not annihilated by a, so $a \notin \operatorname{rad}(R)$. Hence, $R \setminus I \subseteq R \setminus \operatorname{rad}(R)$, or $\operatorname{rad}(R) \subseteq I$. ■

Definition 1.2.2. *Let R be a ring. An element $r \in R$ is said to be* ***left quasi-regular*** *if $1 - r$ has a left inverse in R, i.e., $R(1 - r) = R$. A* ***left ideal is left quasi-regular*** *if all its elements are left quasi-regular.*

Suppose that r is left quasi-regular, so there exists an $r' \in R$ such that $(1 - r')(1 - r) = 1$ or $r'r - r' - r = 0$.

Notation. *Let a, b be arbitrary elements of a ring R. Define the operation $\circ : R \times R \to R$ by $a \circ b = a + b - ab$. Specially, $0 \circ a = a \circ 0 = a$.*

It is easy to check that $(R, \circ, 0)$ is an associative monoid.

Lemma 1.2.4. *If I is a left quasi-regular left ideal of R, then I is a subgroup of $(R, \circ, 0)$.*

Proof. Take $r \in I$. Since is left quasi-regular, there exists an element $r' \in R$ such that $0 = r' \circ r$. This is equivalent to $r' = r'r - r$. Both terms on the right-hand side are from I, thus $r' \in I$. By applying this argument for r' we have that there exists an element $r'' \in I$ such that $0 = r'' \circ r'$. It follows that

$$0 = r'' \circ r' = (r'' \circ 0) \circ r' = (r'' \circ (r' \circ r)) \circ r' = ((r'' \circ r') \circ r) \circ r' = (0 \circ r) \circ r' = r \circ r',$$

whence $r' \circ r = r \circ r' = 0$. ■

Theorem 1.2.5. *The elements of the radical of a ring R are left quasi-regular, and* $\operatorname{rad}(R)$ *contains all left quasi-regular left ideals. Consequently,*

$$\operatorname{rad}(R) = \{r \in R \mid sr \text{ is left quasi-regular for all } s \in R\}.$$

Proof. Take any $r \in \operatorname{rad}(R)$. Suppose for a contradiction that $R(1-r) \neq R$, i.e., r is not left quasi-regular. There exists a maximal left ideal L in R among the left ideals that contain $R(1-r)$. In particular, $1-r \in L$. On the other hand, $L \supseteq \operatorname{rad}(R) \ni r$, thus $1 = 1-r+r \in L$. This is a contradiction. Thus, all elements of $\operatorname{rad}(R)$ are left quasi-regular.

Suppose for a contradiction that J is a left quasi-regular left ideal, which is not contained in $\operatorname{rad}(R)$. There exists a maximal left ideal L in R among the left ideals that not contain J. Since $L \subsetneq J + L \triangleleft R$, using the fact that L is a maximal left ideal, $J + L = R$. It follows that there exist elements $j \in J$ and $\ell \in L$ such that $j+\ell = 1$, that is, $\ell = 1-j$. The element $1-j$, with j being in the left quasi-regular left ideal J, has a left inverse, thus $L \supseteq R\ell = R$. This is a contradiction. Hence, $\operatorname{rad}(R)$ contains all left quasi-regular left ideals. ■

Remark. *A nilpotent element is always left (and right) quasi-regular. Indeed, suppose that $a^n = 0$, then*

$$(1-a)\left(1+a+a^2+\cdots+a^n\right) = 1-a^n = 1,$$

$$\left(1+a+a^2+\cdots+a^n\right)(1-a) = 1-a^n = 1.$$

Corollary 1.2.6. *If J is a left ideal in R consisting of nilpotent elements, then $J \subseteq \operatorname{rad}(R)$.*

1.3 Completely reducible modules

Definition 1.3.1. *Let R be a ring. An R-module M is **completely reducible** if for any submodule $M' \leq M$, there exists a submodule $M'' \leq M$ such that $M' \oplus M''$. (i.e., $M' + M'' = M$ and $M' \cap M'' = \{0\}$)*

For example, an irreducible module is completely reducible, since the only submodules are $\{0\}$ and the module itself.

Proposition 1.3.1. *A submodule and a factor module of a completely reducible module is again completely reducible.*

Proof. Let M be a completely reducible module. Let $M' \leq M$, and $M'' \leq M$ be its direct complement. We have

$$M' \cong M/M''.$$

Hence, it is sufficient to prove the statement for factor modules. Let $N \leq M$ be a submodule of the completely reducible module M. Let $\eta : M \twoheadrightarrow M/N$ be the natural surjection ($m \mapsto m+N$). Let P be a submodule of M/N. By assumption, there exists a $Q \leq M$ such that $M = \eta^{-1}(P) \oplus Q$. Then $M/N = P \oplus \eta(Q)$. Indeed, let $m + N \in M/N$. Since $M = \eta^{-1}(P) \oplus Q$, we can write $m = p + q$, where $p \in \eta^{-1}(P)$ and $q \in Q$. Thus, $m + N = \eta(m) = \eta(p) + \eta(q) \in P + \eta(Q)$. Therefore, $P + \eta(Q) = M/N$. It remains to prove that $P \cap \eta(Q) = \{0 + N\}$. Suppose that $a \in P \cap \eta(Q)$. Then $a = m + N = \eta(m)$, for some $m \in M$. More precisely $m \in \eta^{-1}(P) \cap (Q + N) \subseteq \eta^{-1}(P)$. Then m is in the direct complement of N, thus $a = \eta(m) = 0 + N$. ■

Proposition 1.3.2. *A completely reducible module has a non-zero irreducible submodule.*

Proof. Let M be a completely reducible module. Take $0 \neq x \in M$. Consider the family F of those submodules of M that do not contain x. The F is not empty, since the submodule $\{0\}$ does not contain x. Clearly, $(F, \subseteq)$ is a partially ordered set, and by Zorn's Lemma, there exists a maximal member N of this family. By definition, any submodule $P \supsetneq N$ contains x. Hence, any non-zero submodule of M/N contains $0 \neq x + N \in M/N$. By the previous proposition, M/N is completely reducible. On the other hand, any two non-zero submodule of M/N have a nontrivial intersection ($x + N$ is in the intersection). Thus, M/N is irreducible. Consequently N is a maximal submodule of M, and the direct complement Q of N is an irreducible submodule of M. Indeed, $Q \cong M/N$, which is irreducible. ■

Definition 1.3.2. *A set $\{M_\alpha\}_{\alpha \in \mathcal{A}}$ of submodules of a module M is **independent**, if for all $\beta \in \mathcal{A}$*

$$M_\beta \cap \sum_{\substack{\alpha \in \mathcal{A} \\ \alpha \neq \beta}} M_\alpha = \{0\}\,.$$

Remark. *A set of submodules is independent if and only if any finite subset of those submodules is independent.*

Lemma 1.3.3. *If $\{M_\alpha\}_{\alpha \in \mathcal{A}}$ is an independent set of submodules of the module M, and N is a submodule of M such that*

$$N \cap \sum_{\alpha \in \mathcal{A}} M_\alpha = \{0\}\,,$$

then $\{M_\alpha\}_{\alpha\in\mathcal{A}} \cup \{N\}$ *is independent.*

Proof. Assume the contrary that there exist $\alpha_1, \ldots, \alpha_k \in \mathcal{A}$ such that

$$M_{\alpha_1} \cap N + \sum_{i=2}^{k} M_{\alpha_i} \neq \{0\},$$

i.e., there exist $x_i \in M_{\alpha_i}$ $(i = 1, 2, \ldots, k)$ and $y \in N$ such that

$$0 \neq x_1 = y + x_2 + \cdots + x_k.$$

Since $\{M_{\alpha_i}\}_{i=1}^{k}$ is independent, we have $y \neq 0$. Thus,

$$0 \neq y = x_1 - x_2 - \cdots - x_k \in N \cap \sum_{\alpha\in\mathcal{A}} M_\alpha,$$

which is a contradiction. ∎

Proposition 1.3.4. *The following are equivalent for a module* M*:*

(i) M *is generated by its irreducible submodules;*

(ii) $M = \bigoplus_{\alpha\in\mathcal{A}} M_\alpha$ *with* M_α *being an irreducible submodule of* M*;*

(iii) M *is completely reducible.*

Proof. $\boxed{(i) \Rightarrow (ii)}$ Suppose that $M = \sum_{\alpha\in\mathcal{A}} M_\alpha$ with M_α being an irreducible submodule of M. By Zorn's Lemma, there is a $\mathcal{B} \subseteq \mathcal{A}$ which is maximal with the property that $\{M_\beta\}_{\beta\in\mathcal{B}}$ is independent. By the definition of the independence,

$$N \stackrel{\text{def}}{=} \sum_{\beta\in\mathcal{B}} M_\beta = \bigoplus_{\beta\in\mathcal{B}} M_\beta.$$

We need to show that $N = M$. It is sufficient to show that $M_\alpha \subseteq N$ for all $\alpha \in \mathcal{A} \setminus \mathcal{B}$. Assume the contrary that there exists an $\alpha \in \mathcal{A} \setminus \mathcal{B}$ such that $M_\alpha \not\subseteq N$. By the irreducibility of M_α, $M_\alpha \cap N = \{0\}$. Thus, by the previous lemma, $\{M_\beta\}_{\beta\in\mathcal{B}} \cup \{M_\alpha\}$ is independent. This contradicts the maximum property of $\mathcal{B}$.

$\boxed{(ii) \Rightarrow (iii)}$ Take a submodule P of $M = \bigoplus_{\alpha\in\mathcal{A}} M_\alpha$. By Zorn's Lemma, there is a $\mathcal{B} \subseteq \mathcal{A}$ which is maximal with the property that $\{P\} \cup \{M_\beta\}_{\beta\in\mathcal{B}}$ is independent. Put

$$N \stackrel{\text{def}}{=} P \oplus \left(\sum_{\beta\in\mathcal{B}} M_\beta \right).$$

We need to show that $N = M$. We can prove this very similarly to the way we did in the previous part.

$\boxed{(iii) \Rightarrow (i)}$ Suppose that M is completely reducible. Let N be the submodule of M generated by all irreducible submodules of M. Assume the contrary that $N \subsetneq M$. By the completely reducibility of M, there exists a $\{0\} \neq Q \leq M$ such that $M = N \oplus Q$, with Q being completely reducible by Proposition 1.3.1. By Proposition 1.3.2, Q has an irreducible submodule $\{0\} \neq S$. By the definition of N, $S \subseteq N$. This is a contradiction, since $Q \cap N = \{0\}$. ■

1.4 The Density Theorem

Definition 1.4.1. *Given a ring R, denote by R^{op}, and call the **opposite ring** of R, the ring which has the same underlying set and additive group as R and a multiplication $\cdot_{\mathrm{op}}$ defined as*

$$a \cdot_{\mathrm{op}} b = b \cdot a.$$

Here $\cdot$ denotes the multiplication in R.

A left R-module M can always be viewed as a right module over R^{op}, by simply defining $m \cdot r$ to be rm. This is a well defined right module. Indeed, we have

$$m \cdot (r \cdot_{\mathrm{op}} s) = (r \cdot_{\mathrm{op}} s)m = (sr)m = s(rm) = (rm) \cdot s = (m \cdot r) \cdot s.$$

Given a left R-module ${}_RM$, $S = \mathrm{End}({}_RM)$ is a ring. The M is naturally a left S-module by $s \cdot m = s(m)$. The action of R on M commutes with the action of S on M:

$$r \cdot (s \cdot m) = r \cdot (s(m)) = r \cdot s(m) = s(rm) = s \cdot (rm), \text{ for all } r \in R,\ s \in S.$$

We can view M as a right S^{op}-module similarly to that above. Then, M has a left and a right structure, that commute. This observation leads to the following definition.

Definition 1.4.2. *Given two rings A, B and an abelian group M, we say that M is an A-B **bimodule**, if*

(i) M is a left A-module;

(ii) M is a right B-module;

(iii) for all $a \in A$, $b \in B$ and $m \in M$: $(am)b = a(mb)$.

In the latter case, we write amb.

For example, any R-module M is an R-S^{op} bimodule, where $S = \mathrm{End}({}_RM)$.

Lemma 1.4.1 (Schur)**.** *A non-zero homomorphism between irreducible R-modules is an isomorphism.*

Proof. Let M and N be irreducible R-modules, and $\varphi : M \to N$ be a non-zero R-module homomorphism. We have $\mathrm{Ker}(\varphi) \leq M$ and $\mathrm{Im}(\varphi) \leq N$. Since φ is non-zero, $M \neq \mathrm{Ker}(\varphi)$. Consequently, by the irreducibility of M, $\mathrm{Ker}(\varphi) = \{0\}$. Similarly, $\mathrm{Im}(\varphi) = N$. ■

Corollary 1.4.2. *For any irreducible R-module M, $\mathrm{End}({}_RM)$ is a division ring (skew field).*

Proof. Apply Schur's Lemma with N equals M. It follows that every non-zero element of $\mathrm{End}({}_RM)$ is an isomorphism, that is, has an inverse. Thus, $\mathrm{End}({}_RM)$ is a division ring. ■

Let D be a division ring. A D-module is called *vector space* over D. Given a vector space V over a division ring D, we consider $\mathrm{End}({}_DV)$.

Definition 1.4.3. *A subset S of $\mathrm{End}({}_DV)$ is called **dense** if given any finite set $x_1, x_2, \ldots, x_n$ of linearly independent elements in V and any $y_1, y_2, \ldots, y_n$ in V, there exists an $s \in S$ such that $s(x_i) = y_i$ for all $1 \leq i \leq n$.*

Remark. *If $\dim({}_DV)$ is finite, then the only dense subset of $\mathrm{End}({}_DV)$ is $\mathrm{End}({}_DV)$.*

Theorem 1.4.3 (Jacobson–Chevalley Density Theorem)**.** *A ring is primitive if and only if it is isomorphic to a dense subring of linear transformations of a vector space over a division ring.*

Proof. $\boxed{\Leftarrow}$ Suppose that R is a dense subring of $\mathrm{End}({}_DV)$ where D is a division ring. We claim that ${}_RV$ is a faithful and irreducible R-module. It is faithful, since R is a subring of $\mathrm{End}({}_DV)$. The density of R implies $Rx = V$ for all $x \neq 0$, which means that ${}_RV$ is irreducible.

$\boxed{\Rightarrow}$ Suppose that R is primitive. Let V be a faithful and irreducible R-module. By Schur's Lemma, $\mathrm{End}({}_RV)$ is a division ring. Therefore $D \stackrel{\text{def}}{=} \mathrm{End}({}_RV)^{\mathrm{op}}$ is a division ring. Thus, we can consider ${}_RV_D$ as an R-D bimodule. We remark that since ${}_RV$ is faithful, $R \hookrightarrow \mathrm{End}_R(V_D)$. Take some $n \in \mathbb{N}$, then

$$({}_RV_D)^n \stackrel{\text{def}}{=} V^n \stackrel{\text{def}}{=} \underbrace{V \oplus V \oplus \cdots \oplus V}_{n \text{ times}}$$

is, again, an R-D bimodule. Consider the rings

$$R' \stackrel{\text{def}}{=} \mathrm{End}_R\left(V^n\right) \text{ and } R'' \stackrel{\text{def}}{=} \mathrm{End}_{R'}\left(V^n\right).$$

We shall prove that if W is an R-submodule of V^n, then W is an R''-submodule of V^n. Since V is irreducible, by definition, V^n is completely reducible. Let $\widetilde{W}$ be the direct complement of W. Let us denote by π the projection $V^n \twoheadrightarrow W$ with $\mathrm{Ker}(\pi) = \widetilde{W}$. Clearly, $\pi \in \mathrm{End}_R\left(V^n\right) = R'$. Hence, for any $x \in R''$, $w \in W$: $x(w) = x(\pi(w)) = \pi(x(w)) \in W$. This proves that W is an R''-submodule. Consider the map

$$\eta : \mathrm{End}_R(V_D) \hookrightarrow \mathrm{End}_{R'}(V_D^n)$$

defined by

$$a \mapsto (\tilde{a} : (v_1, v_2, \ldots, v_n) \mapsto (av_1, av_2, \ldots, av_n))$$

We show that $\tilde{a} \in \mathrm{End}_{R'}(V_D^n)$ indeed. Let $\xi_i : V_D \hookrightarrow V_D^n$ defined by $v \mapsto (0, 0, \ldots, \underset{\substack{\uparrow \\ i\text{th space}}}{v}, \ldots, 0)$ for $i = 1, 2, \ldots, n$. Also, let $\pi_j : V_D^n \to V_D$ given by

$$(v_1, v_2, \ldots, v_n) \mapsto v_j$$

for $j = 1, 2, \ldots, n$. For every $x \in R' = \mathrm{End}_R\left(V^n\right)$ set $x_{ij} \stackrel{\text{def}}{=} \pi_j \circ x \circ \xi_i \in \mathrm{End}_R({}_RV) = D^{\mathrm{op}}$. Clearly

$$x \underbrace{(v_1, v_2, \ldots, v_n)}_{V_D^n} = (v_1, v_2, \ldots, v_n) \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} \stackrel{\text{def}}{=} (v_1, v_2, \ldots, v_n)X.$$

Then we have $x(\tilde{a}(v_1, v_2, \ldots, v_n)) = x(av_1, av_2, \ldots, av_n) = (av_1, av_2, \ldots, av_n)X = = \tilde{a}((v_1, v_2, \ldots, v_n)X) = \tilde{a}(x(v_1, v_2, \ldots, v_n))$.

Now, our aim is to show that R is dense in $\mathrm{End}_R(V_D)$. Take any finite linearly independent $x_1, x_2, \ldots, x_n \in D$ and $y_1, y_2, \ldots, y_n \in D$. It is well known that there exists an $a \in \mathrm{End}_R(V_D)$ such that $ax_i = y_i$ for all $i = 1, 2, \ldots, n$. Thus,

$$(y_1, y_2, \ldots, y_n) = (ax_1, ax_2, \ldots, ax_n) = \tilde{a}\,(x_1, x_2, \ldots, x_n) \in R''\,(x_1, x_2, \ldots, x_n)\,.$$

But we showed earlier that the latter one is equal to $R(x_1, x_2, \ldots, x_n)$. Therefore, there is an $r \in R$ such that $(y_1, y_2, \ldots, y_n) = r(x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n)$. This proves that R is dense in $\mathrm{End}_R(V_D)$. ■

1.5 Wedderburn–Artin Theorems

Definition 1.5.1. *An R-module M is said to be **artinian** if the descending chain condition (hereinafter d.c.c.) holds for the submodules of M. (i.e., there is no infinite strictly decreasing chain $M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \cdots$ of submodules of M) Equivalently, any non-empty set of submodules of M contains a minimal element.*

Definition 1.5.2. *A ring R is artinian if ${}_RR$ is artinian.*

Definition 1.5.3. *Let F be a field. By an **associative F-algebra** we mean a ring R, which is also an F-vector space such that the vector space addition is the ring addition and for all $\lambda \in F$, $a, b, \in R$ we have $\lambda(ab) = (\lambda a)b = a(\lambda b)$. Equivalently, $1_R \in F \subset \mathcal{Z}(R)$, where*

$$\mathcal{Z}(R) \stackrel{\text{def}}{=} \{r \in R \mid rs = sr \text{ for all } s \in R\}$$

is the centre of R.

