3. Semisimple rings

We next consider semisimple 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 with sum $M = \sum_{i \in I} S_i$. Then there exists a subset $J \subset I$ such that $M = \bigoplus_{j \in J} S_j$.*

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 $i \in I \smallsetminus J$, then $S_i \cap \sum_{j \in J} S_j \neq \{\mathbf{0}\}$ or else J would not be maximal. Since S_i is simple, we conclude that $S_i \cap \sum_{j \in J} S_j = S_i$. It follows that $\sum_{j \in J} S_j = M$ as desired. □

PROPOSITION 3.2. *Let R be a ring and let M be a semisimple left R-module.*

(i) *Let Q be a left R-module and let $p \colon M \to Q$ be a surjective R-linear map. Then Q is semisimple and there exists an R-linear map $s \colon Q \to M$ such that $p \circ s \colon Q \to Q$ is the identity map.*
(ii) *Let N be a left R-module and let $i \colon N \to M$ be an injective R-linear map. Then N is semisimple and there exists an R-linear map $r \colon M \to N$ such that $r \circ i \colon N \to N$ 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 $p(S_i) \neq \{\mathbf{0}\}$. By Lemma 3.1, we can find a subset $K \subset J$ such that $\bigoplus_{i \in K} p(S_i) = Q$. Let $j \colon \bigoplus_{i \in K} S_i \to M$ be the canonical inclusion. Then $p \circ j$ is an isomorphism which shows that Q is semisimple. Moreover, the composite map $s = j \circ (p \circ j)^{-1} \colon Q \to M$ has the desired property that $p \circ s = \mathrm{id}_Q$.

(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 $q \colon M \to M/P$ is the projection onto the quotient by P, then $q \circ i \colon N \to M/P$ is an isomorphism. This shows that N is semisimple and that the map $r = (q \circ i)^{-1} \circ q \colon M \to N$ satisfies that $r \circ i = \mathrm{id}_N$. □

We fix a ring R and define $\Lambda(R)$ be the set of isomorphism classes of the simple left R-modules that are of the form $S = R/I$ with $I \subset R$ a left ideal.[1] Let S be any simple left R-module. To define the *type* of S, we choose a non-zero element $\boldsymbol{x} \in S$ and consider the R-linear map $p \colon R \to S$ given by $p(a) = a\boldsymbol{x}$. It is surjective, since S is simple, and hence, induces an isomorphism $\bar{p} \colon R/I \to S$, where $I = \mathrm{Ann}_R(\boldsymbol{x})$ is the kernel of p. We now define the type of S to be the isomorphism class $\lambda \in \Lambda(R)$ of R/I. (Exercise: Show that the type of S is well-defined.) We prove that semisimple left R-modules admit the following canonical *isotypic decomposition.*

PROPOSITION 3.3. *Let R be a ring.*

(i) *Let M be a semisimple left R-module, and let $M_\lambda \subset M$ be the submodule given by the sum of all simple submodules of type $\lambda \in \Lambda(R)$. Then*

$$M = \bigoplus_{\lambda \in \Lambda(R)} M_\lambda$$

and M_λ is a direct sum of simple submodules of type λ. In addition, M_λ is zero for all but finitely many $\lambda \in \Lambda(R)$.

[1] It is not possible, within standard ZFC set theory, to speak of the isomorphism classes of all simple R-modules or the set thereof. This is the reason that we define $\Lambda(R)$ in this way.

(ii) *Let M and N be semisimple left R-modules and let $f\colon M \to N$ be an R-linear map. Then for every $\lambda \in \Lambda(R)$, $f(M_\lambda) \subset N_\lambda$.*

