IV.B. Submodules and homomorphisms

Let M be a (left) R-module.

IV.B.1. DEFINITION. An ***R*-submodule** $N \subseteq M$ is an additive subgroup closed under the "scalar multiplication" action of R.

IV.B.2. EXAMPLES. (continuation of IV.A.2)
(a) Given an $\mathbb{F}$-vector space ($=\mathbb{F}$-module), an $\mathbb{F}$-submodule is a subspace (defined over $\mathbb{F}$).

(b) Given an abelian group A ($=\mathbb{Z}$-module), a $\mathbb{Z}$-submodule is just a subgroup.

(c) Regarding R as (left) R-module, the (left) R-submodules are precisely the (left) ideals.

(d) cf. IV.B.8(ii) below.

(e) Sub-vector bundles of a vector bundle $\mathcal{V} \to \mathcal{M}$ yield $C^\infty(\mathcal{M})$-submodules.

(f) There are no proper nontrivial $M_n(\mathbb{R})$-submodules of $\mathbb{R}^n$. (Why?)

(g) The sub-$\mathbb{F}[G]$-modules of a representation V of G are the subrepresentations $W \subset V$ — i.e. sub-$\mathbb{F}$-vector spaces stabilized by G ($G(W) \subset W$).

(h) Given $T \in \mathrm{End}_{\mathbb{F}}(V)$ and regarding V as $\mathbb{F}[\lambda]$-module via $\lambda v := T(v)$, an $\mathbb{F}[\lambda]$-submodule is a subspace $W \subset V$ stabilized by T (that is, $T(W) \subset W$).

IV.B.3. DEFINITION. Given a subset $\mathcal{S} \subset M$, the R-submodule generated by $\mathcal{S}$ is[3]

$$R\langle \mathcal{S} \rangle := \{\textstyle\sum_{s\in\mathcal{S}}^{\text{finite}} r_s s \mid r_s \in R\},$$

or equivalently the intersection of all R-submodules containing $\mathcal{S}$. Just as for ideals, we define sums by

$$\textstyle\sum_\alpha N_\alpha := R\langle \{N_\alpha\} \rangle = \{\sum_\alpha^{\text{finite}} n_\alpha \mid n_\alpha \in N_\alpha\}.$$

[3]See IV.A.3 for finite generation.

"Finite" means that, while the index set may be infinite, only finitely many terms in each sum can be nonzero.

IV.B.4. PROPOSITION-DEFINITION (Quotient R-modules). *Given an R-submodule $N \subset M$, the quotient group M/N has the structure of an R-module.*

PROOF. Define $r\bar{m} = r(m+N) := rm + N = \overline{rm}$. This is well-defined since for $m' - m \in N$, $RN \subset N \implies r(m-m') \in N \implies$

$$rm + N = rm' + rm - rm' + N = rm' + r(m-m') + N = rm' + N.$$

Now check the properties in IV.A.1 for M/N, e.g. $(rs)\bar{m} = \overline{(rs)m} = \overline{r(sm)} = r(\overline{sm}) = r(s\bar{m})$. □

IV.B.5. DEFINITION. A **homomorphism** of R-modules $\eta \colon M \to M'$ is a homomorphism of abelian groups intertwining the action of R: $\eta(rm) = r\eta(m)$. The set of all such is denoted $\mathrm{Hom}_R(M, M')$, and $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$. The usual words on injective and surjective homomorphisms and isomorphisms apply.

IV.B.6. PROPOSITION. $\mathrm{End}_R(M)$ *is a ring, and* $\mathrm{Hom}_R(M, M')$ *an abelian group.*

PROOF. The sum and (if defined) composite of two R-intertwining homomorphisms also intertwine the action of R. □

Just as in the case of groups and rings, kernels and images define subobjects.

IV.B.7. PROPOSITION. *The kernel* $\ker(\eta) \subseteq M$ *and image* $\mathrm{im}(\eta) \subseteq M'$ *are R-submodules.*

PROOF. $R\ker(\eta) \subset \ker(\eta)$ since $\eta(m) = 0 \implies \eta(rm) = r\eta(m) = 0$; and $R\mathrm{im}(\eta) \subset \mathrm{im}(\eta)$ since $r\eta(m) = \eta(rm)$. □

IV.B.8. EXAMPLES. (i) The inclusion $\imath \colon N \hookrightarrow M$ of a submodule and the projection $\nu \colon M \twoheadrightarrow M/N$ to the quotient module are R-module homomorphisms.