Example 1.5.1. *A finite dimensional module over a finite dimensional algebra is artinian. Indeed, submodules are subspaces as well, thus the d.c.c. clearly holds.*

Example 1.5.2. *The ring $\mathbb{Z} \oplus \mathbb{Q}$ is not a $\mathbb{Q}$ algebra, because the identity element of $\mathbb{Q}$ is not the identity element of the ring although $\mathbb{Q}$ is contained in the centre.*

Lemma 1.5.1. *Suppose that $M = M_1 \oplus M_2 \oplus \cdots \oplus M_p$ where $M_1, M_2, \ldots, M_p$ are irreducible R-modules. Then*

(i) the irreducible summands together with their multiplicities are uniquely determined by M;

(ii) for any sub- or factormodule N of M, there exists a subset $J \subseteq \{1, 2, \ldots, p\}$ such that

$$N \cong \bigoplus_{j \in J} M_j.$$

Moreover, if N is a proper submodule or factormodule of M, then $J \subsetneq \{1, 2, \ldots, p\}$.

Proof. $\boxed{(i)}$ Suppose that $M_1 \oplus M_2 \oplus \cdots \oplus M_p = \bigoplus_{\lambda\in\Lambda} N_\lambda$, with N_λ's being irreducible R-modules. By Proposition 1.3.4, M is completely reducible. Let I be the maximal subset of Λ such that $M_1 \cap \sum_{\lambda\in I} N_\lambda = \{0\}$. Then

$$M = M_1 \oplus \bigoplus_{\lambda\in I} N_\lambda.$$

Since

$$M_1 \cong M/\bigoplus_{\lambda\in I} N_\lambda \cong \bigoplus_{\lambda\in\Lambda\setminus I} N_\lambda,$$

by the irreducibility of M_1, $|\Lambda \setminus I| = 1$. Therefore, $\Lambda \setminus I = \{\nu_1\}$, say. Thus, $M_1 \cong N_{\nu_1}$. It follows that

$$M_2 \oplus M_3 \oplus \cdots \oplus M_p \cong M/M_1 \cong \bigoplus_{\lambda\in\Lambda\setminus\{\nu_1\}} N_\lambda.$$

Since p is finite, so inductively we can show that for every $i \in \{1, 2, \ldots, n\}$ there is a $\nu_i \in \Lambda$ such that $M_i \cong N_{\nu_i}$ and $|\Lambda| = p$, indeed for the last step

$$M_p \cong \bigoplus_{\lambda\in\Lambda\setminus\{\nu_i\}_{i=1}^{p-1}} N_\lambda.$$

Since M_p is irreducible we must have $\left|\Lambda \setminus \{\nu_i\}_{i=1}^{p-1}\right| = 1$.

$\boxed{(ii)}$ Since any sub- or factormodule N of M is completely reducible by Proposition 1.3.1, according to Proposition 1.3.4, N can be written as a direct sum of irreducible modules. By the same argument of (i) the desired result follows. ■

Corollary 1.5.2. *A finite direct sum of irreducible R-modules is artinian.*

Proof. By (ii) of Lemma 1.5.1, there is no infinite strictly decreasing chain of submodules, because there is only finitely many of them. ■

Theorem 1.5.3 (First Wedderburn–Artin Theorem)**.** *The following are equivalent for a ring R:*

(i) R is simple artinian;

(ii) R is primitive artinian;

(iii) $R \cong M_n(D)$ for some division ring D and $n \in \mathbb{N}$.

Remark. *The statements of the theorem are also equivalent to (iv) R is prime artinian. We will prove this later, using the Second Wedderburn–Artin Theorem.*

Proof. $\boxed{(i) \Rightarrow (ii)}$ It is true in general, that a simple ring is always primitive.

$\boxed{(ii) \Rightarrow (i)}$ If R is primitive artinian then R is prime artinian. This is (iv). Later we will prove that (iv) implies (i).

$\boxed{(ii) \Rightarrow (iii)}$ Suppose that R is primitive artinian. By the Jacobson–Chevalley Density Theorem, R is a dense subring of $\mathrm{End}(V_D)$ for some division ring D and right D-vector space V. We shall show that V is finite dimensional. Suppose, to the contrary, that V is an infinite dimensional D-vector space. Take an infinite set $\{x_1, x_2, \ldots\} \subseteq V$ of linearly independent elements. Let $L_j = \mathrm{ann}_R(\{x_1, x_2, \ldots, x_j\}) \lhd_{\text{left}} R$ for $j = 1, 2, \ldots$. Since R is dense, for every j we have an $r_j \in R$ such that $r_j(x_1) = r_j(x_2) = \cdots = r_j(x_{j-1}) = 0$, but $r_j(x_j) = v \neq 0$. Thus, $r_j \in L_{j-1} \setminus L_j$, that is

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

is an infinite strictly decreasing chain of left ideals in R. This is a contradiction, since R is artinian. Thus, $\dim(V_D) = n < \infty$. Consequently, the only dense subring of $\mathrm{End}(V_D)$ is $\mathrm{End}(V_D)$. Hence, $R = \mathrm{End}(V_D) \cong M_n(D)$. The latter is by choosing a basis in V_D, and observing that $V_D \cong D^n$.

$\boxed{(iii) \Rightarrow (ii)}$ First, we show that $M_n(D)$ is simple (consequently primitive). Let $\mathcal{I}$ be a two-sided ideal in $M_n(D)$. Suppose that $\mathcal{I} \neq \{0\}$. Then, there is an $A \in \mathcal{I}$ such that $a_{ij} \neq 0$ for some $i, j \in \{1, 2, \ldots, n\}$. Let $E_{ij}(b) \in M_n(D)$ be the matrix that has 0's everywhere except $D \ni b \neq 0$ in entry (i, j). Let c be the left inverse of a_{ij}, then

$$\sum_{k=1}^{n} E_{ki}(c)\, A E_{jk}(1) = \sum_{k=1}^{n} E_{kk}(1) = I \in M_n(D),$$

which is in $\mathcal{I}$, since it is a two-sided ideal. Therefore $\mathcal{I} = M_n(D)$. Let us denote by L_i the set of those matrices in $M_n(D)$ whose every column is the zero vector in D^n except the ith column $(i = 1, 2, \ldots, n)$. It is straightforward to show that

L_i is a left ideal in $M_n(D)$. Then $L_i \cong D^n$ as left $M_n(D)$-modules. Since D^n is an irreducible $M_n(D)$-module, we have that

$$M_n(D) = \bigoplus_{i=1}^{n} L_i$$

is the direct sum of irreducible $M_n(D)$-modules. By Corollary 1.5.2 we conclude that $M_n(D)$ is artinian. ■

Theorem 1.5.4. *The radical of an artinian ring is nilpotent, i.e., for any artinian ring R there exists an $n \in \mathbb{N}$ such that* $(\mathrm{rad}(R))^n = \{0\}$.

Proof. Let R be an artinian ring. Consider the following descending chain of ideals:

$$\mathrm{rad}(R) \supseteq (\mathrm{rad}(R))^2 \supseteq (\mathrm{rad}(R))^3 \supseteq \cdots .$$

Since R is artinian, there is a $k \in \mathbb{N}$ such that

$$(\mathrm{rad}(R))^k = (\mathrm{rad}(R))^{k+1} = (\mathrm{rad}(R))^{k+2} = \cdots \stackrel{\mathrm{def}}{=} P.$$

We shall show that $P = \{0\}$. Assume, to the contrary, that $P \neq \{0\}$. We know that $P = P^2$. Consider the set

$$\{L \mid L \lhd_{\mathrm{left}} R, L \subseteq P, PL \neq \{0\}\} \ni P.$$

By the equivalent definition of an artinian ring, there is a minimal element I of this set. Hence, $PI \neq \{0\}$ which implies that there is a $b \in I$ such that $Pb \neq \{0\}$. Clearly, $Pb \lhd_{\mathrm{left}} R$, $Pb \subseteq I \subseteq P$ and $P(Pb) = P^2 b = Pb \neq \{0\}$. Therefore, Pb is in the above set, and by the minimality of I, we must have $Pb = I$. Consequently, there is an $x \in P$ such that $xb = b$ or $(1-x)b = 0$. Since $x \in P \subseteq \mathrm{rad}(R)$, $1-x$ has a left inverse, thus $b = 0$. This contradicts the assumption that $Pb \neq \{0\}$. ■

Proposition 1.5.5. *If an artinian R-module M is the subdirect product of irreducible R-modules, then M is the direct sum of finitely many irreducible R-modules.*

Proof. The definition of M being a subdirect product of irreducible R-modules means that $\bigcap_{N \text{ is maximal}}^{N \lneq M} N = \{0\}$ (Why?).

Let S be the family of submodules which are the intersection of finitely many maximal submodules. By the artinian property, there is a minimal element in

S, say L with $L = N_1 \cap N_2 \cap \ldots \cap N_k$ for some k ($N_i \lneq M$ being maximal for $i = 1, 2, \ldots, k$). By the definition of S, $L \cap N \in S$ for all maximal submodule N of M. Using the minimality property of L, we have that $L \cap N = L$, therefore $L \leq N$ for all maximal submodule N of M. Thus, $L \subset \bigcap_{\substack{N \lneq M \\ N \text{ is maximal}}} N = \{0\}$. Hence, $N_1 \cap N_2 \cap \ldots \cap N_k = \{0\}$. In this way

$$M \hookrightarrow \bigoplus_{i=1}^{k} \underbrace{M/N_i}_{\text{irreducible}} .$$

By Lemma 1.5.1, M can be written as $\bigoplus_{j \in J \subseteq \{1,2,\ldots,k\}} M/N_j$. ∎

Corollary 1.5.6. *If R is a semisimple ring and the d.c.c. holds for two-sided ideals, then*

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_k$$

is the ring theoretic direct sum of finitely many simple rings: $R_i \triangleleft R$, R_i is a simple ring ($i = 1, 2, , \ldots, k$).

Proof. Let $M(R)$ be the subring of $\mathrm{End}_{\mathbb{Z}}(R)$ generated by the elements of the sets $\{x \mapsto ax \mid a \in R\}$ and $\{x \mapsto xa \mid a \in R\}$. Then R is an $M(R)$-module, and the ideals in R are the same as $M(R)$-submodules in R. We can apply the previous proposition with $R \overset{\text{def}}{=} M(R)$ and $M \overset{\text{def}}{=} R$. ∎

Theorem 1.5.7 (Second Wedderburn–Artin Theorem)**.** *The following are equivalent for a ring R:*

(i) R is semisimple artinian;

(ii) R is semiprimitive artinian;

(iii) R is semiprime artinian;

(iv) $R \cong \bigoplus_{i=1}^{q} M_{n_i}(D_i)$, where $D_1, \ldots, D_q$ are division rings and $n_1, \ldots, n_q \in \mathbb{N}$;

(v) ${}_R R$ is completely reducible;

(vi) all R-modules are completely reducible.

Proof. $\boxed{(i) \Rightarrow (ii)}$ It is true in general, that a semisimple ring is always semiprimitive.

$\boxed{(ii) \Rightarrow (i)}$ Suppose that R is semiprimitive artinian. By definition, a semiprimitive ring is the subdirect product of primitive rings. Since the homomorphic image of an artinian ring is artinian, we conclude that R is the subdirect product of primitive artinian rings. By the First Wedderburn–Artin Theorem, this is a equivalent to the statement that R is the subdirect product of simple artinian rings, hence R is semisimple (and artinian).

$\boxed{(ii) \Rightarrow (iii)}$ It is true in general, that a semiprimitive ring is always semiprime.

$\boxed{(iii) \Rightarrow (ii)}$ By Theorem 1.5.4, $\operatorname{rad}(R)$ is nilpotent. Since R is semiprime, by Proposition 1.1.8, R has no non-zero nilpotent ideals. Thus, $\operatorname{rad}(R) = \{0\}$. Therefore, by Corollary 1.2.2, R is semiprimitive (and artinian).

$\boxed{(i) \Rightarrow (iv)}$ Using Corollary 1.5.6 and the fact that a homomorphic image of an artinian ring is artinian, we conclude that R is the finite direct sum of simple artinian rings. We can now apply the First Wedderburn–Artin Theorem for the summands.

$\boxed{(iv) \Rightarrow (v)}$ In the proof of the First Wedderburn–Artin Theorem, we saw that

$$M_{n_i}(D_i) \cong \underbrace{D_i^{n_i} \oplus D_i^{n_i} \oplus \cdots \oplus D_i^{n_i}}_{n_i \text{ times}},$$

when we view the $D_i^{n_i}$'s as $M_{n_i}(D_i)$-modules. By the natural surjection $R \twoheadrightarrow M_{n_i}(D_i)$, they are isomorphic as R-modules as well. Moreover each $D_i^{n_i}$ is an irreducible R-module. Hence, ${}_RR$ is the finite direct sum of irreducible R-modules, which means by Proposition 1.3.4 that ${}_RR$ is completely reducible.

$\boxed{(v) \Rightarrow (ii)}$ An irreducible submodule of ${}_RR$ is a minimal left ideal of the ring R. Thus, if ${}_RR$ is completely reducible, we have by Proposition 1.3.4 that

$${}_RR = \bigoplus_{\lambda \in \Lambda} M_\lambda,$$

where each M_λ is a minimal left ideal in R. The set Λ is in fact finite. Indeed by the definition of the direct sum, $1 = e_{\lambda_1} + e_{\lambda_2} + \cdots + e_{\lambda_k}$ with $\lambda_i \in \Lambda$, $i = 1, 2, \ldots, k$. Therefore, for any $r \in R$, $r = r \cdot 1 = re_{\lambda_1} + re_{\lambda_2} + \cdots + re_{\lambda_k}$. Hence,

$${}_RR = M_1 \oplus M_2 \oplus \cdots \oplus M_k,$$

where $M_i = Re_{\lambda_i}$ for $i = 1, 2, \ldots, k$. Since each M_i is an irreducible R module, by Corollary 1.5.2, ${}_RR$ is artinian. It remains to show that it is semiprimitive. We have

$$\operatorname{rad}(R) = \bigcap_{\substack{L \text{ is an irreducible} \\ R\text{-module}}} \operatorname{ann}_R(L) \subseteq \bigcap_{i=1}^{k} \operatorname{ann}_R(e_{\lambda_i}) \subseteq \operatorname{ann}_R(1) = \{0\}.$$

Therefore, by Corollary 1.2.2, R is semiprimitive.

$\boxed{(v) \Rightarrow (vi)}$ Let M be any R-module. We have

$$M = \sum_{0 \neq x \in M} Rx.$$

Define, for all $0 \neq x \in M$, $\varphi_x : R \to Rx$ by $r \mapsto rx$. In this way, Rx is a homomorphic image of a completely reducible module, hence it is a completely reducible module. By Proposition 1.3.4, Rx is generated by its simple submodules, and hence M is generated by its simple submodules. Using Proposition 1.3.4 again, M is a completely reducible R-module.

$\boxed{(vi) \Rightarrow (v)}$ This implication is a logical triviality. ∎

Theorem 1.5.8 (Uniqueness in the Second Wedderburn–Artin Theorem)**.** *Let q, s be positive integers. We have*

$$\bigoplus_{i=1}^{q} M_{n_i}(D_i) = \bigoplus_{i=1}^{s} M_{k_i}(\Delta_i)$$

if and only if $q = s$ and after a possible reordering $n_1 = k_1, n_2 = k_2, \ldots, n_q = k_q$ and $D_1 \cong \Delta_1, D_2 \cong \Delta_2, \ldots, D_q \cong \Delta_q$.

Proof. Let $R \overset{\text{def}}{=} \bigoplus_{i=1}^{q} M_{n_i}(D_i)$. We claim that q is the number of isomorphism classes of irreducible R-modules. Indeed, let $S_i \overset{\text{def}}{=} D_i^{n_i}$ as an $M_{n_i}(D_i)$-module $(i = 1, 2, \ldots, q)$. By the natural surjection $R \twoheadrightarrow M_{n_i}(D_i)$ we can view the S_i's as R-modules $(i = 1, 2, \ldots, q)$. The $S_1, S_2, \ldots, S_q$ are irreducible, and $S_i \ncong S_j$ for $i \neq j$, since they have different annihilators:

$$\operatorname{ann}_R(S_i) = \sum_{j \neq i} M_{n_j}(D_j).$$

We have

$$ {}_RR \cong (\underbrace{S_1 \oplus S_1 \oplus \cdots \oplus S_1}_{n_1 \text{ times}}) \oplus \cdots \oplus (\underbrace{S_q \oplus S_q \oplus \cdots \oplus S_q}_{n_q \text{ times}}) $$

as R-modules. By Lemma 1.5.1, any irreducible factormodule of ${}_RR$ is isomorphic to one of the S_i's.

Next, we show that any irreducible R-module is isomorphic to a factormodule of ${}_RR$. Indeed, an irreducible R-module S is cyclic, i.e., $S = Rs$ for some $s \in S$. The map $\varphi : R \twoheadrightarrow S$, $r \mapsto rs$ is an R-module homomorphism. By the Homomorphism Theorem,

$$ S \cong R/\mathrm{Ker}(\varphi). $$

Hence, we proved the claim on q. The n_i's are uniquely determined: n_i is the multiplicity of S_i in the direct decomposition of ${}_RR$.

Finally, we prove that – up to isomorphism – each division ring D_i is uniquely determined, since $D_i \cong \mathrm{End}({}_RS_i)^{\mathrm{op}}$, for all $i = 1, 2, \ldots, q$. Indeed, let i be arbitrary from $\{1, 2, \ldots, q\}$. Define the map $\Phi : D_i \to \mathrm{End}({}_RS_i)^{\mathrm{op}}$ by

$$ d \mapsto (\varphi_d : s \mapsto sd). $$

Clearly, Φ is an injective ring homomorphism and $\varphi_d \in \mathrm{End}({}_RS_i)^{\mathrm{op}}$. We show that Φ is surjective. Let $\varphi \in \mathrm{End}({}_RS_i)^{\mathrm{op}}$ and write $\varphi(e_1) = e_1 d + e_2\mu_2 + \cdots + e_{n_i}\mu_{n_i}$, where $\{e_j\}_{j=1}^{n_i}$ is the standard basis in $D_i^{n_i}$ and $d, \mu_2, \ldots, \mu_{n_i} \in D_i$. Then $\varphi(s) = \varphi([s, 0, \ldots, 0]\, e_1) = [s, 0, \ldots, 0]\, \varphi(e_1) = sd$ for any $s \in S_i$. ∎

Proposition 1.5.9 (Addendum to the First Wedderburn–Artin Theorem)**.** *The following are equivalent for a ring R:*

(i) R is simple artinian;

(iv) R is prime artinian.

Proof. $\boxed{(i) \Rightarrow (iv)}$ It is true in general, that a simple ring is always prime.

$\boxed{(iv) \Rightarrow (i)}$ Suppose that R is prime artinian. Then, naturally, R is semiprime artinian. By the Second Wedderburn–Artin Theorem, R is semisimple. From Corollary 1.5.6 and the fact that the homomorphic image of an artinian ring is artinian, we have that

$$ R \cong \bigoplus_{i=1}^{q} R_i, $$

where $R_i \triangleleft R$, R_i being simple artinian ($i = 1, 2, \ldots, n$). We have $R_i R_j \subseteq R_i \cap R_j = \{0\}$ for $i \neq j$. By the definition of primeness this can happen only if $q = 1$, that is $R \cong R_1$. Thus, R is simple artinian. ■

Chapter 2

Basics of Representation Theory

The notion of a module over a non-commutative ring originates in the area of group representations.

