3. Semi-simple rings

We next consider semi-simple modules in more detail.

**Lemma 3.1.** Let $R$ be a ring, let $M$ be a left $R$-module, and let $\{S_i\}_{i \in I}$ be a finite family of simple submodules the union of which generates $M$. Then there exists a subset $J \subset I$ such that $M = \bigoplus_{i \in J} S_i$.

**Proof.** We consider a subset $J \subset I$ which is maximal among subsets with the property that the sum of submodules $\sum_{j \in J} S_j \subset M$ is direct. Now, if $i \in I \setminus J$, then $S_i \cap \sum_{j \in J} S_j \neq \{0\}$ or else $J$ would not be maximal. Since $S_i$ is simple, we conclude that $S_i$ is contained in the submodule $\sum_{j \in J} S_j \subset M$. It follows that this submodule is all of $M$. This completes the proof. \(\square\)

**Proposition 3.2.** Let $R$ be a ring and let $M$ be a semi-simple left $R$-module.

(i) Let $Q$ be a left $R$-module and let $p: M \to Q$ be a surjective $R$-linear map. Then $Q$ is semi-simple and there exists an $R$-linear map $s: Q \to M$ such that $p \circ s: Q \to Q$ is the identity map.

(ii) Let $N$ be a left $R$-module and let $i: N \to M$ be an injective $R$-linear map. Then $N$ is semi-simple and there exists an $R$-linear map $r: M \to N$ such that $r \circ i: N \to N$ is the identity map.

**Proof.** (i) We write $M = \bigoplus_{i \in I} S_i$ as a finite direct sum of simple submodules. Let $J \subset I$ be the subset of indices $i$ such that $p(S_i)$ is non-zero. By Lemma 3.1, we can find a subset $K \subset J$ such that $\bigoplus_{i \in K} p(S_i) = Q$. Let $j: \bigoplus_{i \in K} S_i \to M$ be the canonical inclusion. Then $p \circ j$ is an isomorphism which shows that $Q$ is semi-simple. Moreover, the composite map $s = j \circ (p \circ j)^{-1}: Q \to M$ has the desired property that $p \circ s$ is the identity map of $Q$.

(ii) It follows from (i) that there exists a submodule $P \subset M$ such that the composition $P \to M \to M/N$ of the canonical inclusion and the canonical projection is an isomorphism. Now, if $q: M \to M/P$ is the projection onto the quotient by $P$, then $q \circ i: N \to M/P$ is an isomorphism. This shows that $N$ is semi-simple and that the map $r = (q \circ i)^{-1} \circ q: M \to N$ satisfies that $r \circ i = \mathrm{id}_N$. \(\square\)

Let $M$ be a semi-simple left $R$-module and let $\Lambda$ be the set of isomorphism classes of simple left $R$-modules. If the simple submodule $S \subset M$ belongs to the class $\lambda \in \Lambda$, we say that $S$ has type $\lambda$. We prove that semi-simple left $R$-modules admit the following canonical isotypic decomposition.

**Proposition 3.3.** Let $R$ be a ring.

(i) Let $M$ be a semi-simple left $R$-module, and let $M_\lambda \subset M$ be the submodule generated by the union of all simple submodules of type $\lambda$. Then

$$M = \bigoplus_{\lambda \in \Lambda} M_\lambda$$

and $M_\lambda$ is a direct sum of simple submodules of type $\lambda$.

(ii) Let $M$ and $N$ be semi-simple left $R$-modules and let $f: M \to N$ be an $R$-linear map. Then $f(M_\lambda) \subset N_\lambda$.

**Proof.** (i) Since $M$ is semi-simple, we can write $M = \bigoplus_{i \in I} S_i$ as a direct sum of simple submodules. Let $M'_\lambda = \bigoplus_{i \in I_\lambda} S_i$ where $I_\lambda \subset I$ is the subset of $i \in I$ such that $S_i$ is of type $\lambda$. We have $M = \bigoplus_{\lambda \in \Lambda} M'_\lambda$ and $M'_\lambda \subset M_\lambda$. We must prove...
that $M'_i = M_{i'}$. So let $S \subset M$ be a simple submodule of type $\lambda$ and let $i \in I$. The composition $f_i : S \to M \to S_i$ of the canonical inclusion and the canonical projection is an $R$-linear map. Since $S$ and $S_i$ are both simple left $R$-modules, the map $f_i$ is either zero or an isomorphism. If it is an isomorphism, we have $i \in I_\lambda$ by definition. This shows that $S \subset M'_i$, and hence, $M_\lambda \subset M'_{i'}$ as desired.