(ii) A (f.g.) R-module M is **free** $\overset{\text{def.}}{\Longleftrightarrow}$ $M \cong R^n$ (as R-module) for some $n \in \mathbb{N}$. (If R is noncommutative, n need not be unique.)

A submodule of a "free" R-module need not be free unless R is a PID: for instance, $\mathbb{Z}_6$ has $3\mathbb{Z}_6$ as sub-$\mathbb{Z}_6$-module.

(iii) Consider the **cyclic** (sub)**module**

$$Rx := \{rx \mid r \in R\} \subset M$$

for some $x \in M$. We have

$$\begin{aligned} \mu_x \colon R &\twoheadrightarrow Rx \\ r &\mapsto rx\,, \end{aligned}$$

which satisfies $r'\mu_x(r) = r'rx = \mu_x(r'r)$ and $\mu_x(r+r') = (r+r')x = rx + r'x = \mu_x(r) + \mu_x(r')$ hence is an R-module homomorphism.

Define the **annihilator**

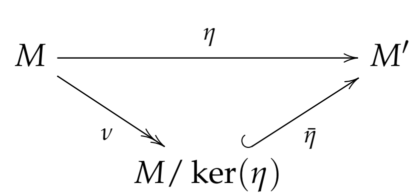
$$\text{ann}(x) := \ker(\mu_x) \subseteq R,$$

which is a (left) R-submodule of R hence a *left ideal*. If $R = \mathbb{Z}$, $\text{ann}(x)$ is the principal ideal of $\mathbb{Z}$ generated by $\text{ord}(x)$, the order of x in M.

(iv) An $\mathbb{F}$-module homomorphism between two $\mathbb{F}$-vector spaces is an $\mathbb{F}$-linear transformation.

In another similarity to groups and rings, the various isomorphism theorems hold for R-modules. In particular, we have the

IV.B.9. FUNDAMENTAL THM. OF R-MODULE HOMOMORPHISMS. *Any given R-module homomorphism $\eta\colon M \to M'$ factors as follows:*



In particular, $\text{im}(\eta) \cong M/\ker(\eta)$ *as R-modules.*

PROOF. As usual, $\bar{\eta}$ is well-defined and the diagram commutes because of the abelian group result. We need to check that $\bar{\eta}$ is an R-module homomorphism: by definition, $\bar{\eta}(\bar{m}) := \eta(m)$, and $r\bar{\eta}(\bar{m}) = r\eta(m) = \eta(rm) = \bar{\eta}(r\bar{m}) = \bar{\eta}(r\bar{m})$. □

IV.B.10. EXAMPLE. Let $x \in M$ be given. Applying this Theorem to IV.B.8(iii) (with $\eta := \mu_x$) gives $Rx \cong R/\text{ann}(x)$. Note that, if M is free, and R is a domain, then $\text{ann}(x) = \{0\}$ and so $Rx \cong R$ (is free).

Free R-modules. Let's go into some more detail on these. First note that $R^n = R\langle \mathbf{e}_1, \ldots, \mathbf{e}_n \rangle$, where as before $\mathbf{e}_i$ is the i^{th} standard basis (column) vector. Moreover, if we write $0_{R^n} = \sum_i r_i \mathbf{e}_i = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$, then $r_i = 0$ for all i. Consequently, there is exactly one way of expressing each element of R^n as $\sum_{i=1}^n r_i \mathbf{e}_i$; and so given any R-module M and $u_1, \ldots, u_n \in M$,

$$\begin{aligned} \theta \colon R^n &\longrightarrow M \\ \textstyle\sum_i r_i \mathbf{e}_i &\longmapsto \textstyle\sum_i r_i u_i \end{aligned} \tag{IV.B.11}$$

is a well-defined R-module homomorphism. [Check: $r\theta(\sum r_i \mathbf{e}_i) = r \sum r_i u_i = \sum r r_i u_i = \theta(\sum r r_i \mathbf{e}_i) = \theta(r \sum r_i \mathbf{e}_i)$.]