2.1 Group representations

Definition 2.1.1. *Let F be a field, G be a group. By a* ***representation*** *of G on F we mean a group homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is an F-vector space and $\mathrm{GL}(V)$ is the group of all invertible transformations of V.*

Definition 2.1.2. *Given two representations $\rho_i : G \to \mathrm{GL}(V_i)$, $i \in \{1, 2\}$, of G on F, any linear map $T : V_1 \to V_2$ is said to be G-**equivariant** if $\rho_2(g) \circ T = T \circ \rho_1(g)$ for all $g \in G$. Given two representations $\rho_i : G \to \mathrm{GL}(V_i)$, $i \in \{1, 2\}$, of G on F, ρ_1 and ρ_2 are said to be* ***isomorphic*** *if there exist some G-equivariant vector space isomorphism from V_1 onto V_2. A representation $\rho : G \to \mathrm{GL}(V)$ of the group G on the field F is said to be* ***faithful*** *if ρ is injective.*

Definition 2.1.3. *By an* ***action*** *of a group G on a set X we mean a group homomorphism $s : G \to \mathrm{Sym}(X) = \{X \to X \text{ bijections}\}$. Given a group action s, we have the following notation: for any $g \in G$ and $x \in X$, $gx \overset{\text{def}}{=} s(g)x$. In this way, $(gh)x = g(hx)$ and $1x = x$. The actions s_1, s_2 of G on X_1, X_2 are* ***isomorphic*** *if there exists a bijection $T : X_1 \to X_2$ such that $gT(x) = T(gx)$ for all $g \in G$ and $x \in X_1$.*

Definition 2.1.4. *Given a representation $\rho : G \to \mathrm{GL}(V)$, any vector subspace W of V is said to be G-**invariant** (or ρ-invariant) if $\rho(g)(W) \subseteq W$ for all $g \in G$.*

A representation $\rho : G \to \mathrm{GL}(V)$ of G on F is said to be ***irreducible*** *if $\{0\}$ and V are the only invariant subspaces of V. A representation $\rho : G \to \mathrm{GL}(V)$ of G on F is said to be* ***completely reducible*** *if any invariant subspace of V has an invariant direct complement.*

Now let F be a field, G be a group and $\rho : G \to \mathrm{GL}(V)$ be a representation of G on F. Let $W \subseteq V$ be invariant subspace of V. One can define a representation $\rho_W : G \to \mathrm{GL}(W)$ by

$$g \mapsto \rho(g)|_W.$$

The ρ_W is well defined. Indeed, W is an invariant subspace, i.e., $\rho(g)(W) \subseteq W$, hence $\rho(g)|_W \in \mathrm{GL}(W)$. Let $g, h \in G$, then for any $w \in W$ we have

$$\rho_W(g+h)(w) = \rho(g+h)(w) = \rho(g)(w) + \rho(h)(w) = \rho_W(g)(w) + \rho_W(h)(w).$$

Therefore, ρ_W is a group homomorphism and so a representation of G on F. We can also define $\rho_{V/W} : G \to \mathrm{GL}(V/W)$ by

$$\rho_{V/W}(g)(v+W) \stackrel{\text{def}}{=} \rho(g)(v) + W.$$

for all $v \in V$ and all $g \in G$. Let $g \in G$, $\rho_{V/W}(g)$ is linear transformation on V/W since $\rho(g)$ is linear transformation on V. The $\rho_{V/W}(g)$ is injective since W is ρ-invariant subspace, and surjective since $\rho(g)$ is surjective. Then $\rho_{V/W}(g) \in \mathrm{GL}(V/W)$ and $\rho_{V/W}$ is well defined. Let $g, h \in G$ and let $v \in V$, then

$$\begin{aligned}
\rho_{V/W}(g+h)(v) &= \rho(g+h)(v) + W \\
&= (\rho(g)(v) + \rho(h)(v)) + W \\
&= (\rho(g)(v) + W) + (\rho(h)(v) + W) \\
&= \rho_{V/W}(g)(v) + \rho_{V/W}(h)(v) \\
&= (\rho_{V/W}(g) + \rho_{V/W}(h))(v).
\end{aligned}$$

Therefore, $\rho_{V/W}$ is a group homomorphism and so a representation of G on F.

Given two representations $\rho_i : G \to \mathrm{GL}(V_i)$, $i \in \{1, 2\}$ of a group G on a field F, we can define the *sum* of ρ_1 and ρ_2 as follows:

$$(\rho_1 + \rho_2) : G \to \mathrm{GL}(V_1 \oplus V_2)$$

$$(\rho_1 + \rho_2)(g)(v_1 + v_2) \stackrel{\text{def}}{=} \rho_1(g)(v_1) + \rho_2(g)(v_2),$$

for all $g \in G$, $v_1 \in V_1$ and $v_2 \in V_2$. Let $g \in G$, then $(\rho_1 + \rho_2)(g)$ is a well defined transformation on $V_1 \oplus V_2$. Indeed, every element $v \in V_1 \oplus V_2$ has a unique

decomposition $v = v_1 + v_2$ for some $v_1 \in V_1$ and some $v_2 \in V_2$. Also $(\rho_1 + \rho_2)(g)$ is injective. Indeed, $\mathrm{Ker}((\rho_1 + \rho_2)(g)) =$

$$\begin{aligned}
&= \{v \in V_1 \oplus V_2 \mid (\rho_1 + \rho_2)(g)(v) = 0\} \\
&= \{v_1 + v_2 \in V_1 \oplus V_2 \mid v_1 \in V_1, v_2 \in V_2 \text{ and } \rho_1(g)(v_1) + \rho_2(g)(v_2) = 0\} \\
&= \{v_1 + v_2 \in V_1 \oplus V_2 \mid v_1 \in V_1, v_2 \in V_2 \text{ and } \rho_1(g)(v_1) = 0 \text{ and } \rho_2(g)(v_2) = 0\} \\
&= \{v_1 + v_2 \in V_1 \oplus V_2 \mid v_1 \in \mathrm{Ker}(\rho_1(g)) \text{ and } v_2 \in \mathrm{Ker}(\rho_2(g))\} \\
&= \{0\}.
\end{aligned}$$

Let $u \in V_1 \oplus V_2$, then there exist $u_1 \in V_1$ and $u_2 \in V_2$ such that $u = u_1 + u_2$. Since $\rho_1(g)$ and $\rho_2(g)$ are surjective, there exist $v_1 \in V_1$ and $v_2 \in V_2$ such that $\rho_1(g)(v_1) = u_1$ and $\rho_2(g)(v_2) = u_2$. Let $v = v_1 + v_2$, then clearly $(\rho_1 + \rho_2)(g)(v) = u$, i.e., $(\rho_1 + \rho_2)(g)$ is surjective. Hence $(\rho_1 + \rho_2)(g) \in \mathrm{GL}(V_1 \oplus V_2)$.

Now let $g, h \in G$ and let $v \in V_1 \oplus V_2$, then there exist $v_1 \in V_1$ and $v_2 \in V_2$ such that $v = v_1 + v_2$, hence

$$\begin{aligned}
(\rho_1 + \rho_2)(g + h)(v) &= \rho_1(g + h)(v_1) + \rho_2(g + h)(v_2) \\
&= \rho_1(g)(v_1) + \rho_1(h)(v_1) + \rho_2(g)(v_2) + \rho_2(h)(v_2) \\
&= (\rho_1 + \rho_2)(g)(v) + (\rho_1 + \rho_2)(h)(v) \\
&= [(\rho_1 + \rho_2)(g) + (\rho_1 + \rho_2)(h)](v).
\end{aligned}$$

Therefore, $(\rho_1 + \rho_2)$ is a group homomorphism and so is a representation of G on F.

Suppose that $\rho : G \to \mathrm{GL}(V)$ is a representation of G on F, and W_1, W_2 are invariant subspaces of V such that $V = W_1 \oplus W_2$. Then

$$\rho \cong (=)(\rho_{W_1} + \rho_{W_2}) \quad \text{and} \quad \rho_{V/W_1} \cong (=)\rho_{W_2}.$$

Definition 2.1.5. *Let G be a group, and F be a field. The* ***group algebra*** *$F[G]$ – or simply FG – is*

$$FG = \left\{ \sum_{g \in G} a_g g \mid a_g \in F \text{ for all } g \in G \text{ and } |\{g \in G \mid a_g \neq 0\}| \text{ is finite} \right\},$$

with addition and multiplication defined as follows:

$$\left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) \stackrel{\text{def}}{=} \sum_{g \in G} (a_g + b_g) g,$$

$$\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g g\right) \stackrel{\text{def}}{=} \sum_{g\in G}\left(\sum_{kh=g} a_k b_h\right) g.$$

The FG becomes an F-algebra by defining

$$a\cdot\sum_{g\in G} a_g g \stackrel{\text{def}}{=} \sum_{g\in G}(a\cdot a_g)g,$$

for all $a\in F$ and $\sum_{g\in G} a_g g\in FG$.

Remark. *One can think about FG as the set of F-valued functions on G with finite support and with pointwise addition and convolution of functions as the multiplication operator.*

Let G be a group, F be a field. Any representation $\rho: G\to \mathrm{GL}(V)$ can be extended to an F-algebra homomorphism $\tilde{\rho}: FG\to \mathrm{End}_F(V)$ by

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g \rho(g).$$

In this way, V can be viewed as an FG-module, by defining $(\sum_{g\in G} a_g g)\cdot v \stackrel{\text{def}}{=} \tilde{\rho}(\sum_{g\in G} a_g g)(v)$ for all $v\in V$.

Conversely, let V be an FG-module. For all $g\in G$, define $\rho(g): V\to V$ by

$$v\mapsto gv \quad (g\in FG).$$

Clearly, $\rho(g)$ is linear. Also $\mathrm{Ker}\rho(g)=\{v\in V\mid \rho(g)(v)=0\}=\{v\in V\mid gv=0\}=\{0\}$, i.e., $\rho(g)$ is injective. For all $v\in V$, $g^{-1}v\in V$ and $\rho(g)(g^{-1}v)=v$, i.e., $\rho(g)$ is surjective. Hence, $\rho(g)$ is an invertible linear map on V. Now define, $\rho: G\to \mathrm{GL}(V)$ by

$$g\mapsto \rho(g).$$

Let $g,h\in G$, and let $v\in V$. Then

$$\rho(g+h)(v)=(g+h)v=gv+hv=\rho(g)(v)+\rho(h)(v)=(\rho(g)+\rho(h))(v).$$

Thus, $\rho(g+h)=\rho(g)+\rho(h)$, i.e., ρ is a representation of G on F. Moreover, $\tilde{\rho}$ gives the same FG-module structure we started with.

Dictionary.

Group representation	$\leftrightarrows$	*FG-module*
Invariant subspaces	$\leftrightarrows$	*FG-submodules*
Factor representations	$\leftrightarrows$	*Factor FG-modules*
Irreducible representations	$\leftrightarrows$	*Irreducible FG-modules*
Completely reducible representations	$\leftrightarrows$	*Completely reducible FG-modules*
G-equivariant linear map	$\leftrightarrows$	*FG-module homomorphism*

Definition 2.1.6. *An element e in a ring is called an **idempotent** if $e^2 = e$ (projection).*

Lemma 2.1.1. *Let V be a vector space over a field F. Then there is a one-to-one correspondence between the sets*

$$\{\textit{Idempotents in } \mathrm{End}_F(V)\} \quad \textit{and}$$
$$\{\textit{Ordered pairs } (V_1, V_2) \textit{ of subspaces of } V \textit{ such that } V = V_1 \oplus V_2\}.$$

Proof. $\boxed{\subseteq}$ Let $e \in \mathrm{End}_F(V)$ be an idempotent. For any $v \in V$, let $v_1 = e(v)$ and $v_2 = v + (-1)e(v)$. First, $e(v_2) = e(v + (-1)e(v)) = e(v) + (-1)e^2(v) = e(v) + (-1)e(v) = (1 + (-1))e(v) = 0e(v) = 0$, i.e., $v_2 \in \mathrm{Ker}(e)$ and $v_1 \in \mathrm{Im}(e)$. Now, $v_1 + v_2 = e(v) + v + (-1)e(v) = (1 + (-1))e(v) + v = 0 + v = v$. Hence, $V = \mathrm{Ker}(e) + \mathrm{Im}(e)$. Let $v \in \mathrm{Ker}(e) \cap \mathrm{Im}(e)$, then there exists a $u \in V$ such that $v = e(u)$ and $e(v) = 0$. Now $v = e(u) = e(e(u)) = e(v) = 0$, i.e., $\mathrm{Ker}(e) \cap \mathrm{Im}(e) = \{0\}$. Therefore, $V = \mathrm{Ker}(e) \oplus \mathrm{Im}(e)$.

$\boxed{\supseteq}$ Suppose that $V = V_1 \oplus V_2$. Define the map $e : V \to V$ by

$$v_1 + v_2 \mapsto v_1 \qquad (v_i \in V_i).$$

Clearly, $e^2 = e$ and $V = V_1 \oplus V_2 = \mathrm{Im}(e) \oplus \mathrm{Ker}(e)$. ■

Lemma 2.1.2. *Given a representation $\rho : G \to \mathrm{GL}(V)$ and a vector space V with the direct sum decomposition $V = V_1 \oplus V_2$. Then the subspaces V_1 and V_2 are invariant subspaces if and only if the idempotent $e : V \to V$, $v_1 + v_2 \mapsto v_1$ is G-equivariant.*

Proof. $\boxed{\Leftarrow}$ If e is G-equivariant, then $V_1 = \mathrm{Im}(e)$ and $V_2 = \mathrm{Ker}(e)$ are invariant subspaces (since the kernel and the image of a homomorphism of modules are submodules).

$\boxed{\Rightarrow}$ Suppose that $V = V_1 \oplus V_2$, and V_1, V_2 are invariant subspaces. Let $g \in G$, take any $v \in V$. Then there exist $v_1 \in V_1$ and $v_2 \in V_2$ such that $v = v_1 + v_2$. Then

$$\rho(g)(v) = \rho(g)(v_1) + \rho(g)(v_2).$$

But $\rho(g)(v_1) \in V_1$ and $\rho(g)(v_2) \in V_2$ (since V_1 and V_2 are invariant subspaces). Hence,

$$e(\rho(g)(v)) = \rho(g)(v_1) = \rho(g)(e(v))$$

for all $g \in G$ and all $v \in V$, i.e., e is G-equivariant. ■

Corollary 2.1.3. *Given a representation $\rho : G \to \mathrm{GL}(V)$ and an invariant subspace $W \subseteq V$. Then W has an invariant direct complement if and only if there exists a G-equivariant idempotent $e \in \mathrm{End}_F(V)$ with $\mathrm{Im}(e) = W$.*

Remark. *Any $\tau \in \mathrm{End}_F(V)$ is G-equivariant if and only if $\rho(g)\tau\rho(g)^{-1} = \tau$ for all $g \in G$.*

Theorem 2.1.4 (Maschke's Theorem)**.** *Let G be a finite group, F be a field. (Then FG is finite dimensional, hence artinian.) Then FG is semisimple if and only if* $\mathrm{char}(F) \nmid |G|$.

Proof. $\boxed{\Rightarrow}$ Suppose that $\mathrm{char}(F) \mid |G|$. So $\mathrm{char}(F) = p$, for some prime p. Let $c \stackrel{\mathrm{def}}{=} \sum_{g \in G} g \in FG$, then for any $h \in G$:

$$hc = h \sum_{g \in G} g = \sum_{g \in G} hg = \sum_{hg \in G} hg = c.$$

Similarly, $ch = c$. So c is central in FG. Moreover, Fc is an ideal in FG and it is central. But,

$$c^2 = \sum_{h \in G} h \sum_{g \in G} g = \underbrace{c + c + \cdots + c}_{|G|\text{-times}} = 0,$$

since $\mathrm{char}(F) \mid |G|$. Therefore, Fc is a non-zero nilpotent ideal in FG. By Proposition 1.1.8, FG is not semiprime. Thus, it can not be semisimple.

$\boxed{\Leftarrow}$ According to the Second Wedderburn–Artin Theorem, it is enough to show that all FG-modules are completely reducible. Let V be any FG-module (i.e., we are given a representation $\rho : G \to \mathrm{GL}(V)$ of G on V) and let $W \subseteq V$ be an invariant subspace. If we show an invariant direct complement to W, then

by definition, ρ will be completely reducible. Therefore, V will be completely reducible (cf. Dictionary). According to Corollary 2.1.3, we need to show that there exists a G-equivariant idempotent in $\mathrm{End}_F(V)$ whose image is W.

Let π be an arbitrary projection from V onto W. Set

$$e \stackrel{\text{def}}{=} \frac{1}{|G|}\sum_{g\in G}\rho(g)\pi\rho(g)^{-1}.$$

At this point we used the assumption, since we divided by $|G|$. Now from the above corollary it is suffices to prove the following:

(i) **The e is G-equivariant.** Let $h \in G$ then

$$\rho(h)e\rho(h)^{-1} = \frac{1}{|G|}\sum_{g\in G}\rho(h)\rho(g)\pi\rho(g)^{-1}\rho(h)^{-1} = \frac{1}{|G|}\sum_{g\in G}\rho(hg)\pi\rho(hg)^{-1}$$
$$= \frac{1}{|G|}\sum_{k\in G}\rho(k)\pi\rho(k)^{-1} = e.$$

By our previous remark, e is G-equivariant.

(ii) **We have $\mathrm{Im}(e) \subseteq W$.** Let $g \in G$, then $\mathrm{Im}(\pi\rho(g)^{-1}) \subseteq \mathrm{Im}(\pi) \subseteq W$. Thus, $\mathrm{Im}(\rho(g)|_{\mathrm{Im}(\pi\rho(g)^{-1})}) \subseteq W$ since W is invariant. Now

$$\mathrm{Im}(e) \subseteq \sum_{g\in G}\mathrm{Im}(\rho(g)|_{\mathrm{Im}(\pi\rho(g)^{-1})}) \subseteq W.$$

(iii) **We have $e|_W = \mathrm{id}_W$.** From this and (ii) it is clear that $e^2 = e$ and $\mathrm{Im}(e) = W$. Let $w \in W$, then $\rho(g)^{-1}w \in W$ since W is invariant. Then $\pi\rho(g)^{-1}w = \rho(g)^{-1}w$. Hence,

$$e(w) = \frac{1}{|G|}\sum_{g\in G}\rho(g)\pi\rho(g)^{-1}w = \sum_{g\in G}\rho(g)\rho(g)^{-1}w = w\frac{1}{|G|}\sum_{g\in G}1 = w.$$

This completes the proof of Maschke's Theorem. ∎

2.2 Matrix representations

Let $\rho : G \to \mathrm{GL}(V)$ be a finite dimensional representation (i.e., $\dim_F(V) = n$ for some $n \in \mathbb{N}$). Take a basis $e \stackrel{\text{def}}{=} \{e_1, e_2, \ldots, e_n\}$ in V. For any $v \in V$ there exist

$v_1, v_2, \ldots, v_n \in F$, such that $v = v_1e_1 + v_2e_2 + \cdots + v_ne_n$. Define an isomorphism $V \to F^n$ by

$$v \mapsto [v_1, v_2, \ldots, v_n]^\top .$$

Let $\varphi \in \mathrm{End}_F(V)$, then φ has a unique matrix representation, namely $[\varphi]_e$, an $n \times n$ matrix whose ith column is $[\varphi(e_i)]_e$. For all $v \in V$, $[\varphi(v)]_e = [\varphi]_e[v]_e$. Let $f \stackrel{\text{def}}{=} \{f_1, f_2, \ldots, f_n\}$ be another basis of V, let S be the matrix whose ith column is $[f_i]_e$, $i = 1, 2, \ldots, n$, then $[v]_f = S^{-1}[v]_e$ and hence $[\varphi]_f = S^{-1}[\varphi]_e S$. So choosing a basis $e \stackrel{\text{def}}{=} \{e_1, e_2, \ldots, e_n\}$ of V we obtain an identification $V \cong F^n$ and

$$\rho : G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(F) \stackrel{\text{def}}{=} \{A \in F^{n\times n} \mid \det(A) \neq 0\}.$$

Definition 2.2.1. *An n-**dimensional matrix representation** of G is a group homomorphism $\psi : G \to \mathrm{GL}_n(F) = \mathrm{GL}(F^n)$.*

Let $\psi_i : G \to \mathrm{GL}_n(F)$, $i \in \{1, 2\}$ be two matrix representation of G. The corresponding representations of G on F^n are isomorphic if and only if there exists an $S \in \mathrm{GL}_n(F)$ such that $S^{-1}\psi_1(g)S = \psi_2(g)$ for all $g \in G$.