PROOF. We first prove (i) Since M is semisimple, we can write M as a finite direct sum $M = \bigoplus_{i \in I} S_i$ of simple submodules. If $M'_\lambda = \bigoplus_{i \in I_\lambda} S_i$, where $I_\lambda \subset I$ is the subset of $i \in I$ such that S_i is of type λ, then $M = \bigoplus_{\lambda \in \Lambda(R)} M'_\lambda$ and $M'_\lambda \subset M_\lambda$. We must show that $M_\lambda \subset M'_\lambda$. So let $S \subset M$ be a simple submodule of type λ and let $i \in I$. The composition $f_i\colon S \to M \to S_i$ of the canonical inclusion and the canonical projection is an R-linear map, and 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, then we have $i \in I_\lambda$, which shows that $S \subset M'_\lambda$, and hence, $M_\lambda \subset M'_\lambda$ as desired. Finally, the finite set I is a the disjoint union of the subsets I_λ with $\lambda \in \Lambda(R)$, and hence, all but finitely many of these subsets must be empty.

Next, to prove (ii), we let $S \subset M$ be a simple submodule of type λ. Since S is simple, either $f(S) \subset N$ is zero or else $f|_S\colon S \to f(S)$ is an isomorphism of left R-modules. Therefore, $f(M_\lambda) \subset N_\lambda$ as stated. □

DEFINITION 3.4. A ring R is *semisimple* if it semisimple as a left module over itself. A ring R is *simple* if it is semisimple and if it has exactly one type of simple modules.

We proceed to prove two theorems that, taken together, constitute a structure theorem for semisimple rings.

THEOREM 3.5. *Let R be a semisimple ring and let $R = \bigoplus_{\lambda \in \Lambda(R)} R_\lambda$ be the isotypic decomposition of R as a left R-module.*

(i) *For every $\lambda \in \Lambda(R)$, the left ideal $R_\lambda \subset R$ is non-zero. In particular, the set of types $\Lambda(R)$ is finite.*
(ii) *For every $\lambda \in \Lambda(R)$, the left ideal $R_\lambda \subset R$ is also a right ideal.*
(iii) *Let $a, b \in R$ and write $a = \sum_{\lambda \in \Lambda(R)} a_\lambda$ and $b = \sum_{\lambda \in \Lambda(R)} b_\lambda$ with $a_\lambda, b_\lambda \in R_\lambda$. Then $ab = \sum_{\lambda \in \Lambda(R)} a_\lambda b_\lambda$ and $a_\lambda b_\lambda \in R_\lambda$.*
(iv) *For every $\lambda \in \Lambda(R)$, the subset $R_\lambda \subset R$ is a ring with respect to the restriction of the addition and multiplication on R, and the identity element is the unique element $e_\lambda \in R_\lambda$ such that $\sum_{\lambda \in \Lambda(R)} e_\lambda = 1$.*
(v) *For every $\lambda \in \Lambda(R)$, the ring R_λ is simple.*

PROOF. (i) Let S be a simple left R-module of type λ. We choose a non-zero element $\boldsymbol{x} \in S$ and consider again the surjective R-linear map $p\colon R \to S$ defined by $p(a) = a\boldsymbol{x}$. By Proposition 3.2 there exists an R-linear map $s\colon S \to R$ such that $p \circ s = \mathrm{id}_S$. But then $s(S) \subset R$ is a simple submodule of type λ, and hence, R_λ is non-zero. Finally, it follows from Proposition 3.3 (i) that $\Lambda(R)$ is a finite set.

(ii) Let $a \in R$ and let $\rho_a\colon R \to R$ 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 $a_\lambda b_\mu \in R_\lambda$. This shows that $a_\lambda b_\mu \in R_\lambda \cap R_\mu$, and since

$$R_\lambda \cap R_\mu = \begin{cases} R_\lambda & \text{if } \lambda = \mu, \\ \{\mathbf{0}\} & \text{if } \lambda \neq \mu, \end{cases}$$

the claim follows.