(ii) Let $S \subset M$ be a simple submodule of type $\lambda$. Then $f(S) \subset N$ is either zero or a simple submodule of type $\lambda$. Therefore, $f(M_\lambda) \subset N_\lambda$ as stated. □

Definition 3.4. (i) The ring $R$ is semi-simple if it semi-simple as a left module over itself.

(ii) The ring $R$ is simple if it is semi-simple and if it has exactly one type of simple modules.

Theorem 3.5. Let $R$ be a semi-simple ring and let $R = \bigoplus_{\lambda \in \Lambda} R_\lambda$ be the isotypic decomposition of $R$ as a left $R$-module.

(i) For every $\lambda \in \Lambda$, the left ideal $R_\lambda \subset R$ is non-zero. In particular, $\Lambda$ is a finite set.

(ii) For every $\lambda \in \Lambda$, the left ideal $R_\lambda \subset R$ is also a right ideal.

(iii) Let $a, b \in R$ and write $a = \sum_{\lambda \in \Lambda} a_\lambda$ and $b = \sum_{\lambda \in \Lambda} b_\lambda$ with $a_\lambda, b_\lambda \in R_\lambda$. Then $ab = \sum_{\lambda \in \Lambda} a_\lambda b_\lambda$ and $a_\lambda b_\lambda \in R_\lambda$.

(iv) For every $\lambda \in \Lambda$, $R_\lambda$ is a ring with respect to the restriction of the multiplication on $R$ and the identity element is the unique element $e_\lambda \in R_\lambda$ such that $\sum_\lambda e_\lambda = 1$.

(v) For every $\lambda \in \Lambda$, the ring $R_\lambda$ is simple.

Proof. (i) Let $S$ be a simple left $R$-module of type $\lambda$. We choose a non-zero element $x \in S$ and consider the $R$-linear map $p : R \to S$ defined by $p(a) = a \cdot x$. The image $p(S) \subset S$, which is a non-zero submodule of a simple left $R$-module, is necessarily all of $S$, so $p$ is surjective. We conclude from Proposition 3.2 that there exists an $R$-linear map $s : S \to R$ such that $p \circ s = \text{id}_S$. But then $s(S) \subset R$ is a simple submodule of type $\lambda$.

(ii) Let $a \in R$ and let $\rho_a : R \to R$ be the map $\rho_a(b) = ba$ defined by right multiplication by $a$. It is an $R$-linear map from the left $R$-module $R$ to itself. By Proposition 3.3 (ii), we conclude that $\rho_a(R_\lambda) \subset R_\lambda$ which is precisely the statement that $R_\lambda \subset R$ is a right ideal.

(iii) Since $R_\mu \subset R$ is a left ideal, we have $a_\lambda b_\mu \in R_\mu$, and since $R_\lambda \subset R$ is a right ideal, we have $a_\lambda b_\mu \in R_\lambda$. It follows that $a_\lambda b_\mu \in R_\lambda \cap R_\mu$ which is equal to $R_\mu$ and $\{0\}$, respectively, as $\lambda = \mu$ and $\lambda \neq \mu$.

(iv) We have already proved in (iii) that the multiplication on $R$ restricts to a multiplication on $R_\lambda$. Now, for all $a_\lambda \in R_\lambda$, we have

$$a_\lambda = a_\lambda \cdot 1 = a_\lambda \cdot \left(\sum_{\mu \in \Lambda} e_\mu\right) = \sum_{\mu \in \Lambda} a_\lambda \cdot e_\mu = a_\lambda \cdot e_\lambda$$

and the identity $a_\lambda = e_\lambda \cdot a_\lambda$ is proved analogously. It follows that $R_\lambda$ is a ring.