Let $\rho : G \to \mathrm{GL}(V)$ be an n-dimensional representation. Choose a basis $e = \{e_1, e_2, \ldots, e_n\}$ of V, define $\rho_e : G \to \mathrm{GL}_n(F)$, by $\rho_e(g) \stackrel{\text{def}}{=} [\rho(g)]_e$ for all $g \in G$. It is straightforward to prove that ρ_e is an n-dimensional matrix representation.

Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G, and $\dim_F(V) = n$. Let W be an invariant subspace of V, choose a basis $e' = \{e_1, e_2, \ldots, e_k\}$ of W and extend it to a basis of V, $e = \{e_1, e_2, \ldots, e_k, e_{k+1}, \ldots, e_n\}$. Let $e'' = \{e_{k+1} + W, \ldots, e_n + W\}$ be the corresponding basis of V/W. Then

$$[\rho(g)]_e = \begin{bmatrix} [\rho_W(g)]_{e'} & \star \\ 0 & [\rho_{V/W}(g)]_{e''} \end{bmatrix}.$$

Moreover, let $V = W \oplus U$, where W and U are invariant subspaces of V. Choose a basis $e' = \{e_1, e_2, \ldots, e_k\}$ of W and a basis $e'' = \{e_{k+1}, e_{k+2}, \ldots, e_n\}$ of U. Then $e = \{e_1, e_2, \ldots, e_k, e_{k+1}, e_{k+2}, \ldots, e_n\}$ is a basis of V. Then

$$[\rho(g)]_e = \begin{bmatrix} [\rho_W(g)]_{e'} & 0 \\ 0 & [\rho_U(g)]_{e''} \end{bmatrix}.$$

Let $\psi_i : G \to \mathrm{GL}_{n_i}(F)$, $i \in \{1, 2\}$ be two matrix representations of G. Define the map $\psi : G \to \mathrm{GL}_{n_1+n_2}(F)$ by

$$g \mapsto \begin{bmatrix} \psi_1(g) & 0 \\ 0 & \psi_2(g) \end{bmatrix}.$$

Then ψ (as a representation of G on $F^{n_1+n_2}$) is isomorphic to $\psi_1 + \psi_2$.

Lemma 2.2.1 (Schur's Lemma I)**.** *Let $\rho_i : G \to \mathrm{GL}(V_i)$, $i \in \{1, 2\}$ be two irreducible representations of G. Then any G-equivariant linear map $V_1 \to V_2$ is either the zero map or an isomorphism.*

Proof. It is just a formulation of Schur's Lemma (Lemma 1.4.1) in the language of representations. ■

Lemma 2.2.2 (Schur's Lemma II)**.** *Let F be an algebraically closed field and $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation with $\dim_F(V) < \infty$. Then*

$$\{G\text{-equivariant linear transformation of } V\} = \{\lambda \cdot \mathrm{id}_V \mid \lambda \in F\}.$$

Proof. $\boxed{\subseteq}$ Let $T : V \to V$ be an G-equivariant linear transformation of V and let λ be an eigenvalue of T. Define the map $T' : V \to V$, $T' \stackrel{\text{def}}{=} T - \lambda \cdot \mathrm{id}_V$. Then clearly T' is also a G-equivariant linear transformation of V. But $\mathrm{Ker}(T')$ contains all the λ-eigenvectors. Thus, T' is not an isomorphism, hence by Schur's Lemma I we have that T' is the zero map and so $T = \lambda \cdot \mathrm{id}_V$.

$\boxed{\supseteq}$ Any map of the form $\lambda \cdot \mathrm{id}_V$ is a G-equivariant linear transformation of V. ■

Corollary 2.2.3. *Any finite dimensional irreducible representation of an abelian group over an algebraically closed field is one-dimensional.*

Proof. Let G be an abelian group, and let $\rho : G \to \mathrm{GL}(V)$ be a finite dimensional irreducible representation over an algebraically closed field F. Let $g, h \in G$, then $\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g)$. Then for all $g \in G$ we have that $\rho(g) : V \to V$ is a G-equivariant linear transformation of V. By Schur's Lemma II, for all $g \in G$, $\rho(g) = \lambda(g)\mathrm{id}_V$, where $\lambda : G \to F$ (in fact, $\lambda : G \to F^\times$ is a group homomorphism).

Consequently, any subspace of V is an invariant subspace ($\lambda \cdot W = W$, for all $W \subseteq V$). So the irreducibility of V implies that V has no non-trivial subspaces, i.e., $\dim_F(V) = 1$. ■

2.3 Construction of representations

Let s be an action of the group G on a set X, and let F be a field. Then, there is a natural representation of G on the vector space $\mathrm{Fun}(X, F)$ (the space of all $X \to F$ functions) as follows: $\hat{s} : G \to \mathrm{GL}(\mathrm{Fun}(X, F))$, $\hat{s}(g)(f)(x) \stackrel{\text{def}}{=} f(g^{-1}x)$ for all $g \in G$, $f \in \mathrm{Fun}(X, F)$ and $x \in X$.

For example the group G acts on itself by left multiplication: $\ell : G \to \mathrm{Sym}(G)$, $\ell(g)(x) \stackrel{\text{def}}{=} gx$. Similarly, we have an action given by the right multiplication: $r : G \to \mathrm{Sym}(G)$, $r(g)(x) \stackrel{\text{def}}{=} xg^{-1}$. These lead us to the following definitions.

Definition 2.3.1. *The map* Left-Reg $: G \to \mathrm{GL}(\mathrm{Fun}(G, F))$, $(gf)(x) \stackrel{\text{def}}{=} f(g^{-1}x)$ *is called the* ***left regular representation*** *of G. Similarly, the map* Right-Reg $: G \to \mathrm{GL}(\mathrm{Fun}(G, F))$, $(gf)(x) \stackrel{\text{def}}{=} f(xg)$ *is called the* ***right regular representation*** *of the group G.*

In fact, $G \times G$ acts on G, namely we have $G \times G \to \mathrm{Sym}(G)$, $(g, h) \mapsto (x \mapsto gxh^{-1})$. Associated to that is the *two-sided regular representation*: $\mathrm{Reg} : G \times G \to \mathrm{GL}(\mathrm{Fun}(G, F))$, $(g, h)(f)(x) \stackrel{\text{def}}{=} f(g^{-1}xh)$.

Let $\eta_1 : G \hookrightarrow G \times G$, $g \mapsto (g, 1)$, then Left-Reg $=$ Reg $\circ\, \eta_1$. Similarly, let $\eta_2 : G \hookrightarrow G \times G$, $g \mapsto (1, g)$, then Right-Reg $=$ Reg$\circ\eta_2$. Finally, let $\delta : G \hookrightarrow G \times G$, $g \mapsto (g, g)$, then Reg $\circ\, \delta : G \to \mathrm{GL}(\mathrm{Fun}(G, F))$, $(gf)(x) \stackrel{\text{def}}{=} f(g^{-1}xg)$.

Let $\rho : G \to \mathrm{GL}(V)$ be a representation of the group G on ${}_FV$. Let $V^* \stackrel{\text{def}}{=} \{f \mid f : V \to F \text{ linear functional}\}$ be the *dual space* of V. Then, we can define the *dual representation* of ρ by

$$\rho^* : G \to \mathrm{GL}(V^*), \quad (gf)(v) \stackrel{\text{def}}{=} f(g^{-1}v) \text{ for all } f \in V^*.$$

Suppose that V is finite dimensional, $\dim(V) = n < \infty$, say. Let $e = \{e_1, e_2, \ldots, e_n\}$ be a basis of V. Let $e^* = \{e_1^*, e_2^*, \ldots, e_n^*\}$ be the corresponding basis of V^*, i.e.,

$$e_i^*(e_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Then we have

$$[\rho^*(g)]_{e^*} = \left([\rho(g)]_e^\top\right)^{-1}.$$

Remark. *The representations ρ and ρ^* are not isomorphic in general.*

Definition 2.3.2. *Given two F-vector space V and W, their **tensor product** $U = V \otimes W$ is an F-vector space together with a bilinear map $V \times W \xrightarrow{\otimes} U$, $(v, w) \mapsto v \otimes w$ having the following property: For any vector space U' and bilinear map $\beta : V \times W \to U'$ there exists a unique linear map $\nu : U \to U'$ such that $\beta = \nu \circ \otimes$. In other words, the following diagram is commutative:*

$$\begin{array}{ccc} V \times W & \xrightarrow{\otimes} & U \\ {\scriptstyle\beta}\big\downarrow & \swarrow_{\exists!\nu} & \\ U' & & \end{array}$$

Remark. *It can be shown that the tensor product exists and it is unique up to isomorphism.*

Definition 2.3.3. *Let $\rho_i : G_i \to \mathrm{GL}(V_i)$, $i = 1, 2$ be two representations. We define their **tensor product** $\rho_1 \otimes \rho_2 : G_1 \times G_2 \to \mathrm{GL}(V_1 \otimes V_2)$ by $(g_1, g_2)(v_1 \otimes v_2) \stackrel{\text{def}}{=} g_1 v_1 \otimes g_2 v_2$.*

Remark. *For a fixed $(g_1, g_2) \in G_1 \times G_2$, the map $V_1 \times V_2 \to V_1 \otimes V_2$, $(v_1, v_2) \mapsto g_1 v_1 \otimes g_2 v_2$ is bilinear, hence, by the universal property of the tensor product, there exists a unique linear transformation $A : V_1 \otimes V_2 \to V_1 \otimes V_2$ such that $A(v_1 \otimes v_2) = g_1 v_1 \otimes g_2 v_2$. Let $(\rho_1 \otimes \rho_2)(g_1, g_2) \stackrel{\text{def}}{=} A$.*

Definition 2.3.4. *Let $\rho_i : G \to \mathrm{GL}(V_i)$, $i = 1, 2$ be two representations of the group G. We define their **product** $\rho_1 \cdot \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2)$ by $g(v_1 \otimes v_2) \stackrel{\text{def}}{=} g v_1 \otimes g v_2$. In other words, $\rho_1 \cdot \rho_2 = (\rho_1 \otimes \rho_2) \circ \delta$, where $\delta : G \hookrightarrow G \times G$, $g \mapsto (g, g)$.*

Proposition 2.3.1. *Let $\rho_i : G_i \to \mathrm{GL}(V_i)$, $i = 1, 2$ be two finite dimensional irreducible representations over an algebraically closed base field F (e.g., $F = \mathbb{C}$). Then, $\rho_1 \otimes \rho_2$ is an irreducible representation of $G_1 \times G_2$.*

Proof. Let U be a non-zero $G_1 \times G_2$-invariant subspace of $V_1 \otimes V_2$. We need to show that U is the whole space.

Let $\eta_1 : G_1 \hookrightarrow G_1 \times G_2$, $g \mapsto (g, 1)$. Define the representation $\psi \stackrel{\text{def}}{=} (\rho_1 \otimes \rho_2) \circ \eta_1 : G_1 \to \mathrm{GL}(V_1 \otimes V_2)$. We shall show that

$$\psi \cong \underbrace{\rho_1 + \rho_1 + \cdots + \rho_1}_{n \text{ times}},$$

where $n = \dim V_2$. Indeed, take a basis $f_1, f_2, \ldots, f_n$ in V_2, then

$$V_1 \otimes V_2 = \bigoplus_{i=1}^{n} V_1 \otimes f_i.$$

Since for all $g_1 \in G_1$ and $v_1 \in V_1$, $\psi(g_1)(v_1 \otimes f_i) = g_1 v_1 \otimes 1 f_i = g_1 v_1 \otimes f_i \in V_1 \otimes f_i$, we conclude that each $V_1 \otimes f_i$ is a ψ-invariant subspace of $V_1 \otimes V_2$. Moreover, the equivariant isomorphism $S_i : V_1 \otimes f_i \to V_1$, $v_1 \otimes f \mapsto v_1$ shows that $\psi|_{V_1 \otimes f_i} \cong \rho_1$, hence $\psi \cong \rho_1 + \rho_1 + \cdots + \rho_1$. (In general, $\psi|_W$ means $\psi(g)|_W$ for all $g \in G$.)

Let U_0 be a minimal G_1- (or ψ-) invariant subspace in U. Then $\psi|_{U_0} \cong \rho_1$. Indeed, using ψ, $V_1 \otimes V_2 = \bigoplus_{i=1}^{n} V_1 \otimes f_i$ becomes an FG_1-module. By the Dictionary, each $V_1 \otimes f_i$ is an irreducible submodule (since $\psi|_{V_1 \otimes f_i} \cong \rho_1$ is irreducible). Since U_0 is invariant, it is a submodule. By Lemma 1.5.1, U_0 is the direct sum of some $V_1 \otimes f_i$'s. But since U_0 is a minimal ψ-invariant subspace, $\psi|_{U_0}$ must be irreducible, hence U_0 is an irreducible submodule. Therefore there is exactly one i such that $U_0 \cong V_1 \otimes f_i$, i.e., $\psi|_{U_0} \cong \psi|_{V_1 \otimes f_i} \cong \rho_1$. Hence, there is a G_1-equivariant isomorphism $T : U_0 \to V_1$. For any $i \in \{1, 2, \ldots, n\}$, define $T_i : U_0 \to V_1$ by

$$\sum_{i=1}^{n} v_i \otimes f_i \mapsto v_i.$$

Each T_i is a G_1-equivariant linear map, since $T_i \circ (\psi|_{U_0}) = \rho_1 \circ T_i$. Using the algebraic closeness of F, by Schur's Lemma II, there exist non-zero $\lambda_1, \lambda_2, \ldots, \lambda_n$ in F such that $T_i \circ T^{-1} = \lambda_i \cdot \mathrm{id}_{V_1}$, i.e., $T_i = \lambda_i T$. Hence,

$$U_0 \ni \underset{\neq 0}{u} = \sum_{i=1}^{n} T_i(u) \otimes f_i = \sum_{i=1}^{n} \lambda_i T(u) \otimes f_i = \sum_{i=1}^{n} T(u) \otimes \lambda_i f_i = T(u) \otimes \underbrace{\sum_{i=1}^{n} \lambda_i f_i}_{\overset{\text{def}}{=} \underset{\neq 0}{f} \in V_2}$$

$$= T(u) \otimes f \in V_1 \otimes f.$$

Since T is an isomorphism, we have that $U \supseteq U_0 \supseteq \{v \otimes f \mid v \in V_1\}$. Set $W \overset{\text{def}}{=} \{w \in W_2 \mid V_1 \otimes w \subseteq U\} \leq V_2$. The W is not the zero subspace, since $f \in W$. Moreover, W is G_2- (ρ_2-) invariant. Indeed, let $w \in W$, then by definition $V_1 \otimes w \subseteq U$. Since U is $\rho_1 \otimes \rho_2$ invariant, we have $\rho_1(g_1)V_1 \otimes \rho_2(g_2)w \subseteq U$ for all $g_1 \in G_1$ and $g_2 \in G_2$. But $\rho_1(g_1)V_1 = V_1$, therefore $\rho_2(g_2)w \in W$. But ρ_2 is an irreducible representation, whence $W = V_2$. Thus, $U = V_1 \otimes V_2$. ∎

2.4 The space of matrix elements of a representation

Let $\rho : G \to \mathrm{GL}(V)$ be a finite dimensional representation of a group G over the field F. Let $n = \dim V$ and $e = \{e_1, e_2, \ldots, e_n\}$ be a basis of V. Finally, let $\rho_{ij}(g)$ be the (i,j)th entry of $[\rho(g)]_e$.

Definition 2.4.1. *The subspace*

$$M(\rho) \stackrel{\text{def}}{=} \mathrm{span}_F \{\rho_{ij} \mid i,j = 1,2,\ldots,n\} \subset \mathrm{Fun}(G,F)$$

is called ***the space of matrix elements of*** ρ.

Note that although the ρ_{ij}'s depend on the basis e, their span does not: choose an other basis $f = \{f_1, f_2, \ldots, f_n\}$ in V, and let ϑ_{ij} be the (i,j)th entry of $[\rho(g)]_f$. Then there is an $S \in \mathrm{GL}_n(F)$ such that

$$[\vartheta_{ij}(g)]_{n\times n} = S^{-1} [\rho_{ij}(g)]_{n\times n} S.$$

Thus, ϑ_{ij} is an F-linear combination of the $\rho_{k\ell}$'s and vice versa.

Remark. *(i) If $\rho \cong \psi$ then $M(\rho) = M(\psi)$. Indeed, we have $T[\rho(g)]_e = [\psi(g)]_e T$, for all $g \in G$, for some basis e of V, and some $T \in \mathrm{GL}_n(F)$. Then, a similar argument to that above applies.*

(ii) If σ is the sub- or factor representation of ρ, then $M(\sigma) \subseteq M(\rho)$. Indeed, let $e = \{e_1, e_2, \ldots, e_n\}$ be a basis of V, and $\sigma = \rho|_U$ for a subspace U of V. Then

$$[\rho(g)]_e = \begin{bmatrix} [\rho_U(g)]_{e'} & \star \\ 0 & [\rho_{V/U}(g)]_{e''} \end{bmatrix},$$

where e' and e'' are the corresponding bases in U and V/U. So there exists a basis on V such that the matrix elements of σ are among the matrix elements of ρ.