IV.B.12. DEFINITION. A **base** for a (f.g., left) R-module is an ordered generating set $m_1, \ldots, m_n$ (for some $n \in \mathbb{N}$) such that

$$\textstyle\sum_{i=1}^n r_i m_i = 0 \quad \Longrightarrow \quad r_i = 0 \ (\forall i).$$

IV.B.13. PROPOSITION. *A (f.g.) R-module M is free $\iff$ M has a base.*

PROOF. ($\Longrightarrow$) is clear: use the standard base. For ($\Longleftarrow$): given a base $\{m_1, \ldots, m_n\} \subset M$, the homomorphism $\theta \colon R^n \to M$ (sending $\sum r_i \mathbf{e}_i \mapsto \sum r_i m_i$) is injective and surjective (by definition of "base"), so that $M \cong R^n$. □

IV.B.14. THEOREM-DEFINITION. *Let M be a (f.g.) free R-module. If R is commutative, then*

$$\textbf{\textit{rank}}(M) := \text{"\# of elements in a base for } M\text{"}$$

is well-defined.

PROOF. Let $\{f_1, \ldots, f_n\}$ and $\{e_1, \ldots, e_m\}$ $(n \geq m)$ be bases of M. We have $e_j = \sum_{k=1}^{n} a_{jk} f_k$ and

$$f_i = \sum_{j=1}^{m} b_{ij} e_j = \sum_{k=1}^{n} \sum_{j=1}^{m} b_{ij} a_{jk} f_k$$

for some $a_{jk}, b_{ij} \in R$. Since $\{f_j\}$ is a base, the displayed equality gives $\sum_{j=1}^{m} b_{ij} a_{jk} = \delta_{ik}$ $(i, k \in \{1, \ldots, n\})$. Adding $n - m$ columns [resp. rows] of zeroes to the $n \times m$ matrix (b_{ij}) [resp. $m \times n$ matrix (a_{jk})] therefore yields $n \times n$ matrices satisfying

$$BA := \begin{pmatrix} b_{11} \cdots b_{1m} & 0 \cdots 0 \\ \vdots \quad\quad \vdots & \vdots \quad \vdots \\ b_{n1} \cdots b_{nm} & 0 \cdots 0 \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = \mathbb{1}_n$$

whence $\det(B)\det(A) = 1$ as R is commutative (cf. III.C.16). If $n > m$ then the rows/columns of zeroes make $\det(A)$ and $\det(B)$ zero, a contradiction. So we have $n = m$. □

IV.B.15. COROLLARY. *Let R be commutative, M a f.g. free R-module. Then $\mathrm{GL}_n(R)$ acts transitively on the set of bases of M.*

PROOF. In the proof of IV.B.14, A sends $\{f_j\}$ to $\{e_i\}$ and $\det(A) \in R^* \implies A \in \mathrm{GL}_n(R)$ (invertible).

Conversely, if A is invertible ($\exists B$ s.t. $AB = \mathbb{1}_n = BA$) and $\{f_j\}$ is a base, I claim that $e_i := \sum_{j=1}^{n} a_{ij} f_j$ is a base. First,

$$\begin{aligned} BA = \mathbb{1}_n &\implies \textstyle\sum_i b_{ki} e_i = \sum_j (\sum_i b_{ki} a_{ij}) f_j = \sum_j \delta_{kj} f_j = f_k \\ &\implies \{e_i\} \text{ generate } M. \end{aligned}$$

Second, if $\sum_i r_i e_i = 0$ then

$$\begin{aligned} AB = \mathbb{1}_n &\implies 0 = i r_i \textstyle\sum_j a_{ij} f_j = \sum_j (\sum_i r_i a_{ij}) f_j \\ [\{f_j\} \text{ base}] &\implies \textstyle\sum_i r_i a_{ij} = 0 \ (\forall j) \\ &\implies 0 = \textstyle\sum_{i,j} r_i a_{ij} b_{jk} = \sum_i r_i \delta_{ik} = r_k \ (\forall k), \end{aligned}$$

so that $\{e_i\}$ is a base by IV.B.12. □

Now let R be general and M, N be free *right*[4] R-modules with bases $\underline{e} = \{e_1, \ldots, e_m\}$ resp. $\underline{f} = \{f_1, \ldots, f_n\}$.