(v) Let $S_\lambda$ be a simple left $R$-module of type $\lambda$. Since $R_\lambda \subset R$, the left multiplication of $R$ on $S_\lambda$ defines a left multiplication of $R_\lambda$ on $S_\lambda$. To prove that this defines a left $R_\lambda$-module structure on $S_\lambda$, we must show that $e_\lambda \cdot x = x$, for all $x \in S_\lambda$. We have just proved that $e_\lambda \cdot y = y$, for all $y \in R_\lambda$. Moreover, by Proposition 3.3 (i), we can find an injective $R$-linear map $f_\lambda : S_\lambda \to R_\lambda$. Since

$$f_\lambda(e_\lambda \cdot x) = e_\lambda \cdot f_\lambda(x) = f_\lambda(x),$$
we conclude that \( e_\lambda \cdot x = x \), for all \( x \in S_\lambda \), as desired. We further note that \( S_\lambda \) is a simple left \( R_\lambda \)-module. Indeed, it follows from (iii) that the subset \( N \subseteq S_\lambda \) is an \( R \)-submodule if and only if it is an \( R_\lambda \)-submodule. Finally, by Proposition 3.3 (i), the left \( R \)-module \( R_\lambda \) is isomorphic to a direct sum \( S_{\lambda,1} + \cdots + S_{\lambda,r} \) of simple submodules, all of which are isomorphic to the simple left \( R \)-module \( S_\lambda \). Therefore, as a left \( R_\lambda \)-module, \( R_\lambda \) is isomorphic to the direct sum \( S_{\lambda,1} + \cdots + S_{\lambda,r} \) of submodules, all of which are isomorphic to the simple left \( R_\lambda \)-module \( S_\lambda \). This shows that \( R_\lambda \) is a semi-simple ring, and we conclude from (i) that every simple left \( R_\lambda \)-module is isomorphic to \( S_\lambda \). So \( R_\lambda \) is a simple ring.

Remark 3.6. The inclusion map \( i_\lambda : R_\lambda \to R \) is not a ring homomorphism unless \( R = R_\lambda \). Indeed, the map \( i_\lambda \) takes the multiplicative identity element \( e_\lambda \in R_\lambda \) to the element \( e_\lambda \in R \) which is not equal to the multiplicative identity element \( 1 \in R \) unless \( R = R_\lambda \). However, the projection map

\[
p_\lambda : R \to R_\lambda
\]

that takes \( a = \sum_{\mu \in \Lambda} a_\mu \) with \( a_\mu \in R_\mu \) to \( a_\lambda \) is a ring homomorphism. In general, the product ring of the family of rings \( \{ R_\lambda : \lambda \in \Lambda \} \) is defined to be the set

\[
\prod_{\lambda \in \Lambda} R_\lambda = \{ (a_\lambda)_{\lambda \in \Lambda} \mid a_\lambda \in R_\lambda \}
\]

with componentwise addition and multiplication. The multiplicative identity element in the product ring is the tuple \((e_\lambda)_{\lambda \in \Lambda}\) where \( e_\lambda \in R_\lambda \) is the multiplicative unit element. We may now restate Theorem 3.5 (ii)–(v) as saying that the map

\[
p : R \to \prod_{\lambda \in \Lambda} R_\lambda
\]

defined by \( p(a) = (p_\lambda(a))_{\lambda \in \Lambda} \) is an isomorphism of rings, and that each of the component rings \( R_\lambda \) is a simple ring.

We next prove the following structure theorem for simple rings. We recall from Schur’s lemma that the endomorphism ring of a simple module is a division ring.

Theorem 3.7. The following statements holds.

(i) Let \( D \) be a division ring and let \( R = M_n(D) \) be the ring of \( n \times n \)-matrices. Then \( R \) is a simple ring with the left \( R \)-module \( S = M_{n,1}(D) \) of column \( n \)-vectors as its simple module, and the map

\[
\rho : D \to \text{End}_R(S)^{\text{op}}
\]

defined by \( \rho(a)(x) = xa \) is a ring isomorphism.

(ii) Let \( R \) be a simple ring and let \( S \) be a simple left \( R \)-module. Then \( S \) is a finite dimensional right vector space over the division ring \( D = \text{End}_R(S)^{\text{op}} \) opposite of the ring of \( R \)-linear endomorphisms of \( S \), and the map

\[
\lambda : R \to \text{End}_D(S)
\]

defined by \( \lambda(a)(x) = ax \) is a ring isomorphism.

Proof. (i) We have proved in Lemma 2.12 that \( S \) is a simple \( R \)-module. Now, let \( e_i \in M_{1,n}(D) \) be the row vector whose \( i \)th entry is 1 and whose remaining entries are 0. Then the map \( f : S \oplus \cdots \oplus S \to R \), where there are \( n \) summands \( S \), defined by \( f(v_1, \ldots, v_n) = v_1 e_1 + \cdots + v_n e_n \) is an isomorphism of left \( R \)-modules. Indeed, in the \( n \times n \)-matrix \( v_i e_i \), the \( i \)th column is \( v_i \) and the remaining columns are zero.
This shows that \( R \) is a semi-simple ring. By Theorem 3.5 (i), we conclude that every simple left \( R \)-module is isomorphic to \( S \). Hence, the ring \( R \) is simple.