(iii) We have $M(\rho_1 + \rho_2 + \cdots + \rho_k) = M(\rho_1) + M(\rho_2) + \cdots + M(\rho_k)$. Indeed, for an appropriate basis,

$$\{\textit{nonzero matrix elements of } \rho_1 + \rho_2 + \cdots + \rho_k\} = \bigcup_{j=1}^{k} \{\textit{matrix elements of } \rho_j\}.$$

In particular $M(\rho+\rho) = M(\rho) + M(\rho) = M(\rho)$*, using that* $M(\rho)$ *is a subspace. However,* $\rho+\rho \ncong \rho$*. (The dimensions are different.)*

Proposition 2.4.1. *Let* $\rho : G \to \mathrm{GL}(V)$ *be a finite dimensional irreducible representation of a group* G *over an algebraically closed base field* F *(e.g.,* $F = \mathbb{C}$*). The* $M(\rho)$ *is a* Reg*-invariant subspace in* $\mathrm{Fun}(G, F)$*. Moreover,* $\mathrm{Reg}_{M(\rho)} \cong \rho^* \otimes \rho$ *as* $G \times G$ *representations.*

(In particular, by Proposition 2.3.1, $\mathrm{Reg}_{M(\rho)}$ *is an irreducible representation, i.e.,* $M(\rho)$ *is a minimal* $G \times G$*-invariant subspace in* $\mathrm{Fun}(G, F)$*.)*

Proof. Define the map $\varphi : V^* \otimes V \to M(\rho)$ by

$$\xi \otimes v \mapsto (g \mapsto \xi(gv)) \in \mathrm{Fun}(G, F).$$

First, we show that $g \mapsto \xi(gv) \in M(\rho)$. Let $e = \{e_1, e_2, \ldots, e_n\}$ be a basis of V, and $e^* = \{e_1^*, e_2^*, \ldots, e_n^*\}$ be the corresponding basis of V^*. Then we can write $[\xi]_{e^*}^\top$, $[v]_e$ and

$$g \mapsto [\xi]_{e^*}^\top [\rho(g)]_e [v]_e .$$

Thus, $g \mapsto \xi(gv)$ is a linear combination of entries of $[\rho(g)]_e$, i.e., $g \mapsto \xi(gv) \in M(\rho)$. From the definition of the tensor product, φ is a linear map. We show that φ is $G \times G$-equivariant. Since $(h_1, h_2)(\xi \otimes v) = h_1\xi \otimes h_2 v$, we have

$$(h_1, h_2)(\xi \otimes v) \overset{\varphi}{\mapsto} (g \mapsto (h_1\xi)(g(h_2 v))).$$

The left-hand side is

$$(h_1, h_2)(\xi \otimes v) = h_1\xi \otimes h_2 v = (\rho^* \otimes \rho)(h_1, h_2)(\xi \otimes v),$$

whereas the right-hand side is

$$\begin{aligned} g \mapsto (h_1\xi)(g(h_2 v)) = \xi(h_1^{-1}(g(h_2 v))) = \xi((h_1^{-1} g h_2)v) &= \mathrm{Reg}(h_1, h_2)(g \mapsto \xi(gv)) \\ &= \mathrm{Reg}(h_1, h_2)(\varphi(\xi \otimes v)). \end{aligned}$$

Thus

$$\varphi((\rho^* \otimes \rho)(h_1, h_2)(\xi \otimes v)) = \mathrm{Reg}(h_1, h_2)(\varphi(\xi \otimes v)).$$

It remains to show that φ is an isomorphism. Indeed, φ is surjective:

$$\varphi(e_i^* \otimes e_j) = (g \mapsto (0, 0, \ldots, \underset{\substack{\uparrow \\ i\text{th space}}}{1}, \ldots, 0)\, [\rho(g)]_e\, (0, 0, \ldots, \underset{\substack{\uparrow \\ j\text{th space}}}{1}, \ldots, 0)^\top = \rho_{ij}(g)),$$

i.e., the natural basis corresponds to the natural basis. The φ is injective: since $\varphi \neq 0$, $\mathrm{Ker}(\varphi) \subsetneq V^* \otimes V$. But $\mathrm{Ker}(\varphi)$ is a $G \times G$-invariant subspace in $V^* \otimes V$, and by Proposition 2.3.1, $\rho^* \otimes \rho$ is irreducible, hence, $\mathrm{Ker}(\varphi) = \{0\}$. ∎

Corollary 2.4.2. *Suppose that the base field F is algebraically closed.*

(i) We have Right-Reg$|_{M(\rho)} \cong \underbrace{\rho + \rho + \cdots + \rho}_{\dim V \text{ times}}$, *where* Right-Reg *denotes the right regular representation of G. Indeed, define $\eta_2 : G \hookrightarrow G \times G$ by $\eta_2(g) \stackrel{\mathrm{def}}{=} (1, g)$ for all $g \in G$. Then define $\psi \stackrel{\mathrm{def}}{=} (\rho^* \otimes \rho) \circ \eta_2$ and using similar argument as in the proof of Proposition 2.3.1, we find that $\psi \cong \underbrace{\rho + \rho + \cdots + \rho}_{\dim V \text{ times}}$. But, by the previous proposition, $\psi \cong$ Right-Reg$|_{M(\rho)}$.*

(ii) Any irreducible finite dimensional representation of G occurs as a subrepresentation of the right regular representation of G. Indeed (i) holds for all irreducible finite dimensional representation ρ of G.

(iii) We have $\mathrm{Reg}_{M(\rho)} \cong \mathrm{Reg}_{M(\rho')}$ if and only if $\rho \cong \rho'$. Indeed, $\boxed{\Rightarrow}$ From $\mathrm{Reg}_{M(\rho)} \cong \mathrm{Reg}_{M(\rho')}$ we have Right-Reg$_{M(\rho)} \cong$ Right-Reg$_{M(\rho')}$. *Then, by (i), $\rho + \rho + \cdots + \rho \cong \rho' + \rho' + \cdots + \rho'$. From this it can be shown that $\rho \cong \rho'$. $\boxed{\Leftarrow}$ If $\rho \cong \rho'$, then $\rho^* \otimes \rho \cong \rho'^* \otimes \rho'$. Then, by the previous proposition, $\mathrm{Reg}_{M(\rho)} \cong \mathrm{Reg}_{M(\rho')}$.*

Thus, if ρ is an irreducible representation over an algebraically closed base field F, then $G \times G$ acts irreducibly and pairwise non-isomorphically on the space $M(\rho)$. (It is a consequence of (iii) of Corollary 2.4.2.)

Theorem 2.4.3. *Let G be a finite group, and let the base field F to be $\mathbb{C}$ (it would be sufficient to have an algebraically closed base field F, such that* $\mathrm{char}(F) \nmid G$*). Then*

$$\mathrm{Fun}(G, \mathbb{C}) = \bigoplus_{i=1}^{q} M(\rho_i),$$

where $\rho_1, \rho_2, \ldots, \rho_q$ is a complete list of isomorphism classes of irreducible representations of G.

Proof. Since G is finite, $\mathbb{C}G$ is a finite dimensional algebra, hence artinian. Since $\mathrm{char}(\mathbb{C}) \nmid G$, by Maschke's Theorem, $\mathbb{C}G$ is a semisimple ring. Using the Second

Wedderburn–Artin Theorem, we conclude that every $\mathbb{C}G$-module is completely reducible. Thus, the right regular representation is completely reducible. It is also finite dimensional, since $\dim \mathrm{Fun}(G, \mathbb{C}) = |G| < \infty$. So up to isomorphism, it has finitely many subrepresentations. From (ii) of Corollary 2.4.2 it follows that there are only finitely many isomorphism classes of irreducible representations of G.

Since $G \times G$ acts irreducibly and pairwise non-isomorphically on the spaces $M(\rho_1), M(\rho_2), \ldots, M(\rho_q)$, these spaces are linearly independent. Indeed, take, for example, $N \stackrel{\text{def}}{=} M(\rho_1) \cap (M(\rho_2) + M(\rho_3) + \cdots + M(\rho_q))$. Then $N \subseteq M(\rho_1)$ and it is a $G \times G$ invariant subspace. Thus, $N = \{0\}$ or $N = M(\rho_1)$ (since $G \times G$ acts irreducibly on $M(\rho_1)$). If the latter holds then $M(\rho_2) + M(\rho_3) + \cdots + M(\rho_q) \subseteq M(\rho_1)$. Each summand on the left-hand side is a $G \times G$ invariant subspace, hence we must have $M(\rho_1) = M(\rho_2) = M(\rho_3) = \cdots = M(\rho_q)$ using that $G \times G$ acts irreducibly on $M(\rho_1) \neq 0$. Since $G \times G$ acts non-isomorphically on the spaces $M(\rho_1), M(\rho_2), \ldots, M(\rho_q)$, we must have $\rho_1 \cong \rho_2 \cong \cdots \cong \rho_q$, a contradiction. Thus, $N = \{0\}$ as required. Therefore,

$$\sum_{i=1}^{q} M(\rho_i) = \bigoplus_{i=1}^{q} M(\rho_i).$$

All we need to show is that $\mathrm{Fun}(G, \mathbb{C})$ is spanned by $M(\rho_1), M(\rho_2), \ldots, M(\rho_q)$. Let $e_g : G \to \{0, 1\} \subset \mathbb{C}$ be the characteristic function of $g \in G$:

$$e_g(h) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } h = g, \\ 0 & \text{if } h \neq g. \end{cases}$$

Then $\{e_g \mid g \in G\}$ is a basis of $\mathrm{Fun}(G, \mathbb{C})$. We show that $e_g \in \sum_{i=1}^{q} M(\rho_i)$. Fix $x \in G$. Let $\psi_{g,h}$ be the (g, h)th element of $[\text{Right-Reg}(x)]_{\{e_g \mid g \in G\}}$. In the beginning of the proof, we showed that the right regular representation is completely reducible. Thus, Right-Reg is a sum of irreducible representations, therefore $M(\text{Right-Reg}) \subseteq \sum_{i=1}^{q} M(\rho_i)$. From this, we find

$$\begin{aligned} e_g(x) = e_g(1_G \cdot x) = (\text{Right-Reg}(x)(e_g))(1_G) &= \left(\sum_{h \in G} \psi_{h,g}(x)\, e_h \right)(1_G) \\ &= \sum_{h \in G} e_h(1_G)\, \psi_{g,h}(x). \end{aligned}$$

Since this holds for all $x \in G$, we have $e_g = \sum_{h \in G} e_h(1_G)\, \psi_{g,h} \in \sum_{i=1}^{q} M(\rho_i)$. ∎

Corollary 2.4.4. *By the notations and assumptions of the previous theorem, we have (n_i is the dimension of ρ_i)*

(i) Right-Reg $\cong \sum_{i=1}^{q} n_i\rho_i$, *where* $n_i\rho_i = \underbrace{\rho_i + \rho_i + \cdots + \rho_i}_{n_i \text{ times}}$;

(ii) $\sum_{i=1}^{q} n_i^2 = |G|$ *(Burnside's Theorem).*

Proof. $\boxed{(i)}$ By (i) of 2.4.2, we have

$$\text{Right-Reg}|_{M(\rho_i)} \cong \underbrace{\rho_i + \rho_i + \cdots + \rho_i}_{n_i = \dim V_i \text{ times}} \quad \text{for} \quad i = 1, 2, \ldots, q.$$

Using Theorem 2.4.3, we conclude that Right-Reg $\cong \sum_{i=1}^{q} \text{Right-Reg}|_{M(\rho_i)} \cong \sum_{i=1}^{q} n_i\rho_i$.

$\boxed{(ii)}$ Follows from (i) by considering the dimensions of the representations on each side. ■

Definition 2.4.2. *The subspace*

$$\text{Cent}(G) \stackrel{\text{def}}{=} \left\{ f \in \text{Fun}(G, F) \mid f(gxg^{-1}) = f(x) \text{ for all } x, g \in G \right\}$$

is called ***the space of central functions****. The* ***character*** *of a representation $\rho : G \to \text{GL}(V)$ is $\text{ch}_\rho : G \to F$, $g \mapsto \text{Tr}(\rho(g))$. Since for all $x, g \in G$,*

$$\begin{aligned} \text{ch}_\rho\left(gxg^{-1}\right) = \text{Tr}\left(\rho\left(gxg^{-1}\right)\right) = \text{Tr}\left(\rho(g)\,\rho(x)\,\rho(g)^{-1}\right) &= \text{Tr}\left(\rho(g)^{-1}\,\rho(g)\,\rho(x)\right) \\ &= \text{Tr}\left(\rho(x)\right) = \text{ch}_\rho(x), \end{aligned}$$

every character is a central function: $\text{ch}_\rho \in \text{Cent}(G)$. *A character* ch_ρ *is called* ***irreducible*** *if ρ is an irreducible representation of G.*

Theorem 2.4.5. *Let G be a finite group, and suppose that the base field F is algebraically closed and* $\text{char}(F) \nmid G$. *Denote by $\rho_1, \rho_2, \ldots, \rho_q$ the complete list of isomorphism classes of irreducible representations of G. Then* $\text{ch}_{\rho_1}, \text{ch}_{\rho_2}, \ldots, \text{ch}_{\rho_q}$ *is a basis in* $\text{Cent}(G)$. *Particularly,* $q = \dim_F \text{Cent}(G) =$ *number of conjugacy classes in G.*

Proof. Define $\delta : G \to \mathrm{GL}(\mathrm{Fun}(G,F))$ by $(\delta(g)f)(x) \stackrel{\mathrm{def}}{=} f(g^{-1}xg)$. Note that $f \in \mathrm{Cent}(G)$ if and only if $\delta(g)f = f$ for all $g \in G$. By Theorem 2.4.3, any $f \in \mathrm{Fun}(G,F)$ has a unique representation of the form

$$f = f_1 + f_2 + \cdots + f_q \quad \text{where} \quad f_i \in M(\rho_i) \quad \text{for} \quad i = 1, 2, \ldots, q.$$

Suppose that $f \in \mathrm{Cent}(G)$, then

$$f = \delta(g)\, f = \delta(g)\, f_1 + \delta(g)\, f_2 + \cdots + \delta(g)\, f_q,$$

for all $g \in G$. By the uniqueness of the representation f, we conclude that $\delta(g)\, f_i = f_i$ for all $i = 1, 2, \ldots, q$, hence, each f_i is a central function. Clearly, the converse also holds. Hence, each $f \in \mathrm{Cent}(G)$ has a unique representation of the form

$$f = f_1 + f_2 + \cdots + f_q \quad \text{where} \quad f_i \in M(\rho_i) \cap \mathrm{Cent}(G) \quad \text{for} \quad i = 1, 2, \ldots, q.$$

To complete the proof, it is enough to show that $M(\rho) \cap \mathrm{Cent}(G) = F \cdot \mathrm{ch}_\rho$, for all irreducible representations $\rho : G \to \mathrm{GL}(V)$. We know that $\mathrm{ch}_\rho \in \mathrm{Cent}(G)$. On the other hand, $\mathrm{ch}_\rho \in M(\rho)$, since by definition, it is a sum of matrix elements. Thus, it is enough to show that $\dim_F(M(\rho) \cap \mathrm{Cent}(G)) = 1$.

The G acts on $M(\rho)$ via δ and G acts on $\mathrm{End}_F(V)$ via $\mathrm{Adj} : G \to \mathrm{GL}(\mathrm{End}_F(V))$, $\mathrm{Adj}(g)(A) = \rho(g)A\rho(g)^{-1}$. We have the G-equivariant linear isomorphism $\mu : \mathrm{End}_F(V) \to M(\rho)$, $A \mapsto (g \mapsto \mathrm{Tr}(A\rho(g)))$. Via μ, $M(\rho) \cap \mathrm{Cent}(G)$ corresponds to

$$\begin{aligned}
&\{A \in \mathrm{End}_F(V) \mid \mathrm{Adj}(g)(A) = A \text{ for all } g \in G\} \\
&= \left\{A \in \mathrm{End}_F(V) \mid \rho(g)A\rho(g)^{-1} = A \text{ for all } g \in G\right\} \\
&= \{A \in \mathrm{End}_F(V) \mid \rho(g)A = A\rho(g) \text{ for all } g \in G\} \\
&= \{G\text{-equivariant linear transformation of } V\}.
\end{aligned}$$

By Schur's Lemma II, this set is equal to $\{\lambda \cdot \mathrm{id}_V \mid \lambda \in F\}$, which is a one dimensional space. ∎

Corollary 2.4.6. *Let G be a finite group and let F be an algebraically closed field such that* $\mathrm{char}(F) = 0$. *Let ρ and ψ be representations of G. Then $\rho \cong \psi$ if and only if* $\mathrm{ch}_\rho = \mathrm{ch}_\psi$.

Proof. Since G is finite, FG is a finite dimensional algebra, hence artinian. Since $0 = \mathrm{char}(F) \nmid G$, by Maschke's Theorem, FG is a semisimple ring. Using

the Second Wedderburn–Artin Theorem, we conclude that every FG-module is completely reducible. Thus, the representations ρ and ψ are completely reducible. Therefore there exist non-negative integers m_i and n_i $(i = 1, 2, \ldots, q)$ such that

$$\rho \cong m_1\rho_1 + m_2\rho_2 + \cdots + m_q\rho_q \quad \text{and} \quad \psi \cong k_1\rho_1 + k_2\rho_2 + \cdots + k_q\rho_q,$$

where $\rho_1, \rho_2, \ldots, \rho_q$ is a complete list of isomorphism classes of irreducible representations of G. So $\rho \cong \psi$ if and only if $m_i = k_i$ $(\in \mathbb{Z})$ for all $i = 1, 2, \ldots, q$.

On the other hand, we have

$$\mathrm{ch}_\rho = \sum_{i=1}^{q} m_i \mathrm{ch}_{\rho_i} \quad \text{and} \quad \mathrm{ch}_\psi = \sum_{i=1}^{q} k_i \mathrm{ch}_{\rho_i}.$$

From Theorem 2.4.3, we find

$$\mathrm{Fun}(G, F) = \sum_{i=1}^{q} M(\rho_i),$$

which implies that $\mathrm{ch}_1, \mathrm{ch}_2, \ldots, \mathrm{ch}_q \in \mathrm{Fun}(G, F)$ are linearly F-independent. Thus, $\mathrm{ch}_\rho = \mathrm{ch}_\psi$ if and only if $m_i = k_i \in F$ $(\cong m_i = k_i \in \mathbb{Z})$, for all $i = 1, 2, \ldots, q$. The latter isomorphism follows from the assumption that $\mathrm{char}(F) = 0$. ■

This corollary already indicates that the character is an efficient computational device for studying certain questions about representations.

2.5 Character theory of groups

From now on the base field is $F = \mathbb{C}$. First, we review the complex euclidean spaces.

Definition 2.5.1. *By an n-**dimensional complex euclidean space** we mean an n-dimensional complex vector space V together with a **scalar product**, i.e., a map $V \times V \to \mathbb{C}$, $(x, y) \mapsto \langle x, y \rangle$ such that*

*(i) the $\langle \cdot, \cdot \rangle$ is $\frac{1}{2}$-1 linear (**sesquilinear**), i.e.,*

$$\langle x, \lambda_1 y_1 + \lambda_2 y_2 \rangle = \lambda_1 \langle x, y_1 \rangle + \lambda_2 \langle x, y_2 \rangle ,$$

$$\langle \lambda_1 x_1 + \lambda_2 x_2, y \rangle = \overline{\lambda_1} \langle x_1, y \rangle + \overline{\lambda_2} \langle x_2, y \rangle ;$$

(ii) the $\langle \cdot, \cdot \rangle$ *is* ***hermitian****, i.e.,* $\langle y, x \rangle = \overline{\langle x, y \rangle}$ *(which implies that* $\langle x, x \rangle \in \mathbb{R}$*);*

(iii) ***positive definite****, i.e.,* $\langle x, x \rangle \geq 0$ *with equality if and only if* $x = 0$*.*

By choosing an orthonormal basis (from now on ONB) in V (it is possible), we may identify V with $\mathbb{C}^n$, where $n = \dim V$. Then $\langle \cdot, \cdot \rangle$ is identified with $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$, $(x, y) \mapsto x^* y$ where $x^* = \overline{x}^\top$. This is called the *standard scalar product* on $\mathbb{C}^n$.