IV.B.16. DEFINITION. The matrix of $\eta \in \mathrm{Hom}_R(M, N)$ relative to $\underline{e}, \underline{f}$ is

$$ {}_{\underline{f}}[\eta]_{\underline{e}} := (a_{ij})_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} $$

where $\eta(e_j) = \sum_{i=1}^n f_i a_{ij}$ (with $a_{ij} \in R$). Also write

$$ {}_{\underline{e}}[x] := \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} $$

for $x = \sum_{j=1}^m e_j x_j \in M$ (with $x_j \in R$), and similarly for $y \in N$.[5]

IV.B.17. PROPOSITION. ${}_{\underline{f}}[\eta]_{\underline{e}} \cdot {}_{\underline{e}}[x] = {}_{\underline{f}}[\eta(x)]$, *where the dot is computed by matrix-vector multiplication and the R-module structure.*

PROOF. This says that if the a_{ij} and x_j are as above, then

$$ \sum_i f_i (\sum_j a_{ij} x_j) = \eta(x). \tag{IV.B.18} $$

To check this, write LHS(IV.B.18) $= \sum_j (\sum_i f_i a_{ij}) x_j = \sum_j \eta(e_j) x_j = \eta(\sum_j e_j x_j) = \eta(x)$. □

Writing $[\cdot]$ as a shorthand for ${}_{\underline{f}}[\cdot]_{\underline{e}}$ when the bases are understood, we have

IV.B.19. PROPOSITION. $[\cdot]\colon \mathrm{Hom}_R(M, N) \to M_{n\times m}(R)$ *is an isomorphism of abelian groups.*

PROOF. It is clear that $[\eta + \eta'] = [\eta] + [\eta']$. Any $A \in M_{n\times m}(R)$ can be used to define η on the $\underline{e}$, and this gives a homomorphism with $[\eta] = A$, proving surjectivity. Finally, $[\cdot]$ is injective since $[\eta]$ defines η via IV.B.17. □

---

[4]If R is commutative, these are just left R-modules by $rm := mr$. The main point here is that I want the transpose of what **[Jacobson]** gets.

[5]In contrast, **[Jacobson]** uses row vectors.

Generalizing IV.B.17, if L is a free R-module with base $\{\delta_1, \ldots, \delta_\ell\}$ then the diagram

$$\text{(IV.B.20)} \qquad \begin{array}{ccc} \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(L,M) & \xrightarrow{\text{compose}} & \mathrm{Hom}_R(L,N) \\ \cong \downarrow {}_{\underline{f}}[\cdot]_{\underline{e}} \times {}_{\underline{e}}[\cdot]_{\underline{\delta}} & & \cong \downarrow {}_{\underline{f}}[\cdot]_{\underline{\delta}} \\ M_{n\times m}(R) \times M_{m\times \ell}(R) & \xrightarrow{\text{matrix mult.}} & M_{n\times \ell}(R) \end{array}$$

commutes. Since composition of maps is associative, (IV.B.20) $\implies$ matrix multiplication is too.

PROOF OF (IV.B.20). Let $\eta \in \mathrm{Hom}_R(M,N)$ and $\zeta \in \mathrm{Hom}_R(L,M)$. Writing $(A)_{ik}$ for the $(i,k)^{\text{th}}$ entry of a matrix A, we have

$$\begin{aligned} \textstyle\sum_{i=1}^n f_i ({}_{\underline{f}}[\eta\zeta]_{\underline{\delta}})_{ik} &= (\eta\zeta)(\delta_k) = \eta(\zeta(\delta_k)) \\ &= \eta(\textstyle\sum_{j=1}^m e_j ({}_{\underline{e}}[\zeta]_{\underline{\delta}})_{jk}) = \sum_{j=1}^m \eta(e_j)({}_{\underline{e}}[\zeta]_{\underline{\delta}})_{jk} \\ &= \textstyle\sum_{j=1}^m (\sum_{i=1}^n f_i ({}_{\underline{f}}[\eta]_{\underline{e}})_{ij})({}_{\underline{e}}[\zeta]_{\underline{\delta}})_{jk} \\ &= \textstyle\sum_{i=1}^n f_i \{\sum_{j=1}^m ({}_{\underline{f}}[\eta]_{\underline{e}})_{ij}({}_{\underline{e}}[\zeta]_{\underline{\delta}})_{jk}\} \\ &= \textstyle\sum_{i=1}^n f_i ({}_{\underline{f}}[\eta]_{\underline{e}} \cdot {}_{\underline{e}}[\zeta]_{\underline{\delta}})_{ik}. \end{aligned}$$