It is readily verified that the map \( \rho \) is a ring homomorphism. Now, the kernel of \( \rho \) is a two-sided ideal in the division ring \( D \), and hence, is either zero or all of \( D \). But \( \rho(1) = \text{id}_S \) is not zero, so the kernel is zero, and hence the map \( \rho \) is injective.

It remains to show that \( \rho \) is surjective. So let \( f: S \rightarrow S \) be an \( R \)-linear map. We must show that there exists \( a \in D \) such that for all \( y \in S \), \( f(y) = ya \). To this end, we fix a non-zero element \( x \in S \) and choose a matrix \( P \in R \) such that \( Px = x \) and such that \( PS = xD \subset S \). Since \( f \) is \( R \)-linear, we have

\[
f(x) = f(Px) = Pf(x) \in xD
\]

which shows that \( f(x) = xa \) with \( a \in D \). Now, given any \( y \in S \), we can find a matrix \( A \in R \) such that \( Ax = y \). Again, since \( f \) is \( R \)-linear, we have

\[
f(y) = f(Ax) = Af(x) = Axa = ya
\]

as desired. This shows that \( \rho \) is surjective, and hence, an isomorphism.

(ii) Since \( R \) is a simple ring with simple left \( R \)-module \( S \), there exists an isomorphism of left \( R \)-modules \( f: S^n \rightarrow R \) from the direct sum of finite number \( n \) copies of \( S \) onto \( R \). We now have ring isomorphisms

\[
R^{op} \cong \text{End}_R(R) \cong \text{End}_R(S^n) \cong M_n(\text{End}_R(S)) = M_n(D^{op})
\]

where the left-hand isomorphism is given by Remark 2.6, the middle isomorphism is induced by the chosen isomorphism \( f \), and the right-hand isomorphism takes the endomorphism \( g \) to the matrix of endomorphisms \( (g_{ij}) \) with the endomorphism \( g_{ij} \) defined to be the composition \( g_{ij} = p_i \circ g \circ i_j \) of the inclusion \( i_j: S \rightarrow S^n \) of the \( j \)th summand, the endomorphism \( g: S^n \rightarrow S^n \), and the projection \( p_i: S^n \rightarrow S \) on the \( i \)th summand. It follows that we have a ring isomorphism

\[
R \cong M_n(D^{op})^{op} \cong M_n((D^{op})^{op}) = M_n(D)
\]

given by the composition of the isomorphism above and the isomorphism that takes the matrix \( A \) to its transpose \( ^tA \). This shows that the simple ring \( R \) is isomorphic to the simple ring \( M_n(D) \) we considered in (i). Therefore, it suffices to show that the map \( \lambda \) is an isomorphism in this case. But this is precisely the statement of Corollary 2.5. \( \square \)

**Exercise 3.8.** Let \( D \) be a division ring, let \( R = M_n(D) \), and let \( S = M_{n,1}(D) \). We view \( S \) as a left \( R \)-module and as a right \( D \)-vector space.

1. Let \( x \in S \) be a non-zero vector. Show that there exists a matrix \( P \in R \) such that \( PS = xD \subset S \). (Hint: Try \( x = e_1 \) first.)

2. Let \( x, y \in S \) be non-zero vectors. Show that there exists a matrix \( A \in R \) such that \( Ax = y \).

**Remark 3.9.** The center of a ring \( R \) is the subring \( Z(R) \subset R \) of all elements \( a \in R \) with the property that for all \( b \in R \), \( ab = ba \); it is a commutative ring. The center \( k = Z(D) \) of the division ring \( D \) clearly is a field, and it is not difficult to show that also \( Z(M_n(D)) = k \). It is possible for a division ring \( D \) to be of infinite dimension over the center \( k \). However, one can show that if \( D \) is of finite dimension \( d \) over \( k \), then it is not difficult to show that also \( Z(M_n(D)) = k \). It is possible for a division ring \( D \) to be of infinite dimension over the center \( k \). However, one can show that if \( D \) is of finite dimension \( d \) over \( k \), then \( d = m^2 \) is a square and every maximal subfield \( E \subset D \) has dimension \( m \) over \( k \). For example, the center of the division ring of quaternions \( \mathbb{H} \) is the field of real numbers \( \mathbb{R} \) and the complex numbers \( \mathbb{C} \subset \mathbb{H} \) is a maximal subfield.
It is high time that we see an example of a semi-simple ring. In general, if $k$ is a commutative ring and if $G$ is a group, the group ring $k[G]$ is defined to be the free $k$-module with basis $G$ and with multiplication