Definition 2.5.2. *Given a complex euclidean space* $(V, \langle \cdot, \cdot \rangle)$*, an* $A \in \mathrm{End}_{\mathbb{C}}(V)$ *is called* ***unitary*** *if* $\langle A(x), A(y) \rangle = \langle x, y \rangle$*. The group of unitary linear transformations of* $(V, \langle \cdot, \cdot \rangle)$ *is denoted by* $\mathscr{U}(V)$*. We have* $\mathscr{U}(V) \leq \mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{C})$*, where the latter isomorphism follows by choosing a suitable basis in* V *(*$n = \dim V$*). By choosing a suitable basis in* V*,* $\mathscr{U}(V) \cong \mathscr{U}_n(\mathbb{C})$*, where the latter is the group of unitary complex matrices (the complex matrix* A *is called unitary if* $A^* A = I$*).*

Definition 2.5.3. *A finite dimensional complex representation* $\rho : G \to \mathrm{GL}(V)$ *is* ***unitary*** *if there exists a* G*- (*ρ*-) invariant scalar product* $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$*, i.e.,* $\langle x, y \rangle = \langle gx, gy \rangle$ *for all* $x, y \in V$ *and* $g \in G$*. (This means that* $\rho(G) \subseteq \mathscr{U}(V)$ *with respect to this* $\langle \cdot, \cdot \rangle$*.)*

Proposition 2.5.1. *A finite dimensional complex representation of a finite group is always unitary.*

Proof. Let $\rho : G \to \mathrm{GL}(V)$ be a finite dimensional complex representation of a finite group G. Take any scalar product $\beta : V \times V \to \mathbb{C}$ on V. Define

$$\langle x, y \rangle \stackrel{\mathrm{def}}{=} \sum_{g \in G} \beta(gx, gy).$$

It is straightforward to check that $\langle \cdot, \cdot \rangle$ is a G-invariant scalar product. ∎

Proposition 2.5.2. *A unitary representation is always completely reducible.*

Proof. Let $\rho : G \to \mathrm{GL}(V)$ be a unitary representation. Let W be an invariant subspace in V. The $W \oplus W^\perp$, where $W^\perp \stackrel{\mathrm{def}}{=} \{x \in V \mid \langle x, w \rangle = 0 \text{ for all } w \in W\}$ is the *orthogonal complement* of W. We claim that $W^\perp$ is an invariant subspace in V. Indeed, using the invariance of W and the fact that our representation is unitary, we obtain $\langle gx, w \rangle = \langle g^{-1} gx, g^{-1} w \rangle = \langle x, g^{-1} w \rangle = 0$ for all $g \in G$, $x \in W^\perp$ and $w \in W$. ∎

Lemma 2.5.3. *Let ρ be an irreducible representation of G on V, $\dim V < \infty$. An invariant scalar product on V (if exists) is unique up to a non-zero (positive real) scalar multiplier.*

Proof. Fix an invariant scalar product $\langle \cdot, \cdot \rangle$ on V, and take an orthonormal basis on V. Identify V by $\mathbb{C}^n$, so $\langle \cdot, \cdot \rangle = x^*y$. Let β be any other scalar product on $\mathbb{C}^n$. It is well known that there exists a $B \in \mathbb{C}^{n\times n}$ such that $\beta(x, y) = x^*By$.

Suppose that β is G-invariant, i.e.,

$$x^*By = \beta(x, y) = \beta(gx, gy) = x^*(\rho(g)^{-1}B\rho(g))y.$$

Since this holds for all $x, y \in V$, we must have $B = \rho(g)^{-1}B\rho(g)$ for all $g \in G$. Hence, $B \in \mathrm{End}_{\mathbb{C}}(V) = \mathbb{C}^{n\times n}$ commute with $\rho(g)$ for all $g \in G$. By Schur's Lemma II, $B = \lambda \cdot \mathrm{id}_V$ for some $\lambda \in \mathbb{C}$. Thus, $\beta(x, y) = x^*(\lambda \cdot \mathrm{id}_V)y = \lambda x^*y = \lambda \langle x, y\rangle$. ■

Lemma 2.5.4. *Given a representation $\rho : G \to \mathrm{GL}(V)$, U, W invariant subspaces in V, such that ρ_U and ρ_W are irreducible and non-isomorphic. Then $U \perp W$ with respect to any G-invariant scalar product on V.*

Proof. Fix a G-invariant scalar product on V. We have $V = U \oplus U^{\perp}$. Denote by $\pi \in \mathrm{End}_{\mathbb{C}}(V)$ the projection to U (i.e., $\pi|_U = \mathrm{id}_U$, $\mathrm{Ker}(\pi) = U^{\perp}$). Since U is an invariant subspace, from the proof of Proposition 2.5.2, we know that $U^{\perp}$ is also an invariant subspace. From the definition of the direct sum, we have a decomposition $v = u + u^{\perp}$ for all $v \in V$ ($u \in U$, $u^{\perp} \in U^{\perp}$). Then for all $g \in G$ and $v \in V$, we have

$$\begin{aligned}\pi\left(\rho\left(g\right)v\right) &= \pi\left(\rho\left(g\right)u + \rho\left(g\right)u^{\perp}\right) = \pi(\underbrace{\rho\left(g\right)u}_{\in U}) + \pi(\underbrace{\rho\left(g\right)u^{\perp}}_{\in U^{\perp}}) = \rho\left(g\right)u = \rho\left(g\right)\pi\left(u\right)\\ &= \rho\left(g\right)\pi\left(u\right) + \rho\left(g\right)\underbrace{\pi\left(u^{\perp}\right)}_{0} = \rho\left(g\right)\left(\pi\left(u\right) + \pi\left(u^{\perp}\right)\right) = \rho\left(g\right)\pi\left(u + u^{\perp}\right)\\ &= \rho\left(g\right)\pi\left(v\right).\end{aligned}$$

Therefore, π is a G-equivariant linear map. Specially, $\pi|_W : W \to U$ is a G-equivariant linear map. By assumption ρ_U and ρ_W are irreducible and non-isomorphic, hence, by Schur's Lemma I, $\pi|_W \equiv 0$. Therefore $W \subseteq \mathrm{Ker}(\pi) = U^{\perp}$. ■

A natural Reg-invariant scalar product on $\mathrm{Fun}(G, \mathbb{C})$ (G is finite) is given by

$$\langle f, h\rangle \stackrel{\mathrm{def}}{=} \frac{1}{|G|}\sum_{g\in G}\overline{f(g)}h(g),$$

for all $f, h \in \mathrm{Fun}(G, \mathbb{C})$.

Let $\rho^{(i)} : G \to \mathrm{GL}(V_i)$ $(i = 1, 2, \ldots, q)$ be a complete list of isomorphism classes of irreducible representations of the finite group G. Let $n_i = \dim V_i$. Denote by $\rho_{ij}^{(k)}$ $(i, j = 1, 2, \ldots, n_k)$ the matrix elements of $\rho^{(k)}$ with respect to an ONB in V_k (with respect to an invariant scalar product on V_k).

Theorem 2.5.5. *We have*

$$\left\langle \rho_{ij}^{(k)}, \rho_{i'j'}^{(k')} \right\rangle = \begin{cases} \frac{1}{n_k} & \text{if } k = k', i = i' \text{ and } j = j'; \\ 0 & \text{otherwise.} \end{cases}$$

Hence, by Theorem 2.4.3, the unitary matrix elements of the irreducible representations of a finite group constitute an ***orthogonal basis*** *in* $\mathrm{Fun}(G, \mathbb{C})$.

Proof. As a consequence of (iii) of Corollary 2.4.2, for different k and k', $G \times G$ acts irreducibly and non-isomorphically on the spaces $M(\rho^{(k)})$ and $M(\rho^{(k')})$. Therefore, by Lemma 2.5.4, $M(\rho^{(k)}) \perp M(\rho^{(k')})$, i.e., $\left\langle \rho_{ij}^{(k)}, \rho_{i'j'}^{(k')} \right\rangle = 0$ if $k \neq k'$. Hence, we can suppose that $k = k'$ and fix k. We simplify our notations as follows: $\rho \stackrel{\text{def}}{=} \rho^{(k)}$, $V \stackrel{\text{def}}{=} V_k$, $n \stackrel{\text{def}}{=} n_k$ and $\rho_{ij} \stackrel{\text{def}}{=} \rho_{ij}^{(k)}$ for $i, j = 1, 2, \ldots, n$.

In the proof of Proposition 2.4.1 we saw that $V^* \otimes V \cong_\varphi M(\rho)$, where φ is given by $\xi \otimes v \mapsto (g \mapsto \xi(gv))$ for all $\xi \in V^*$, $v \in V$ and $g \in G$. We also have

$$V^* \otimes V \cong_\nu \mathrm{End}_{\mathbb{C}}(V),$$

where ν is defined by $\xi \otimes v \mapsto (x \mapsto \xi(x)\, v)$ for all $\xi \in V^*$, $v \in V$ and $x \in V$. It can be shown that ν is, indeed, an isomorphism. Finally, we have

$$\mathrm{End}_{\mathbb{C}}(V) \cong_\mu M(\rho),$$

where μ is defined by $A \mapsto (g \mapsto \mathrm{Tr}(A\rho(g)))$ for all $A \in \mathrm{End}_{\mathbb{C}}(V)$ (the matrix of the endomorphism in the basis e) and $g \in G$. It can be shown that μ is, indeed, an isomorphism.

$$\begin{array}{ccc} V^* \otimes V & \xrightarrow{\varphi} & M(\rho) \\ \nu \big\downarrow & \nearrow_{\mu} & \\ \mathrm{End}_{\mathbb{C}}(V) & & \end{array}$$

Let $e = \{e_1, e_2, \ldots, e_n\}$ be an orthonormal basis in V. The group $G \times G$ acts on $\mathrm{End}_{\mathbb{C}}(V)$ since $(g,h)A \stackrel{\text{def}}{=} \rho(h)A\rho(g)^{-1}$. This action corresponds to $\rho^* \otimes \rho$ on $V^* \otimes V$ and $\mathrm{Reg}_{M(\rho)}$ on $M(\rho)$. Define the following scalar product on $\mathrm{End}_{\mathbb{C}}(V)$:

$$(A, B) \mapsto \mathrm{Tr}(A^*B),$$

where A^* is the adjoint of A. This is a $G \times G$ invariant scalar product. Indeed,

$$\begin{aligned}
\mathrm{Tr}\left(((g,h)\,A)^*\,(g,h)\,B\right) &= \mathrm{Tr}\left(\left(\rho\left(h\right)A\rho\left(g\right)^{-1}\right)^*\left(\rho\left(h\right)B\rho\left(g\right)^{-1}\right)\right) \\
&= \mathrm{Tr}\left(\left(\rho\left(g^{-1}\right)^*A^*\rho\left(h\right)^*\right)\left(\rho\left(h\right)B\rho\left(g^{-1}\right)\right)\right) \\
&= \mathrm{Tr}\left(\rho\left(g^{-1}\right)^*A^*\left(\rho\left(h\right)^*\rho\left(h\right)\right)B\rho\left(g^{-1}\right)\right) \\
&= \mathrm{Tr}\left(\left(\rho\left(g^{-1}\right)\rho\left(g^{-1}\right)^*\right)A^*\left(\rho\left(h\right)^*\rho\left(h\right)\right)B\right) = \mathrm{Tr}\left(A^*B\right).
\end{aligned}$$

In the last step we used the unitarity property of ρ. Let $E_{ij} \in \mathrm{End}_{\mathbb{C}}(V)$ be the matrix that has 0's everywhere except 1 in entry (i,j). Then $(E_{ij})_{i,j=1}^n$ is an orthogonal basis in $\mathrm{End}_{\mathbb{C}}(V)$:

$$\mathrm{Tr}(E_{ij}^*E_{k\ell}) = \mathrm{Tr}(E_{ji}E_{k\ell}) = \begin{cases} 1 & \text{if } i = k, j = \ell; \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$\begin{aligned}
\mu\left(E_{ij}\right) &= \left(g \mapsto \mathrm{Tr}\left(E_{ij}\rho\left(g\right)\right)\right) = \left(g \mapsto \mathrm{Tr}\left(E_{ij}\left[\sum\nolimits_{k,\ell}\rho_{k\ell}\left(g\right)E_{k\ell}\right]\right)\right) \\
&= \left(g \mapsto \sum\nolimits_{k,\ell}\rho_{k\ell}\left(g\right)\mathrm{Tr}\left(E_{ij}E_{k\ell}\right)\right) = g \mapsto \rho_{ji}\left(g\right),
\end{aligned}$$

i.e., $\mu(E_{ij}) = \rho_{ji}$. The $\mathrm{Tr}\left(\mu^{-1}\left(\,\cdot\,\right)^*\mu^{-1}\left(\,\cdot\,\right)\right)$ is a Reg-invariant scalar product, hence, by Lemma 2.5.3, we must have

$$\left\langle\,\cdot\,,\,\cdot\,\right\rangle = \lambda \cdot \mathrm{Tr}\left(\mu^{-1}\left(\,\cdot\,\right)^*\mu^{-1}\left(\,\cdot\,\right)\right),$$

for some constant λ. Thus,

$$\langle \rho_{ij}, \rho_{i'j'}\rangle = \lambda \cdot \mathrm{Tr}\left(E_{ji}^*E_{j'i'}\right) = \begin{cases} \lambda & \text{if } i = i', j = j'; \\ 0 & \text{otherwise.} \end{cases}$$

It remains to show that $\lambda = \frac{1}{n}$. We have

$$\lambda = \langle \rho_{ij}, \rho_{ij}\rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\rho_{ij}\left(g\right)}\rho_{ij}\left(g\right), \quad \text{for } \; i,j = 1,2,\ldots,n.$$

Taking the sum over i, we find

$$\begin{aligned} n\lambda &= \sum_{i=1}^{n} \frac{1}{|G|} \sum_{g\in G} \overline{\rho_{ij}(g)}\rho_{ij}(g) = \frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{n} \overline{\rho_{ij}(g)}\rho_{ij}(g) \\ &= \frac{1}{|G|}\sum_{g\in G} \left([\rho(g)^*]\cdot[\rho(g)]\right)_{jj} = \frac{1}{|G|}\sum_{g\in G} 1 = \frac{1}{|G|}|G| = 1. \end{aligned}$$

Here, we used the unitarity property of the matrix of ρ. Hence, $\lambda = \frac{1}{n}$. ∎

Corollary 2.5.6. *Denote by $\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(q)}$ the complete list of isomorphism classes of irreducible representations of the finite group G. The $\chi_i \overset{\text{def}}{=} \mathrm{ch}_{\rho^{(i)}}$ ($i = 1, 2, \ldots, q$) constitute an ONB in $\mathrm{Cent}(G, \mathbb{C}) \subseteq \mathrm{Fun}(G, \mathbb{C})$.*

Proof. By Theorem 2.4.5, they form a basis in $\mathrm{Cent}(G, \mathbb{C})$. We have $\chi_k = \sum_{i=1}^{n_k} \rho_{ii}^{(k)}$. Thus

$$\langle \chi_k, \chi_\ell \rangle = \left\langle \sum_{i=1}^{n_k} \rho_{ii}^{(k)}, \sum_{j=1}^{n_\ell} \rho_{jj}^{(\ell)} \right\rangle = \sum_{i=1}^{n_k}\sum_{j=1}^{n_\ell} \left\langle \rho_{ii}^{(k)}, \rho_{jj}^{(\ell)} \right\rangle = \begin{cases} 0 & \text{if } k \neq \ell, \\ \sum_{i=1}^{n_k} \left\langle \rho_{ii}^{(k)}, \rho_{ii}^{(\ell)} \right\rangle & \text{if } k = \ell. \end{cases}$$

Since

$$\sum_{i=1}^{n_k} \left\langle \rho_{ii}^{(k)}, \rho_{ii}^{(\ell)} \right\rangle = \sum_{i=1}^{n_k} \frac{1}{n_k} = 1,$$

if $k = \ell$, the proof is complete. ∎

Corollary 2.5.7. *Denote by $\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(q)}$ the complete list of isomorphism classes of irreducible representations of the finite group G. Let ρ be any representation of G. We have*

(i) $\rho \cong \sum_{k=1}^{q} \langle \mathrm{ch}_\rho, \chi_k \rangle \rho^{(k)}$;

(ii) the ρ is irreducible if and only if $\langle \mathrm{ch}_\rho, \mathrm{ch}_\rho \rangle = 1$.

Proof. $\boxed{(i)}$ Every representation is isomorphic to the linear combination of irreducible representations. Suppose that $\rho \cong \sum_{k=1}^{q} m_k \rho^{(k)}$. Taking the trace of both sides yields

$$\mathrm{ch}_\rho = \sum_{k=1}^{q} m_k \chi_k.$$

Taking the scalar product of both sides by χ_j, and using the previous corollary, we obtain $\langle \mathrm{ch}_\rho, \chi_j \rangle = m_j$.

$\boxed{(ii)}$ Suppose that $\rho \cong \sum_{k=1}^{q} m_k \rho^{(k)}$. Then

$$\langle \mathrm{ch}_\rho, \mathrm{ch}_\rho \rangle = \left\langle \sum_{k=1}^{q} m_k \chi_k, \sum_{j=1}^{q} m_j \chi_j \right\rangle = \sum_{k=1}^{q} m_k^2.$$

If ρ is irreducible, then $\rho \cong \rho^{(i)}$ for some $i \in \{1, 2, \ldots, q\}$. Then, using Corollary 2.4.6, $m_i = 1$ and $m_j = 0$ for $i \neq j$, therefore $\langle \mathrm{ch}_\rho, \mathrm{ch}_\rho \rangle = 1$. Conversely, if $\langle \mathrm{ch}_\rho, \mathrm{ch}_\rho \rangle = 1$, then by the above calculation we must have $m_i = 1$ for some $i \in \{1, 2, \ldots, q\}$, and $m_j = 0$ for $i \neq j$. Hence $\mathrm{ch}_\rho = \chi_i$, and by Corollary 2.4.6, $\rho \cong \rho^{(i)}$. ■

Definition 2.5.4. *Denote by $\mathscr{C}_j$ $(j = 1, 2, \ldots, q)$ the conjugacy classes in the finite group G. Let χ_j $(j = 1, 2, \ldots, q)$ be the list of irreducible characters of G. Finally, let us denote by $\chi_j(\mathscr{C}_k)$ the value $\chi_j(g)$ for any $g \in \mathscr{C}_k$. Then the $q \times q$ complex matrix whose (i, j)th entry is $\chi_i(\mathscr{C}_j)$ is called the* ***character table*** *of G.*

Denote by D the $q \times q$ complex matrix, whose (i, j)th entry is

$$\chi_i(\mathscr{C}_j) \sqrt{\frac{|\mathscr{C}_j|}{|G|}}.$$

The orthonormality of irreducible characters shows that the rows of D are orthonormal with respect to the standard scalar product, i.e., $DD^* = I$, where I is the $q \times q$ identity matrix. This gives $D^*D = I$, i.e., the columns of D are orthonormal with respect to the standard scalar product:

$$\sum_{k=1}^{q} \overline{\chi_k(\mathscr{C}_i) \sqrt{\frac{|\mathscr{C}_i|}{|G|}}} \chi_k(\mathscr{C}_j) \sqrt{\frac{|\mathscr{C}_j|}{|G|}} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Thus we have deduced the following theorem.

Theorem 2.5.8 (Second Orthogonality Relation)**.**

$$\sum_{k=1}^{q} \overline{\chi_k(\mathscr{C}_i)} \chi_k(\mathscr{C}_j) = \begin{cases} \frac{|G|}{|\mathscr{C}_i|} & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Remark. *We have*

$$\frac{|G|}{|\mathscr{C}_i|} = |C_G(g)|, \quad g \in \mathscr{C}_i,$$

where $C_G(g)$ is the centralizer of g in G.

2.6 Burnside's Theorem

In this section, we shall use representation theory to prove Burnside's Theorem about solvability of groups. Burnside's Theorem has long been one of the best-known applications of representation theory to the theory of finite groups, though a proof avoiding the use of group characters is known since around 1970.

Definition 2.6.1. *A complex number α is an **algebraic integer** if α is a root of a monic polynomial with integer coefficients.*

Remark. *A rational number is an algebraic integer if and only if it is an integer.*

Let G be a finite group, $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation of G with character χ. If $g \in G$, then there is an $n \in \mathbb{N}$ such that $g^n = 1$, thus $\mathrm{id}_V = \rho(1) = \rho(g^n) = \rho(g)^n$. In a suitable basis of V ($\dim V = d$), $\rho(g)$ is a $d \times d$ diagonal matrix. Hence, the eigenvalues must be roots of unity $(\omega_1, \omega_2, \ldots, \omega_d)$. Therefore $\chi(g) = \omega_1 + \omega_2 + \cdots + \omega_d$ is an algebraic integer.