Now use that $\{f_i\}$ is a base. $\square$

Applying this in the case $M = N = L$ ($\implies m = n = \ell$), we have proved

IV.B.21. THEOREM. *Given a free right R-module M, we have an isomorphism of rings* ${}_{\underline{e}}[\cdot] := {}_{\underline{e}}[\cdot]_{\underline{e}} \colon \mathrm{End}_R(M) \xrightarrow{\cong} M_m(R)$.

IV.B.22. REMARK. A natural question is whether $\mathrm{Hom}_R(M,N)$ has the structure of an R-module. Let's consider this in the *left*-R-module case. If R is non-commutative, the answer is in general *no*: given $f \in \mathrm{Hom}_R(M,N)$, we can try to define rf by[6]

$$\text{(IV.B.23)} \qquad (rf)(m) := r \cdot f(m)$$

(where the RHS $= f(rm)$ since $f \in \mathrm{Hom}_R(M,N)$). The problem is that, in order for this rf to still lie in $\mathrm{Hom}_R(M,N)$, we need $r' \cdot$

[6] We occasionally use a "$\cdot$" to indicate some (but not all) R-module actions, so as to clarify the order of operations.

$(rf)(m) = (rf)(r'm)$. But by (IV.B.23), this becomes $r' \cdot (r \cdot f(m)) = r \cdot f(r'm)$, hence (using $f \in \text{Hom}_R(M, N)$) $r'r \cdot f(m) = rr' \cdot f(m)$, which is clearly not true in general. On the other hand, if M and N are right R-modules, and N *also* has a left R-module structure, then $\text{Hom}_{\text{right } R\text{-mod}}(M, N)$ *will* have a left R-module structure, defined by[7] (IV.B.23). Needless to say, all these delicate issues vanish if R is commutative; but if you want to think about modules over matrix rings or group rings, you have to face them.

Direct summands. We have been examining the special case of M a "sum" of copies of R (as R-module). Let's consider more general "sums":[8]

IV.B.24. DEFINITION. (i) Given R-modules $\{M_i\}_{i=1}^n$, their **direct sum** is the R-module[9] $M_1 \oplus \cdots \oplus M_n$ with underlying abelian group $M_1 \times \cdots \times M_n$ and R-action by $r(m_1, \ldots, m_n) := (rm_1, \ldots, rm_n)$.

(ii) Given R-module homomorphisms $\eta_i \colon M_i \to N$ and $\mu_i \colon M_i \to N_i$, we define R-module homomorphisms

- $\sum_i \eta_i \colon M_1 \oplus \cdots \oplus M_n \to N$, by $(m_1, \ldots, m_n) \mapsto \sum \eta_i(m_i)$; and
- $\oplus_i \mu_i \colon M_1 \oplus \cdots \oplus M_n \to N_1 \oplus \cdots \oplus N_n$, by

$$(m_1, \ldots, m_n) \mapsto (\mu_1(m_1), \ldots, \mu_n(m_n)).$$

The following is (for $n = 2$, at least) reminiscent of the direct product theorem for groups.

IV.B.25. THEOREM. *Let $\{M_i\}_{i=1}^n$ be R-submodules of M. If*

(i) [spanning] $M = \sum M_i$ *and*

(ii) [independence] $M_j \cap \sum_{i \neq j} M_i = \{0\}$ $(\forall j)$,

then $M \cong \oplus_{i=1}^n M_i$.

[7] Note that RHS(IV.B.23) will no longer be given by $f(rm)$, since f is not assumed to be a left R-module homomorphism (and I haven't even assumed a left R-module structure on M.

[8] For simplicity, all modules are henceforth left modules; though the results also hold for right modules.

[9] Also written $\oplus_{i=1}^n M_i$ or just $\oplus_i M_i$ or $\oplus M_i$.