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

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

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

(v) Let S_λ be a simple left R-module of type λ. Since $R_\lambda \subset R$, the left multiplication by R on S_λ defines a left multiplication by R_λ on S_λ. To prove that this defines a left R_λ-module structure on S_λ, we must show that $e_\lambda \cdot \boldsymbol{x} = \boldsymbol{x}$, for all $\boldsymbol{x} \in S_\lambda$. 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 $f_\lambda \colon S_\lambda \to R_\lambda$. Since

$$f_\lambda(e_\lambda \cdot x) = e_\lambda \cdot f_\lambda(x) = f_\lambda(x),$$

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

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

$$p_\lambda \colon R \to R_\lambda$$

that takes $a = \sum_{\mu \in \Lambda} a_\mu$ with $a_\mu \in R_\mu$ to a_λ is a ring homomorphism. In general, the *product ring* of the family of rings $(R_\lambda)_{\lambda \in \Lambda}$ is the 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 identity element in the product ring is the tuple $(e_\lambda)_{\lambda \in \Lambda}$, where $e_\lambda \in R_\lambda$ is the identity element. We may now restate Theorem 3.5 (ii)–(v) as saying that the map

$$p \colon R \to \prod_{\lambda \in \Lambda(R)} R_\lambda$$

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

$$\rho \colon D \to \mathrm{End}_R(S)^{\mathrm{op}}$$

defined by $\rho(a)(\boldsymbol{x}) = \boldsymbol{x}a$ 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 $D = \mathrm{End}_R(S)^{\mathrm{op}}$ opposite of the ring of R-linear endomorphisms of S, and the map*

$$\lambda\colon R \to \mathrm{End}_D(S)$$

defined by $\lambda(a)(\boldsymbol{x}) = a\boldsymbol{x}$ is a ring isomorphism.

Here, in (ii), the ring $\mathrm{End}_R(S)^{\mathrm{op}}$ is a division ring by Schur's lemma, which we proved last time.

PROOF. (i) We have proved in Lemma 2.11 that S is a simple left R-module. Now, let $\boldsymbol{e}_i \in M_{1,n}(D)$ be the row vector whose ith entry is 1 and whose remaining entries are 0. Then the map $f\colon S \oplus \cdots \oplus S \to R$, where there are n summands S, defined by $f(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) = \boldsymbol{v}_1\boldsymbol{e}_1 + \cdots + \boldsymbol{v}_n\boldsymbol{e}_n$ is an isomorphism of left R-modules. Indeed, in the $n \times n$-matrix $\boldsymbol{v}_i\boldsymbol{e}_i$, the ith column is $\boldsymbol{v}_i$ and the remaining columns are zero. This shows that R is a semisimple 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 ρ is a ring homomorphism. Now, the kernel of ρ is a two-sided ideal in the division ring D, and hence, is either zero or all of D. But $\rho(1) = \mathrm{id}_S$ is not zero, so the kernel is zero, and hence the map ρ is injective. It remains to show that ρ is surjective. So let $f\colon S \to S$ be an R-linear map. We must show that there exists $a \in D$ such that for all $\boldsymbol{y} \in S$, $f(\boldsymbol{y}) = \boldsymbol{y}a$. To this end, we fix a non-zero element $\boldsymbol{x} \in S$ and choose a matrix $P \in R$ such that $P\boldsymbol{x} = \boldsymbol{x}$ and such that $PS = \boldsymbol{x}D \subset S$. (The existence of such a matrix P will be shown on the problem set.) Since f is R-linear, we have

$$f(\boldsymbol{x}) = f(P\boldsymbol{x}) = Pf(\boldsymbol{x}) \in \boldsymbol{x}D$$

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

$$f(\boldsymbol{y}) = f(A\boldsymbol{x}) = Af(\boldsymbol{x}) = A\boldsymbol{x}a = \boldsymbol{y}a$$

as desired. This shows that ρ 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 $f\colon S \oplus \cdots \oplus S \to R$ from the direct sum of a finite number, say n, of copies of S onto R. We now have ring isomorphisms

$$R^{\mathrm{op}} \xrightarrow{\sim} \mathrm{End}_R(R) \xrightarrow{\sim} \mathrm{End}_R(S^n) \xrightarrow{\sim} M_n(\mathrm{End}_R(S)) = M_n(D^{\mathrm{op}})$$