Denote by $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_q$ the conjugacy classes in the finite group G. Let ρ be an irreducible representation of G, and χ be its character. We saw earlier that if $\rho : G \to \mathrm{GL}(V)$ then we have a natural extension $\tilde{\rho} : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(V)$. Consider

$$\mathbb{C}G \ni c_i \stackrel{\text{def}}{=} \sum_{g \in \mathscr{C}_i} g \quad \text{for} \quad i = 1, 2, \ldots, q.$$

Clearly, each c_i is in the centre $\mathscr{Z}(\mathbb{C}G)$ and they form a $\mathbb{C}$-basis in $\mathscr{Z}(\mathbb{C}G)$. We have

$$c_i c_j = \sum_{k=1}^{q} m_{ijk} c_k,$$

where

$$m_{ijk} = |\{(g, h) \mid g \in \mathscr{C}_i, h \in \mathscr{C}_j, gh \in \mathscr{C}_k\}|.$$

From

$$\tilde{\rho}\left(c_i\right)\rho\left(g\right)=\sum_{h\in\mathscr{C}_i}\rho\left(h\right)\rho\left(g\right)=\sum_{h\in\mathscr{C}_i}\rho\left(hg\right)=\sum_{s\in\mathscr{C}_i}\rho\left(gs\right)=\sum_{s\in\mathscr{C}_i}\rho\left(g\right)\rho\left(s\right)$$
$$=\rho\left(g\right)\tilde{\rho}\left(c_i\right),$$

we conclude that $\tilde{\rho}\left(c_i\right)$ is a G-equivariant linear map of V $(i=1,2,\ldots,q)$. By Schur's Lemma II, $\tilde{\rho}\left(c_i\right)$ is a scalar multiple of id_V, $\tilde{\rho}\left(c_i\right)=\lambda_i\mathrm{id}_V$, say. The value of λ_i follows by taking the trace of each side and by noting that $\mathrm{Tr}(\mathrm{id}_V)=\dim V=\chi(1)$:

$$\tilde{\rho}(c_i)=\frac{\mathrm{Tr}\left(\tilde{\rho}\left(c_i\right)\right)}{\chi\left(1\right)}\mathrm{id}_V=\frac{\sum_{g\in\mathscr{C}_i}\mathrm{Tr}\left(\rho\left(g\right)\right)}{\chi\left(1\right)}\mathrm{id}_V=\frac{\sum_{g\in\mathscr{C}_i}\chi\left(g\right)}{\chi\left(1\right)}\mathrm{id}_V=\frac{\sum_{g\in\mathscr{C}_i}\chi\left(\mathscr{C}_i\right)}{\chi\left(1\right)}\mathrm{id}_V$$
$$=\underbrace{\frac{\chi\left(\mathscr{C}_i\right)\left|\mathscr{C}_i\right|}{\chi\left(1\right)}}_{u_i}\mathrm{id}_V.$$

From $\tilde{\rho}\left(c_i\right)\tilde{\rho}\left(c_j\right)=\tilde{\rho}\left(c_ic_j\right)=\tilde{\rho}\left(\sum_{k=1}^{q}m_{ijk}c_k\right)=\sum_{k=1}^{q}m_{ijk}\tilde{\rho}\left(c_k\right)$, we obtain $u_iu_j=\sum_{k=1}^{q}m_{ijk}u_k$. Thus, $R\overset{\mathrm{def}}{=}\mathbb{Z}u_1+\mathbb{Z}u_2+\cdots+\mathbb{Z}u_q$ is a subring of $\mathbb{C}$.

Proposition 2.6.1. *An element $\alpha\in\mathbb{C}$ is an algebraic integer if and only if there exists a subring R of $\mathbb{C}$ containing α, such that R is a finitely generated abelian group.*

From our argument above and the proposition, we immediately deduce the following lemma.

Lemma 2.6.2. *Let G be a finite group, χ be an irreducible (complex) character of G. Let $\mathscr{C}$ be a conjugacy class in G. Then $\frac{\chi(\mathscr{C})|\mathscr{C}|}{\chi(1)}$ is an algebraic integer.*

Proof of Proposition 2.6.1. $\boxed{\Rightarrow}$ Suppose that α is an algebraic integer. Then there exist $a_1,a_2,\ldots,a_n\in\mathbb{Z}$ such that

$$\alpha^n+a_1\alpha^{n-1}+\cdots+a_{n-1}\alpha+a_n=0,$$

i.e., $\alpha^n=-a_n-a_{n-1}\alpha-\cdots-a_1\alpha^{n-1}\in\mathbb{Z}+\mathbb{Z}\alpha+\cdots+\mathbb{Z}\alpha^{n-1}\overset{\mathrm{def}}{=}R$. Then R is the desired subring of $\mathbb{C}$.

$\boxed{\Leftarrow}$ Suppose that R is a subring of $\mathbb{C}$, such that $\alpha\in R$ and R is finitely generated $\mathbb{Z}$-module by $e_1,e_2,\ldots,e_n$: $R=\mathbb{Z}e_1+\mathbb{Z}e_2+\cdots+\mathbb{Z}e_n$. Then

$$\alpha e_j=\sum_{i=1}^{n}a_{ij}e_i\quad\text{for some}\quad a_{ij}\in\mathbb{Z}.$$

Define $A \stackrel{\text{def}}{=} (a_{ij})_{i,j=1}^{n} \in \mathbb{Z}^{n\times n}$. The characteristic polynomial $f(x) \stackrel{\text{def}}{=} \det(xI - A) \in \mathbb{Z}[x]$ is a monic polynomial ($I = \mathrm{id}_{\mathbb{C}^n}$). By the Cayley–Hamilton Theorem, $f(A) = 0$. Let $0 = f(A) = (b_{ij})_{i,j=1}^{n}$, then

$$f(\alpha) \underbrace{e_j}_{\neq 0} = \sum_{i=1}^{n} b_{ij} e_i = \sum_{i=1}^{n} 0 e_i = 0.$$

Thus, $f(\alpha) = 0$. Therefore, α is a root of a monic polynomial with integer coefficients, i.e., α is an algebraic integer. ■

Corollary 2.6.3. *The algebraic integers constitute a subring in* $\mathbb{C}$.

Corollary 2.6.4 (Corollary of Lemma 2.6.2)**.** *We have* $\chi(1) \mid |G|$ *for all irreducible characters* χ *of* G.

Proof. Let χ be any irreducible character of G. We have

$$1 = \langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi(g)} \chi(g) = \frac{1}{|G|} \sum_{j=1}^{q} \overline{\chi(\mathscr{C}_j)} \chi(\mathscr{C}_j) |\mathscr{C}_j|,$$

whence

$$\frac{|G|}{\chi(1)} = \sum_{j=1}^{q} \overline{\chi(\mathscr{C}_j)} \frac{\chi(\mathscr{C}_j) |\mathscr{C}_j|}{\chi(1)}.$$

We remarked earlier that the first factor under the sum on the right-hand side is an algebraic integer (sum of roots of unity). From Lemma 2.6.2, the second factor is also an algebraic integer. Product and sum of algebraic integers is again an algebraic integer (cf. Corollary 2.6.3). Thus, the right-hand side is an algebraic integer. Therefore, on the left-hand side there is a rational number which is an algebraic integer. This means that it is an integer. Consequently, $\chi(1) \mid |G|$. ■

Lemma 2.6.5. *Let* G *be a finite group,* $\rho : G \to \mathrm{GL}(V)$ *be a complex irreducible representation with character* χ. *Let* $\mathscr{C}$ *be a conjugacy class in* G. *If* $\gcd(|\mathscr{C}|, \chi(1)) = 1$, *then* $\chi(\mathscr{C}) = 0$ *or* $\rho(g) \in \mathbb{C} \cdot \mathrm{id}_V$ *for all* $g \in \mathscr{C}$.

Proof. Since $\gcd(|\mathscr{C}|, \chi(1)) = 1$, there exist $k, \ell \in \mathbb{Z}$ such that $k|\mathscr{C}| + \ell\chi(1) = 1$. Thus,

$$k \frac{\chi(\mathscr{C}) |\mathscr{C}|}{\chi(1)} + \ell \chi(\mathscr{C}) = \frac{\chi(\mathscr{C})}{\chi(1)}.$$

On the left hand side, both terms are algebraic integers, hence $\frac{\chi(\mathscr{C})}{\chi(1)}$ is an algebraic integer. We know that $\chi(\mathscr{C})$ is the sum of roots of unity, $\chi(\mathscr{C}) = \omega_1 + \omega_2 + \cdots + \omega_n$, say $(n = \chi(1) = \dim V)$. Note that

$$|\chi(\mathscr{C})| = |\omega_1 + \omega_2 + \cdots + \omega_n| \leq |\omega_1| + |\omega_2| + \cdots + |\omega_n| = n = \chi(1),$$

hence, $\left|\frac{\chi(\mathscr{C})}{\chi(1)}\right| \leq 1$. Moreover, equality holds if and only if $\rho(g) \in \mathbb{C} \cdot \mathrm{id}_V$ for all $g \in \mathscr{C}$. Let $g \in \mathscr{C}$, then $\omega_i^d = 1$ with d being the order of g in G (the smallest non-negative integer r such that $g^r = 1$) and $i = 1, 2, \ldots, n$. We have

$$\mathbb{C}^\times > \langle \omega_1, \omega_2, \ldots, \omega_n \rangle \leq \left\langle e^{2\pi i/d} \right\rangle$$

as groups. The field $F \stackrel{\text{def}}{=} \mathbb{Q}(e^{2\pi i/d})$ contains all the ω_i's (a cyclotomic field), and $\dim_{\mathbb{Q}}(F) = \varphi(d)$ where φ is the Euler-function.

We need a few facts from Galois-Theory: If $\mathrm{Aut}(F)$, the group of field automorphisms of F, then

(i) $|\mathrm{Aut}(F)| < \infty$ (in fact it is equal to $\dim_{\mathbb{Q}}(F) = \varphi(d)$);

(ii) if for some $b \in F$, $\sigma(b) = b$ for all $\sigma \in \mathrm{Aut}(F)$, then $b \in \mathbb{Q}$;

(iii) every $\sigma \in \mathrm{Aut}(F)$ sends an algebraic integer in F to an algebraic integer (with the same minimal polynomial).

Take any $g \in \mathscr{C}$ and set

$$w \stackrel{\text{def}}{=} \prod_{\sigma \in \mathrm{Aut}(F)} \sigma\left(\frac{\chi(g)}{\chi(1)}\right).$$

By (i), this product is well-defined. Since w is fixed by any element of $\mathrm{Aut}(F)$, by (ii), $w \in \mathbb{Q}$. Moreover, by (iii), each factor of the product is an algebraic integer, hence w is an algebraic integer. Consequently, $w \in \mathbb{Z}$. Since $\sigma(\omega_i)^d = \sigma(\omega_i^n) = \sigma(1) = 1$, it follows that $\sigma(\omega_i)$ is a root of 1 for all $\sigma \in \mathrm{Aut}(F)$. Thus,

$$\begin{aligned}
&\left|\sigma\left(\frac{\chi(g)}{\chi(1)}\right)\right| = \left|\frac{1}{\chi(1)}\sigma(\chi(g))\right| = \left|\frac{\sigma(\omega_1 + \omega_2 + \cdots + \omega_n)}{\chi(1)}\right| \\
&= \left|\frac{\sigma(\omega_1) + \sigma(\omega_2) + \cdots + \sigma(\omega_n)}{\chi(1)}\right| \leq \frac{|\sigma(\omega_1)| + |\sigma(\omega_2)| + \cdots + |\sigma(\omega_n)|}{\chi(1)} \\
&= \frac{n}{\chi(1)} = 1,
\end{aligned}$$

for all $\sigma \in \mathrm{Aut}(F)$. Therefore, $|w| \leq 1$. But $w \in \mathbb{Z}$, hence, $w = 0, 1$ or -1. The $w = 0$ if and only if $\chi(g) = 0$. By the triangular inequality, $|w| = 1$ implies

$\left|\frac{\chi(g)}{\chi(1)}\right| = 1$, and hence $\rho(g) \in \mathbb{C} \cdot \mathrm{id}_V$ for all $g \in \mathscr{C}$, as we remarked earlier. ■

Remark. *Let* $\mathcal{Z}(G) \stackrel{\text{def}}{=} \{z \in G \mid zg = gz \text{ for all } g \in G\} \lhd G$ *be the* ***centre*** *of the group* G. *If* $G = \mathcal{Z}(G)$, *then* G *is abelian. For a* ***non-abelian simple*** *group* G *we have* $\mathcal{Z}(G) = \{1\}$. *Indeed, let* G *be a non-abelian simple group. We have* $\mathcal{Z}(G) \lhd G$, *thus, by simplicity,* $\mathcal{Z}(G) = \{1\}$ *or* $\mathcal{Z}(G) = G$. *The latter can not be hold since* G *is non-abelian.*

A non-trivial (irreducible) representation of a non-abelian simple group is faithful. Indeed, let $\rho : G \to \mathrm{GL}(V)$ *be a non-trivial representation of the non-abelian simple group* G. *Since* $\mathrm{Ker}(\rho) \lhd G$ *and* G *is simple, we must have* $\mathrm{Ker}(\rho) = \{1\}$ *or* $\mathrm{Ker}(\rho) = G$. *The latter can not be hold since* ρ *is non-trivial. Therefore,* $\mathrm{Ker}(\rho) = \{1\}$, *i.e.,* ρ *is faithful.*

Theorem 2.6.6. *A non-abelian simple group contains no conjugacy class of size a prime power, except the conjugacy class of* $1 \in G$.

Proof. Assume to the contrary that $\mathscr{C}$ is a conjugacy class in G, such that $|\mathscr{C}| = p^\alpha$, where p is a prime and α is a positive integer. Note that for a non-trivial irreducible representation $\rho : G \to \mathrm{GL}(V)$ and $1 \neq g \in G$, $\rho(g) \notin \mathbb{C} \cdot \mathrm{id}_V$. Indeed, by the second part of the above remark, ρ is injective and so an isomorphism between G and $\rho(G) \stackrel{\text{def}}{=} \mathrm{Im}(\rho)$. Therefore,

$$\mathcal{Z}\left(\rho\left(G\right)\right) = \rho\left(\mathcal{Z}\left(G\right)\right) = \rho\left(\{1\}\right) = \{\rho\left(1\right)\}.$$

The second equality follows from the first part of the above remark. If we would have $\rho(g) \in \mathbb{C} \cdot \mathrm{id}_V$ for some $1 \neq g$, then $\rho(g) \in \mathcal{Z}\left(\rho\left(G\right)\right)$, and by the above $\rho(g) = \rho(1)$. This is a contradiction, since ρ is faithful (injective).

Let χ_j $(j = 1, 2, \ldots, q)$ be the list of irreducible characters of G with χ_1 being the trivial one. If $p \nmid \chi_j(1)$ for some $j = 2, \ldots, q$, then $\gcd(|\mathscr{C}|, \chi_j(1)) = 1$, hence, by Lemma 2.6.5, $\chi_j(\mathscr{C}) = 0$ (as $\rho_j(g) \notin \mathbb{C} \cdot \mathrm{id}_V$ for $g \in \mathscr{C}$). Thus, by the Second Orthogonality Relation

$$0 = \sum_{i=1}^{q} \chi_i\left(1\right) \chi_i\left(\mathscr{C}\right) = 1 + \sum_{i=2}^{q} \chi_i\left(1\right) \chi_i\left(\mathscr{C}\right) = 1 + \sum_{\substack{i \in \{2,3,\ldots,q\} \\ p \mid \chi_i(1)}} \chi_i\left(1\right) \chi_i\left(\mathscr{C}\right),$$

which gives

$$-\frac{1}{p} = \sum_{\substack{i \in \{2,3,\ldots,q\} \\ p \mid \chi_i(1)}} \frac{\chi_i\left(1\right)}{p} \chi_i\left(\mathscr{C}\right).$$

We remarked earlier that the second factor under the sum on the right-hand side is an algebraic integer (sum of roots of unity). The first factor is also an algebraic integer (it is an integer). Product and sum of algebraic integers is again an algebraic integer (cf. Corollary 2.6.3). Thus, the right-hand side is an algebraic integer. Therefore, on the left-hand side there is a rational number which is not an integer but an algebraic integer. This is a contradiction. ∎

Definition 2.6.2. *A group G is said to be* ***solvable*** *if there exists a chain of subgroups*

$$\{1\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{k-1} \leq G_k = G,$$

such that $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian ($i = 0, 1, \ldots, k-1$).

Proposition 2.6.7. *Suppose that $|G| = p^\alpha$. Then $\mathcal{Z}(G) \neq \{1\}$, i.e., the centre of G is non-trivial.*

Proof. Let $\{1\} = \mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_k$ be the conjugacy classes of G. We have $|\mathscr{C}_i| \mid |G| = p^\alpha$ and $|\mathscr{C}_i| = [G : C_G(g)]$, where $g \in \mathscr{C}_i$ and $C_G(g)$ is the centralizer of g in G ($i = 1, 2, \ldots, k$). Since G is the disjoint union of the conjugacy classes, we have

$$|G| = p^\alpha = \sum_{i=1}^{k} |\mathscr{C}_i| = \sum_{g_i \in \mathscr{C}_i} [G : C_G(g_i)] \,.$$

Observing that each element of the center $\mathcal{Z}(G)$ forms a conjugacy class containing just itself gives rise to the following important *class equation*:

$$|G| = p^\alpha = |\mathcal{Z}(G)| + \sum_{\substack{g_i \in \mathscr{C}_i \\ |\mathscr{C}_i| > 1}} [G : C_G(g_i)] \,.$$

From this we see that p must divide $|\mathcal{Z}(G)|$, so $|\mathcal{Z}(G)| > 1$. ∎

Theorem 2.6.8 (Burnside's $p^\alpha q^\beta$ Theorem)**.** *A group of order $p^\alpha q^\beta$ (p, q being primes) is solvable.*

Proof. First, assume that $|G| = p^\alpha$. If it is abelian, we are done. Suppose that it is not abelian. Take $G_1 \stackrel{\text{def}}{=} \mathcal{Z}(G) \gneq \{1\}$ (here we used Proposition 2.6.7). Since G is not abelian, $G_1 \lneq G$. Thus, we have

$$\{1\} \lneq G_1 \lneq G, \; G_1 \triangleleft G \;\text{ and }\; G_1 \;\text{ being abelian.}$$

Take $G/G_1 = G/\mathcal{Z}(G)$. If it is abelian, we are done. Suppose that it is not abelian, then $\{1\} \lneq \mathcal{Z}(G/\mathcal{Z}(G)) \lneq G/\mathcal{Z}(G)$. Let G_2 be such that $G_2/G_1 = \mathcal{Z}(G/G_1) = \mathcal{Z}(G/\mathcal{Z}(G))$. Then

$$\{1\} \lneq G_1 \lneq G_2 \lneq G,\ G_2 \lhd G \ \text{ and } \ G_2/G_1 \ \text{ being abelian.}$$

If G/G_2 is abelian, we are done. If it is not, we can proceed further in this way to get a chain of subgroups. The process should come to a halt, since $|G|$ is finite and $|G_k| > |G_{k-1}|$ $(k = 2, 3, 4, \ldots)$. Thus, we have proved the theorem for $\beta = 0$.

Now suppose that $|G| = p^\alpha q^\beta$. We shall prove by induction on $|G|$. For $|G| = p^\alpha$ the theorem is already proved. Let N be a maximal normal subgroup of G.

If $N \neq \{1\}$, then $|G/N| < |G|$ and $|G/N| = p^{\alpha'} q^{\beta'}$ $(\alpha' + \beta' < \alpha + \beta)$. Hence, by the induction hypothesis, G/N is solvable and so is G.