$$
(\sum_{g \in G} a_g g) \cdot (\sum_{g \in G} b_g g) = \sum_{h, k \in G} (\sum_{h_k = g} a_h b_k) g.
$$

We note that $G \subset k[G]$ as the set of basis elements; the unit element $e \in G$ is also the multiplicative unit element in the ring $k[G]$. Moreover, the map $\eta: k \to k[G]$ defined by $\eta(a) = a \cdot e$ is ring homomorphism. If $M$ is a left $k[G]$-module, we also say that $M$ is a $k$-linear representation of the group $G$.

Let $k$ be a field and let $\eta: \mathbb{Z} \to k$ be the unique ring homomorphism. We define the characteristic of $k$ to be the unique non-negative integer $\text{char}(k)$ such that $\ker(\eta) = \text{char}(k)\mathbb{Z}$. For example, the fields $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ have characteristic zero while, for every prime number $p$, the field $\mathbb{Z}/p\mathbb{Z}$ has characteristic $p$.

**Exercise 3.10.** Let $k$ be a field. Show that $\text{char}(k)$ is either zero or a prime number, and that every integer $n$ not divisible by $\text{char}(k)$ is invertible in $k$.

**Theorem 3.11** (Maschke’s theorem). Let $k$ be a field and let $G$ be finite group whose order is not divisible by the characteristic of $k$. Then the group ring $k[G]$ is a semi-simple ring.

**Proof.** We show that every left $k[G]$-module $M$ of finite dimension $m$ over $k$ is a semi-simple left $k[G]$-module. The proof is by induction on $m$; the basic case $m = 1$ follows from Example 2.11, since a left $k[G]$-module of dimension 1 over $k$ is simple as a left $k$-module, and hence, also as a left $k[G]$-module. So we let $M$ be a left $k[G]$-module of dimension $m > 1$ over $k$ and assume, inductively, that every left $k[G]$-module of smaller dimension is semi-simple. We must show that $M$ is semi-simple. If $M$ is simple, we are done. If $M$ is not simple, there exists a non-zero proper submodule $N \subset M$. We let $i: N \to M$ be the inclusion and choose a $k$-linear map $\sigma: M \to N$ such that $\sigma \circ i = \text{id}_N$. The map $\sigma$ is not necessarily $k[G]$-linear. However, we claim that the map $s: M \to N$ defined by

$$
s(x) = \frac{1}{|G|} \sum_{g \in G} g \sigma(g^{-1}x)
$$

is $k[G]$-linear and satisfies $s \circ i = \text{id}_N$. Indeed, $s$ is $k$-linear and if $h \in G$, then

$$
s(hx) = \frac{1}{|G|} \sum_{g \in G} g \sigma(g^{-1}hx) = \frac{1}{|G|} \sum_{g \in G} hh^{-1}g \sigma(g^{-1}hx)
$$

$$
= \frac{1}{|G|} \sum_{kk \in G} kk \sigma(k^{-1}x) = hs(x)
$$

which shows that $s$ is $k[G]$-linear. Moreover, we have

$$
(s \circ i)(x) = \frac{1}{|G|} \sum_{g \in G} g \sigma(g^{-1}i(x)) = \frac{1}{|G|} \sum_{g \in G} g \sigma(i(g^{-1}x))
$$

$$
= \frac{1}{|G|} \sum_{g \in G} gg^{-1}x = x
$$

which shows that $s \circ i = \text{id}_N$. This proves the claim. Now, let $P$ be the kernel of $s$. The claim shows that $M$ is equal to the direct sum of the submodule $N, P \subset M$. 