PROOF. Let $\eta_i \colon M_i \hookrightarrow M$ be the inclusions. By (i),

$$\eta := \sum_i \eta_i \colon \oplus M_i \to M$$

is surjective. By (ii), given $x_i \in M_i$ with $0 = \sum_{i=1}^n x_i$, we have

$$x_j = \sum_{i \neq j}(-x_i) \in M_j \cap \sum_{i \neq j} M_i \implies x_j = 0$$

for all j; hence η is injective. □

IV.B.26. REMARK. (a) In this setting, where $\sum_i \eta_i \colon \oplus M_i \xrightarrow{\cong} M$ for *submodules* $M_i \subset M$ satisfying (i) and (ii), we shall write $M = \oplus_i M_i$, and call M an *internal direct sum* (of these submodules).

(b) **[Jacobson]** has a converse result, which says that if $M \cong \oplus M_i$ then (i) and (ii) hold (for the submodules arising from $M_1 \times \{0\}$ and $\{0\} \times M_2$ on the RHS); he also has an "associativity" result for $\oplus$.

(c) Applying the Fund. Thm. IV.B.9 to the projection $\pi \colon M \oplus N \twoheadrightarrow M$ ($(m, n) \mapsto m$) produces an isomorphism $(M \oplus N)/N \cong M$.

(d) We can take infinite $\oplus$'s indexed by a set $\mathcal{I}$. Elements are $\mathcal{I}$-tuples with all but finitely many entries zero. (Axiom of choice plays no role here.)

We now consider the question of when it is possible to use direct sums to "atomize" a given module. What is an "atom"?

IV.B.27. DEFINITION. A nonzero R-module M is **irreducible** (or **simple**) if $\{0\}$ and M are its only submodules.

IV.B.28. PROPOSITION. *M is irreducible $\iff$ M is cyclic with every nonzero element as generator.*

PROOF. ($\Longleftarrow$): no proper subset of M but $\{0\}$ is closed under the action of R.

($\Longrightarrow$): If some $x \in M \backslash \{0\}$ has $Rx \neq M$ then Rx is a nontrivial proper submodule. □

IV.B.29. COROLLARY. *M irreducible $\iff$ $M \cong R/I$ with I a maximal* (*left*) *ideal of R.*

PROOF. Use an isomorphism theorem. (HW) □

IV.B.30. SCHUR'S LEMMA. *Given M_1, M_2 irreducible R-modules, any nonzero R-module homomorphism $\theta\colon M_1 \to M_2$ is an isomorphism.*

PROOF. (Assume $M_1 \neq \{0\}$.) Since $\ker(\theta) \subset M_1$ is a submodule, either $\ker(\theta) = \{0\}$ or M_1, hence θ is injective or zero. If θ is injective, then $\theta(M_1) \subset M_2$ is a nonzero submodule, so equals M_2, making θ also surjective. □

IV.B.31. COROLLARY. *If M is irreducible, then* $\mathrm{End}_R(M)$ *is a division ring.*

PROOF. Every nonzero $\theta \in \mathrm{End}_R(M)$ is invertible, by Schur's Lemma. □

You may wonder what happens if we have an irreducible submodule $N \subset M$ — is it a **direct summand**, i.e. is there a "complementary" submodule N' so that $M = N \oplus N'$? In general, this is *false* — consider $2\mathbb{Z} \subset \mathbb{Z}$ (as $\mathbb{Z}$-module), which has no such "complement" — but it's obviously true for finite-rank modules over a field (i.e. vector spaces).

IV.B.32. DEFINITION. An R-module is **semisimple** if every submodule of M is a direct summand.

We now jump into a bit of deep water:

IV.B.33. THEOREM. *The following are equivalent for an R-module M:*
(a) *M is semisimple;*
(b) *M is isomorphic to a direct sum of irreducible R-modules; and*
(c) *M is the internal direct sum of some irreducible R-submodules.*

PROOF. <u>(c) $\Longrightarrow$ (b)</u>: obvious

<u>(b) $\Longrightarrow$ (a)</u>: Say $M \cong \oplus_{i\in\mathcal{I}} M_i$, with M_i irreducible, with $N \subset M$ a submodule. Invoking Zorn's lemma, we let $\mathcal{K} \subset \mathcal{I}$ be maximal with respect to the property that $(\sum_{i\in\mathcal{K}} M_i) \cap N = \{0\}$.