If $N = \{1\}$, then G is simple. Let P be a p-Sylow subgroup of G, i.e., $|P| = p^\alpha$. By Proposition 2.6.7, there exist a $g \neq 1$ in $\mathcal{Z}(P)$. Then g commutes with all the elements of P, hence

$$G \gneq C_G(g) \geq P,$$

where $C_G(g)$ is the centralizer of g in G. Indeed, $G = C_G(g)$ can not hold, since then $\langle g \rangle$ would be a non-trivial normal subgroup of G, which contradicts the fact that G is simple. Let $\mathscr{C}$ be the conjugacy class of g, then

$$|\mathscr{C}| = [G : C_G(g)] \mid [G : P] = p^\beta,$$

hence, $1 < |\mathscr{C}| = p^{\beta'}$. Therefore, by Theorem 2.6.6, our simple group G must be abelian. But abelian groups are always solvable. ■

Chapter 3

Commutative rings

Throughout this chapter, a ring will always mean a commutative ring with unity. Frequently we shall also assume that the ring R is also a commutative K-algebra (K is a field). In this case $K \subset R$ and the unity elements of R and K coincide.

Let K be a field, we denote by $K[x_1, x_2, \ldots, x_m]$ the m-variable polynomial ring over K. If I is an ideal in $K[x_1, x_2, \ldots, x_m]$, we can consider $K[x_1, x_2, \ldots, x_m]/I$, i.e., finitely generated K-algebras. These are important for Algebraic Geometry.

Let F be a field such that $\mathbb{Q} \subset F \subset \mathbb{C}$. We assume that $[F : \mathbb{Q}] \stackrel{\text{def}}{=} \dim_{\mathbb{Q}} F < \infty$. Then we can consider the ring R of algebraic integers in F. Such rings are important in Number Theory. Two important examples are the Gauss- and Euler-integers, i.e., the algebraic integers in $\mathbb{Q}(i)$ and $\mathbb{Q}(e^{2\pi i/3})$.

3.1 The Noether Normalization Lemma

First, we introduce the basic concepts.

Definition 3.1.1. *Suppose that R is a commutative K-algebra. We say that $r_1, r_2, \ldots, r_m \in R$ are **algebraically independent over** K if $f(r_1, r_2, \ldots, r_m) = 0$ for some $f \in K[x_1, x_2, \ldots, x_m]$ implies that $f = 0 \in K[x_1, x_2, \ldots, x_m]$. Otherwise $r_1, r_2, \ldots, r_m \in R$ are said to be **algebraically dependent over** K. For infinitely many elements, we say that they are algebraically independent over K if any of their finite subset is algebraically independent over K.*

Definition 3.1.2. *Suppose that K is a subfield of L. A set G of L is a* ***transcendence generating system of*** *L* ***over*** *K if L is algebraic over its subfield generated by G over K.*

Definition 3.1.3. *By a* ***transcendence basis*** *of L over K we mean an algebraically independent transcendence generating system of L over K.*

Proposition 3.1.1. *Suppose that K is a subfield of L. The L always has a transcendence basis over K, and its cardinality is uniquely determined. It is called the* ***transcendence degree*** *of L over K. In notation:* $\operatorname{tr\,deg}_K(L)$.

The key point of the proof is the following lemma.

Lemma 3.1.2. *Let I be an algebraically independent subset of L, G be a transcendence generating system of L. Then for all $a \in I$ there is a $b \in G$ such that $G \setminus \{b\} \cup \{a\}$ is still a transcendence generating system of L.*

Definition 3.1.4. *Let R be a K-algebra which is an integral domain (contains no zero-divisors). Let L be the field of fractions of R (see Definition 3.2.3). Then* $\operatorname{tr\,deg}_K(R) \stackrel{\text{def}}{=} \operatorname{tr\,deg}_K(L)$.

Example 3.1.1. *We have* $\operatorname{tr\,deg}_K(K[x_1, x_2, \ldots, x_m]) = m$. *Also*

$$\operatorname{tr\,deg}_K(K[x_1, x_2, \ldots, x_m]/f) = m - 1,$$

where $f \in K[x_1, x_2, \ldots, x_m]$ is an irreducible polynomial.

Given a K-algebra R, $a_1, a_2, \ldots, a_n \in R$, then $K[a_1, a_2, \ldots, a_n]$ stands for the K-subalgebra of R generated by $a_1, a_2, \ldots, a_n$. If $n = 0$, then the generated K-subalgebra is K, because a subalgebra always contains $1 \in K$.

Definition 3.1.5. *Let R be a subring of S. We say that $s \in S$ is* ***integral over*** *R if there is a monic polynomial f in $R[x]$ such that $f(s) = 0$. We say that S is integral over R if all $s \in S$ is integral over R.*

A special case is given by $R = \mathbb{R}$ and $S \subseteq \mathbb{C}$.

Lemma 3.1.3. *Given a subring $R \subseteq S$, $a \in S$, the following are equivalent:*

(i) the a is integral over R;

(ii) there is a subring T, $R \subseteq T \subseteq S$ such that $a \in T$ and T is a finitely generated R-module (briefly let it call finite R-module);

(iii) the $R[a]$ is a finite R-module.

Proof. $\boxed{(iii) \Rightarrow (ii)}$ Let T be $R[a]$.

$\boxed{(i) \Rightarrow (iii)}$ Suppose that a is integral over R. Then there is a positive integer n and $b_1, b_2, \ldots, b_n \in R$ such that $a^n + b_1 a^{n-1} + \cdots + b_{n-1}a + b_n = 0$, whence $a^n \in Ra^{n-1} + Ra^{n-2} + \cdots + R \cdot 1$ (the R-module of S generated by $1, a, \ldots, a^{n-1}$). This shows that $\sum_{i=0}^{n-1} Ra^i$ is a subring.

$\boxed{(ii) \Rightarrow (i)}$ Suppose that T is a subring of S, such that $a \in T$ and T is a finitely generated R-module by $e_1, e_2, \ldots, e_n$: $T = Re_1 + Re_2 + \cdots + Re_n$. Then

$$ae_j = \sum_{i=1}^{n} a_{ij} e_i \quad \text{for some} \quad a_{ij} \in R.$$

Define $A \stackrel{\text{def}}{=} (a_{ij})_{i,j=1}^{n} \in R^{n \times n}$. The characteristic polynomial $f(x) \stackrel{\text{def}}{=} \det(xI - A) \in R[x]$ is a monic polynomial (I stands for the identity matrix). By the Cayley–Hamilton Theorem, $f(A) = 0$. Let $0 = f(A) = (b_{ij})_{i,j=1}^{n}$, then

$$f(a) \underbrace{e_j}_{\neq 0} = \sum_{i=1}^{n} b_{ij} e_i = \sum_{i=1}^{n} 0 e_i = 0.$$

Thus, $f(a) = 0$. Therefore, a is a root of a monic polynomial with coefficients from R, i.e., a is integral over R. ∎

Lemma 3.1.4. *Let $R \subseteq S \subseteq T$ be rings. If S is a finite R-module, T is a finite S-module; then T is a finite R-module.*

Proof. By assumption, there exist $a_1, a_2, \ldots, a_n \in S$ such that $S = \sum_{i=1}^{n} Ra_i$ and there exist $b_1, b_2, \ldots, b_k \in T$ such that $T = \sum_{j=1}^{k} Sb_j$. Then we have $T = \sum_{i=1}^{n} \sum_{j=1}^{k} Ra_i b_j$. ∎

Corollary 3.1.5. *Given a subring $R \subseteq S$, such that S is a finitely generated R-algebra (an R-module which is also a ring). Then S is integral over R if and only if S is finite over R, i.e., S is a finite R-module.*

Proof. $\boxed{\Leftarrow}$ Let $s \in S$ be arbitrary. Using the implication $(ii) \Rightarrow (i)$ of Lemma 3.1.3 with $R \subseteq S \subseteq S$, we find that s is integral over R. Since s was arbitrary, every element of S is integral over R, i.e., S is integral over R.

$\boxed{\Rightarrow}$ Let $s_1, s_2, \ldots, s_n$ be the generators of the finitely generated R-algebra S. Since s_1 is integral over R (by assumption every element of S is integral over R), by the implication $(i) \Rightarrow (iii)$ of Lemma 3.1.3, $R[s_1]$ is finite over R. Similarly, $R[s_1, s_2] = R[s_1][s_2]$ is finite over $R[s_1]$. Hence, by Lemma 3.1.4, $R[s_1, s_2]$ is finite over R. By continuing this process, we find that $S = R[s_1, s_2, \ldots, s_n]$ is finite over R. ∎

Corollary 3.1.6. *Let $R \subseteq S \subseteq T$ be rings. Suppose that S is integral over R and T is integral over S. Then T is integral over R.*

Proof. Take $t \in T$. Then there exist $s_1, s_2, \ldots, s_n \in S$ such that $t^n + s_1 t^{n-1} + \cdots + s_{n-1}t + s_n = 0$ (since T is integral over S). Let $S' \stackrel{\text{def}}{=} R[s_1, s_2, \ldots, s_n] \subseteq S$. Clearly, $R \subseteq S'$ and S' is integral over R. Then, by Corollary 3.1.5, S' is a finite R-module. The $S'[t]$ is a finite S'-module (since t is integral over S', hence we can use Lemma 3.1.3). Now, we can apply Lemma 3.1.4 for $R \subseteq S' \subseteq S'[t]$ to conclude that $S'[t]$ is a finite R-module.

Using the implication $(ii) \Rightarrow (i)$ of Lemma 3.1.3 with $R \subseteq S'[t] \subseteq T$, we find that t is integral over R. Since t was arbitrary, every element of T is integral over R, i.e., T is integral over R. ∎

Theorem 3.1.7 (Noether Normalization Lemma)**.** *Let R be a finitely generated K-algebra, where K is a field. Then there is a non-negative (!) integer k, $r_1, \ldots, r_k \in R$ such that*

(i) the elements $r_1, r_2, \ldots, r_k$ are algebraically independent over K;

(ii) the R is integral over its subalgebra $K[r_1, r_2, \ldots, r_k]$.

By Corollary 3.1.5, (ii) is equivalent to the statement that R is a finite module over its subalgebra $K[r_1, r_2, \ldots, r_k]$.

Proof. Since R is a finitely generated K-algebra, there exist $u_1, u_2, \ldots, u_n \in R$ such that $R = K[u_1, u_2, \ldots, u_n]$. If $u_1, u_2, \ldots, u_n$ are algebraically independent then we are done. Otherwise there is an

$$0 \neq f(x_1, x_2, \ldots, x_n) = \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in K[x_1, x_2, \ldots, x_n]$$

such that $f(u_1, u_2, \ldots, u_n) = 0$.

Our aim is to find a new generating system $v_1, v_2, \ldots, v_n$ of R such that v_1 is integral over $K[v_2, v_3, \ldots, v_n]$. Set

$$\begin{aligned} v_1 &\stackrel{\text{def}}{=} u_1 \\ v_2 &\stackrel{\text{def}}{=} u_2 - v_1^c \\ v_3 &\stackrel{\text{def}}{=} u_3 - v_1^{c^2} \\ &\vdots \\ v_n &\stackrel{\text{def}}{=} u_n - v_1^{c^{n-1}}. \end{aligned}$$

Here c is a positive integer such that it is greater than any power i_j in f with non-zero coefficient. Since $u_1 = v_1$ and $u_i = v_i + v_1^{c^{i-1}}$ $(i = 2, 3, \ldots, n)$, we have $K[v_1, v_2, \ldots, v_n] = R$. We can substitute $u_1 = v_1$ and $u_i = v_i + v_1^{c^{i-1}}$ into $f(u_1, u_2, \ldots, u_n) = 0$ and expand f in powers of v_1. In this way we get a polynomial of v_1 with coefficients in $K[v_2, v_3, \ldots, v_n]$. If we could cancel by the leading coefficient of this polynomial, we would have a monic polynomial which is zero at v_1. By definition, this means that v_1 is integral over $K[v_2, v_3, \ldots, v_n]$. The leading term is

$$a_{i_1 i_2 \ldots i_n} v_1^{i_1 + i_2 c + \cdots + i_n c^{n-1}},$$

where $(i_n, i_{n-1}, \ldots, i_1)$ is lexicographically the largest in $f(x_1, x_2, \ldots, x_n)$. (This is because of the special choice of c.) The $a_{i_1 i_2 \ldots i_n} \in K$ is non-zero, hence we can cancel by it.

By induction on the number of generators, we may assume that the lemma holds for $T \stackrel{\text{def}}{=} K[v_2, v_3, \ldots, v_n]$, i.e., there exist $w_1, w_2, \ldots, w_m \in T$ such that they are algebraically independent over K and T is a finite $S \stackrel{\text{def}}{=} K[w_1, w_2, \ldots, w_m]$-module. Clearly, $R = T[v_1]$ and we showed that v_1 is integral over T. Thus, by Lemma 3.1.3, $R = T[v_1]$ is a finite T-module. But, since T is a finite S-module, by Lemma 3.1.4, R is a finite S-module. ∎

3.2 Hilbert's Nullstellensatz

Theorem 3.2.1 (Hilbert's Basissatz)**.** *Let K be a field. Then every ideal of $K[x_1, x_2, \ldots, x_n]$ is finitely generated, i.e., finitely generated K-algebras are noetherian.*

Definition 3.2.1. *Let K be a field. Let I be an ideal in $K[x_1, x_2, \ldots, x_n]$. The set*

$$\mathcal{V}(I) \stackrel{\text{def}}{=} \{(a_1, a_2, \ldots, a_n) \in K^n \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

is called the ***common zero locus of*** *I.*

For an arbitrary subset S of $K[x_1, x_2, \ldots, x_n]$, we can define $\mathcal{V}(S)$ in a similar way. If $\langle S \rangle$ is the ideal of $K[x_1, x_2, \ldots, x_n]$ generated by S, then $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$.

Definition 3.2.2. *Let K be a field. Let X be a subset of K^n. The set*

$$\mathcal{Y}(X) \stackrel{\text{def}}{=} \{f \in K[x_1, x_2, \ldots, x_n] \mid f|_X = 0\} \lhd K[x_1, x_2, \ldots, x_n]$$

is called the ***vanishing ideal of*** *X.*

Theorem 3.2.2 (Hilbert's Nullstellensatz)**.** *Suppose that K is an algebraically closed field. Then*

$$\mathcal{Y}(\mathcal{V}(I)) = \sqrt{I},$$

for any ideal I in $K[x_1, x_2, \ldots, x_n]$. Here

$$\sqrt{I} \stackrel{\text{def}}{=} \left\{f \in K[x_1, x_2, \ldots, x_n] \mid f^k \in I \text{ for some positive integer } k\right\}$$

is the ***radical*** *of I.*

Using Hilbert's Basissatz, we have the following equivalent form of Hilbert's Nullstellensatz: if $f \in K[x_1, x_2, \ldots, x_n]$ vanishes on the common zero locus of some polynomials $f_1, f_2, \ldots, f_\ell \in K[x_1, x_2, \ldots, x_n]$, then there exist a positive integer d and $h_1, h_2, \ldots, h_\ell \in K[x_1, x_2, \ldots, x_n]$, such that

$$f^d = \sum_{j=1}^{\ell} h_j f_j.$$

Example 3.2.1. *We give an example that shows that the algebraical closeness of the base field is necessary. Let $K = \mathbb{R}$, $n = 1$ and $I = \langle x^2 + 1 \rangle$. We have $\mathcal{V}(I) = \emptyset$ and $\mathcal{Y}(\mathcal{V}(I)) = \mathbb{R}[x]$. The latter is not equal to $\sqrt{I}$, since $1 \notin \sqrt{I}$.*

For the proof of Hilbert's Nullstellensatz, we need several preparations.

Lemma 3.2.3. *Suppose that S is a subring of the field F, and F is integral over S. Then S is a field.*

Proof. Take any $0 \neq s \in S$. Since F is integral over S, $\frac{1}{s} \in F$ is integral over S. Thus there exist $a_1, a_2, \ldots, a_n \in S$ such that

$$\frac{1}{s^n} + a_1 \frac{1}{s^{n-1}} + \cdots + a_{n-1} \frac{1}{s} + a_n = 0.$$

Multiplying through by s^{n-1} and reordering the equation yields

$$\frac{1}{s} = -a_1 - a_2 s - \cdots - a_{n-1} s^{n-2} - a_n s^{n-1} \in S,$$

which shows that S is a field. ∎

Definition 3.2.3. *Let R be an integral domain. The* ***field of fractions of*** *R, denoted by $Q(R)$, is defined as follows.*

Introduce a relation $\sim$ on $R \times (R \setminus \{0\})$: $(a, s) \sim (b, t)$ if and only if $at - bs = 0$. It is straightforward to show that $\sim$ is an equivalence relation. Denote by $\frac{a}{s}$ the equivalence class of (a, s). Let $Q(R) = \left\{ \frac{a}{s} \mid a \in R, s \in R \setminus \{0\} \right\}$. Define the operations $+ : Q(R) \times Q(R) \to Q(R)$, $\cdot : Q(R) \times Q(R) \to Q(R)$ by

$$\frac{a}{s} + \frac{b}{t} \stackrel{\text{def}}{=} \frac{at + bs}{st} \quad \text{and} \quad \frac{a}{s} \cdot \frac{b}{t} \stackrel{\text{def}}{=} \frac{ab}{st}.$$

It is straightforward to check that these definitions are correct and that $Q(R)$ becomes a commutative ring, and that $Q(R)$ is a field.

Remark. *The map $R \hookrightarrow Q(R)$, $a \mapsto \frac{a}{1}$ is an injective ring homomorphism. Hence, we can write $R \subseteq Q(R)$. The $Q(R)$ is characterized by the following property: it is a field $F \supset R$ such that for all $x \in F$ there exist $a, s \in R$, $s \neq 0$ such that $x = as^{-1}$.*

Proposition 3.2.4. *Let B be an integral domain, which is a finitely generated algebra over a subring A. Suppose that B is algebraic over A, i.e., for every element $b \in B$ there is an $f \in A[x]$ such that $f(b) = 0$. Then there exists an $0 \neq a \in A$ such that $B[a^{-1}] \subseteq Q(B)$ is integral over $A[a^{-1}]$.*

Proof. Since B is a finitely generated algebra over A, there exist $b_1, b_2, \ldots, b_k \in B$ such that $B = A[b_1, b_2, \ldots, b_k]$. By assumption, each b_j is a root of

$$a_0^{(j)} x^{n_j} + a_1^{(j)} x^{n_j - 1} + \cdots \in A[x], \; A \ni a_0^{(j)} \neq 0 \text{ for } j = 1, 2, \ldots, k.$$

Let $a \stackrel{\text{def}}{=} a_0^{(1)} a_0^{(2)} \cdots a_0^{(k)}$. Then for all $j = 1, 2, \ldots, k$, the b_j is the root of a monic polynomial in $A\left[a^{-1}\right][x]$, i.e., b_j is integral over $A\left[a^{-1}\right]$. Then, by induction and Corollary 3.1.6, $B\left[a^{-1}\right] = A\left[a^{-1}\right][b_1, b_2, \ldots, b_k]$ is integral over $A\left[a^{-1}\right]$. ■

Proposition 3.2.5. *If a field F is finitely generated as an algebra over a subfield K, then F is a finite extension of K, i.e.,* $\dim_K(F) < \infty$.

About the lecturer

Mátyás Domokos was born in 1968. He earned his Ph.D. degree in mathematics in 1996. He has been the doctor of the Hungarian Academy of Sciences since 2007. He has been working as a research fellow at the Alfréd Rényi Institute of Mathematics since 1998. He has written more than 40 research papers. His main fields of interest are invariant theory and representation theory.