But $N$ and $P$ both have dimension less than $m$ over $k$, and hence, are semi-simple by the inductive hypothesis. This shows that $M$ is semi-simple as desired. \hfill $\Box$

**Example 3.12 (Cyclic groups).** To illustrate the theory above, we determine the structure of the group rings $\mathbb{C}[C_n]$, $\mathbb{R}[C_n]$, and $\mathbb{Q}[C_n]$, where $C_n$ is the cyclic group of order $n$. Theorem 3.11 shows that the three rings are semi-simple rings, and their structure are given by Theorems 3.5 and 3.7 once we identify their isomorphism classes of simple modules; we proceed to do so. We fix choices of a generator $g \in C_n$ and of a primitive $n$th root of unity $\zeta_n \in \mathbb{C}$.

We first consider the complex group ring $\mathbb{C}[C_n]$. For every $0 \leq k < n$, we define the left $\mathbb{C}[C_n]$-module $\mathbb{C}(\zeta_n^k)$ to be the sub-$\mathbb{C}$-vector space $\mathbb{C}(\zeta_n^k) \subset \mathbb{C}$ spanned by the elements $\zeta_n^k$ with $0 \leq i < n$ and with the module structure defined by

$$\left(\sum_{i=0}^{n-1} a_i g^i\right) \cdot z = \sum_{i=0}^{n-1} a_i \zeta_n^{ki} z.$$  

The left $\mathbb{C}[C_n]$-module $\mathbb{C}(\zeta_n^k)$ is simple. For as a $\mathbb{C}$-vector space, $\mathbb{C}(\zeta_n^k) = \mathbb{C}$, and therefore has no non-trivial proper submodules. Suppose that $f: \mathbb{C}(\zeta_n^k) \to \mathbb{C}(\zeta_n^l)$ is a $\mathbb{C}[C_n]$-linear isomorphism. Then we have

$$\zeta_n^k f(1) = f(\zeta_n^k) = f(g \cdot 1) = g \cdot f(1) = \zeta_n^l f(1),$$

where the first and third equalities follows from $\mathbb{C}[C_n]$-linearity. Since $f(1) \neq 0$, we conclude that $k = l$. So the $n$ simple left $\mathbb{C}[C_n]$-modules $\mathbb{C}(\zeta_n^k)$, $0 \leq k < n$, are pairwise non-isomorphic. Therefore, Theorem 3.5 (i) implies that

$$\mathbb{C}[C_n] = \bigoplus_{k=0}^{n-1} \mathbb{C}(\zeta_n^k)$$

as a left $\mathbb{C}[C_n]$-module. The endomorphism ring $\text{End}_{\mathbb{C}[C_n]}(\mathbb{C}(\zeta_n^k))$ is isomorphic to the field $\mathbb{C}$ for all $0 \leq k < n$.

We next consider the real group ring $\mathbb{R}[C_n]$. Again, for $0 \leq k < n$, we define the left $\mathbb{R}[C_n]$-module $\mathbb{R}(\zeta_n^k)$ to be the sub-$\mathbb{R}$-vector space $\mathbb{R}(\zeta_n^k) \subset \mathbb{C}$ spanned by the elements $\zeta_n^k$ with $0 \leq i < n$ and with the module structure defined by

$$\left(\sum_{i=0}^{n-1} a_i g^i\right) \cdot z = \sum_{i=0}^{n-1} a_i \zeta_n^{ki} z.$$  

The left $\mathbb{R}[C_n]$-module $\mathbb{R}(\zeta_n^k)$ is simple. For given two elements $z, z' \in \mathbb{R}(\zeta_n^k)$, there exists $\omega \in \mathbb{R}[C_n]$ with $\omega \cdot z = z'$. The dimension of $\mathbb{R}(\zeta_n^k)$ as an $\mathbb{R}$-vector space is either 1 or 2 according as $\zeta_n^k \in \mathbb{R}$ or $\zeta_n^k \not\in \mathbb{R}$. Moreover, we find that the left $\mathbb{R}[C_n]$-modules $\mathbb{R}(\zeta_n^k)$ and $\mathbb{R}(\zeta_n^l)$ are isomorphic if and only if the complex numbers $\zeta_n^k$ and $\zeta_n^l$ are conjugate. Again, from Theorem 3.5 (i), we conclude that