Given $i_0 \in \mathcal{K}$, $M_{i_0} \subset (\sum_{i\in\mathcal{K}} M_i) + N$. (Duh.)

Given $i_0 \notin \mathcal{K}$, maximality $\implies (M_{i_0} + \sum_{i\in\mathcal{K}} M_i) \cap N \neq \{0\}$. So there exist $m_{i_0} \in M_{i_0}$ and $m_{\mathcal{K}} \in \sum_{i\in\mathcal{K}} M_i$ such that $m_{i_0} + m_{\mathcal{K}} =: n \in N\backslash\{0\}$. Note that necessarily $m_{i_0} \neq 0$, and so $M_{i_0} = Rm_{i_0}$. Since $m_{i_0} = n - m_{\mathcal{K}}$, we find $M_{i_0} \subset Rm_{\mathcal{K}} + Rn \subset (\sum_{i\in\mathcal{K}} M_i) + N$.

Thus for every $i_0 \in \mathcal{I}$, M_{i_0} is contained in $(\sum_{i\in\mathcal{K}} M_i) + N$, hence that $M = \sum_{i\in\mathcal{K}} M_i + N$. By IV.B.25, we have $M \cong (\sum_{i\in\mathcal{K}} M_i) \oplus N$. Conclude that M is semisimple.

<u>(a) $\implies$ (c)</u>: Let $N \subset M$ be a submodule, and $n \in N\backslash\{0\}$. Invoking Zorn again, we let $L \subset N$ be maximal with $n \notin L$. Since M is semisimple, we have $M = L \oplus L'_0$; intersecting with[10] N gives $N = L \oplus (L'_0 \cap N) =: L \oplus L'$.

Suppose L' is not simple: then it has a proper nonzero submodule L'_1; applying semisimplicity of M and "intersecting" as above, we get $L' = L'_1 \oplus L'_2$. Hence $N = L \oplus L'_1 \oplus L'_2$. If $n \in L \oplus L'_i$ $(i = 1, 2)$ then we can write $n = \ell_1 + \ell'_1 = \ell_2 + \ell'_2$ (with $\ell_1, \ell_2 \in L$). But then $\ell_1 - \ell_2 = \ell'_2 - \ell'_1 \in L \cap L' = \{0\} \implies \ell'_1 = \ell'_2 \in L'_1 \cap L'_2 = \{0\} \implies n \in L$, a contradiction. So $n \notin L \oplus L'_2$ (swapping 1 and 2 if needed), which violates the maximality of L, another contradiction! Conclude that L' is simple.

So we have shown that *every submodule N of M contains a simple direct summand.*

Next, let $\{M_i \mid i \in \mathcal{I}\}$ be a set of simple submodules of M, maximal (Zorn again) with respect to the property that

$$M_{\mathcal{I}} := \sum_{i\in\mathcal{I}} M_i \boxed{=} \oplus_{i\in\mathcal{I}} M_i.$$

By semisimplicity of M, $M = M_{\mathcal{I}} \oplus M'$. Suppose $M' \neq \{0\}$. Then the italicized statement above produces a direct sum decomposition $M' = L \oplus L'$ with L' simple. But this contradicts maximality of

[10]One has to be a bit careful here: the classic example from linear algebra is that $\mathbb{R}^2$ is the direct sum of the two coordinate axes, a decomposition that you certainly can't "intersect" with (say) the diagonal. The difference here is that N contains one of the summands (namely, L). So given $m = \ell + \ell'_0 \in L \oplus L'_0 = M$, if it happens that $m \in N$ then $\ell'_0 = m - \ell \in N$ (since $m, \ell \in N$). So $\ell'_0 \in L'_0 \cap N$ as desired.

$\{M_i\}_{i\in\mathcal{I}}$ (since you can now throw in L'). So $M = M_{\mathcal{I}} = \oplus_{i\in\mathcal{I}} M_i$ is a direct sum of irreducibles as desired. $\square$

This brings us to one of the topics we shall explore next semester:

IV.B.34. DEFINITION. R is a (left) **semisimple** ring $\iff$ all (left) R-modules are semisimple.

In particular, in representation theory it is paramount to know when the representations of a group G are "completely reducible" (to direct sums of irreducible representations).