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 $i_j\colon S \to S^n$ of the jth summand, the endomorphism $g\colon S^n \to S^n$, and the projection $p_i\colon S^n \to S$ onto the ith summand. It follows that we have a ring isomorphism

$$R \xrightarrow{\sim} M_n(D^{\mathrm{op}})^{\mathrm{op}} \xrightarrow{\sim} M_n((D^{\mathrm{op}})^{\mathrm{op}}) = M_n(D)$$

given by the composition of the isomorphism above and the isomorphism that takes the matrix A to its transpose matrix A^t. 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 λ is an isomorphism in this case. But this is precisely the statement of Corollary 2.5, so the proof is complete. □

Remark 3.8. 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 is a field, and it is not difficult to show that also $Z(M_n(D)) = k \cdot I_n$. 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 quarternions $\mathbb{H}$ is the field of real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C} \subset \mathbb{H}$ is a maximal subfield.

It is now high time that we see an example of a semisimple ring. In general, if k is a commutative ring and G a group, then the group ring $k[G]$ is defined to be the free k-module with basis G and with the "convolution" multiplication

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

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 $\eta \colon k \to k[G]$ defined by $\eta(a) = a \cdot e$ is ring homomorphism. If M is a left $k[G]$-module, then we also say that M is a k-linear representation of the group G.

Let k be a field and let $\eta \colon \mathbb{Z} \to k$ be the unique ring homomorphism. We define the characteristic of k to be the unique non-negative integer $\operatorname{char}(k)$ such that $\ker(\eta) = \operatorname{char}(k)\mathbb{Z}$. For example, the fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ have characteristic 0, while for every prime number p, the field $\mathbb{Z}/p\mathbb{Z}$ has characteristic p.

Exercise 3.9. Let k be a field. Show that $\operatorname{char}(k)$ is either zero or a prime number, and that every integer n not divisible by $\operatorname{char}(k)$ is invertible in k.

Theorem 3.10 (Maschke's theorem). *Let k be a field and let G be a finite group, whose order is not divisible by the characteristic of k. Then the group ring $k[G]$ is a semisimple ring.*

Proof. We show that every left $k[G]$-module M of finite dimension m over k is a semisimple 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 $n > 1$ and assume, inductively, that every left $k[G]$-module of dimension $m < n$ over k is semisimple. We must show that if M is a left $k[G]$-module of dimension $m = n$ over k, then M is semisimple. If M is simple, we are done. If M is not simple, there exists a non-zero proper submodule $N \subset M$. We let $i \colon N \to M$ be the inclusion and choose a k-linear map $\rho \colon M \to N$ such that $\sigma \circ i = \mathrm{id}_N$. The map ρ is not necessarily $k[G]$-linear. However, we claim that the map $r \colon M \to N$ defined by

$$r(\boldsymbol{x}) = \frac{1}{|G|} \sum_{g \in G} g\rho(g^{-1}\boldsymbol{x})$$

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

$$\begin{aligned} r(h\boldsymbol{x}) &= \frac{1}{|G|} \sum_{g \in G} g\rho(g^{-1}h\boldsymbol{x}) = \frac{1}{|G|} \sum_{g \in G} hh^{-1}g\rho(g^{-1}h\boldsymbol{x}) \\ &= \frac{1}{|G|} \sum_{k \in G} hk\rho(k^{-1}\boldsymbol{x}) = hr(\boldsymbol{x}) \end{aligned}$$

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

$$\begin{aligned}(r \circ i)(\boldsymbol{x}) &= \frac{1}{|G|}\sum_{g\in G} g\rho(g^{-1}i(\boldsymbol{x})) = \frac{1}{|G|}\sum_{g\in G} g\rho(i(g^{-1}\boldsymbol{x})) \\ &= \frac{1}{|G|}\sum_{g\in G} gg^{-1}\boldsymbol{x} = \boldsymbol{x}\end{aligned}$$

which shows that $r \circ i = \mathrm{id}_N$. This proves the claim. Now, let P be the kernel of r. The claim shows that M is equal to the direct sum of the submodules $N, P \subset M$. But N and P both have dimension less than n over k, and hence, are semisimple by the induction hypothesis. This shows that M is semisimple as desired. □