$$\mathbb{R}[C_n] = \bigoplus_{k=0}^{[n/2]} \mathbb{R}(\zeta_n^k)$$

as a left $\mathbb{R}[C_n]$-module. Here $[n/2]$ is the largest integer less than or equal to $n/2$. The endomorphism ring $\text{End}_{\mathbb{R}[C_n]}(\mathbb{R}(\zeta_n^k))$ is isomorphic to $\mathbb{R}$, if $k = 0$ or $k = n/2$, and to $\mathbb{C}$, otherwise.
Finally, we consider the rational group ring $\mathbb{Q}[C_n]$. For all $0 \leq k < n$, we define the left $\mathbb{Q}[C_n]$-module $\mathbb{Q}(\zeta_n^k)$ to be the sub-$\mathbb{Q}$-vector space $\mathbb{Q}(\zeta_n^k) \subset \mathbb{C}$ spanned by the elements $\zeta_n^{ki}$ with $0 \leq i < n$ and with the module structure defined by

$$\left( \sum_{i=0}^{n-1} a_i g^i \right) \cdot z = \sum_{i=0}^{n-1} a_i \zeta_n^{ki} z.$$ 

Again, $\mathbb{Q}(\zeta_n^k)$ is a simple left $\mathbb{Q}[C_n]$-module, since given $z, z' \in \mathbb{Q}(\zeta_n^k)$, there exists an element $\omega \in \mathbb{Q}[C_n]$ with $\omega \cdot z = z'$. Suppose that

$$\{ \zeta_n^{ki} \mid 0 \leq i < n \} = \{ \zeta_n^i \mid 0 \leq i < n \} \subset \mathbb{C}.$$ 

Then we may define a $\mathbb{Q}[C_n]$-linear isomorphism

$$f : \mathbb{Q}(\zeta_n^k) \to \mathbb{Q}(\zeta_n^l)$$

to be the unique $\mathbb{Q}$-linear map that takes $\zeta_n^{ki}$ to $\zeta_n^{li}$, for all $0 \leq i < n$. Suppose that the set $\{ \zeta_n^i \mid 0 \leq i < n \}$ has $d$ elements. Then $d$ divides $n$ and

$$\{ \zeta_n^{ki} \mid 0 \leq i < n \} = \{ \zeta_n^i \mid 0 \leq i < d \}$$

with $\zeta_d \in \mathbb{C}$ a primitive $d$th root of unity. Let $\mathbb{Q}(\zeta_d) \subset \mathbb{C}$ be the left $\mathbb{Q}(\zeta_d)$-module defined by the sub-$\mathbb{Q}$-vector space $\mathbb{Q}(\zeta_d) \subset \mathbb{C}$ spanned by the $\zeta_d^i$ with $0 \leq i < d$ and with the module structure

$$\left( \sum_{i=0}^{d-1} z_i g^i \right) \cdot z = \sum_{i=0}^{d-1} a_i \zeta_d^i z.$$ 

Then we define a $\mathbb{Q}[C_n]$-linear isomorphism

$$f : \mathbb{Q}(\zeta_d) \to \mathbb{Q}(\zeta_n^k)$$

to be the unique $\mathbb{Q}$-linear map that takes $\zeta_d^i$ to $\zeta_n^{ki}$. It is not difficult to show that the dimension of $\mathbb{Q}(\zeta_d)$ as a $\mathbb{Q}$-vector space is equal to the number $\varphi(d)$ of the integers $1 \leq i \leq d$ that are prime to $d$. Moreover, since

$$\sum_{d \mid n} \varphi(d) = n$$

we conclude from Theorem 3.5 (i) that these represent all isomorphism classes of simple left $\mathbb{Q}[C_n]$-modules. Therefore,

$$\mathbb{Q}[C_n] = \bigoplus_{d \mid n} \mathbb{Q}(\zeta_d)$$

as a left $\mathbb{Q}[C_n]$-module. We note that $\mathbb{Q}(\zeta_d) \subset \mathbb{C}$ is a subfield, the $d$th cyclotomic field over $\mathbb{Q}$. The endomorphism ring $\text{End}_{\mathbb{Q}[C_n]}(\mathbb{Q}(\zeta_d))^{\text{op}}$ is isomorphic to the field $\mathbb{Q}(\zeta_d)$ for every divisor $d$ of $n$.

**Remark 3.13 (Modular representation theory).** If the characteristic of the field $k$ divides the order of the group $G$, then the group ring $k[G]$ is not semi-simple, and it is a very difficult problem to understand the structure of this ring. For example, if $F_p$ is the field with $p$ elements and $\mathcal{S}_p$ is the symmetric group on $p$ letters, then the structure of the ring $F_p[\mathcal{S}_p]$ is only understood for a few primes $p$. 