MGO Colloquium

Indecomposable Injective Modules over Noetherian Rings

Richard Bartels

May 13, 2021

Throughout these notes, R denotes a unital ring and an R-map is an R-module homomorphism.

Lifting property of free modules

Definition 0.1. A left R-module F is a **free** R-module if F is isomorphic to a direct sum of copies of R; that is, there is a (possibly infinite) index set X with $F \cong \bigoplus_{x \in X} R_x$, where $R_x = \langle x \rangle \cong R$ for all $x \in X$. We call X a **basis** of F.

Each $m \in F$ has a unique representation of the form $m = \sum_{x \in X} r_x x = (r_x)_{x \in X} = (r_x)$, where $r_x \in R$ for each $x \in X$, and $r_x = 0$ for all but finitely many $x \in X$.

Proposition 0.2. *Let F be a free R-module with basis X. Given an R-module M, an R-map $f : X \to M$, and inclusion map $\mu : X \to F$, there exists a unique R-map $\tilde{f} : F \to M$ with $\tilde{f}\mu = f$. So $\tilde{f}(x) = f(x)$ for all $x \in X$.*

$$\begin{tikzcd}
F & \\
X \arrow[u, "\mu"] \arrow[r, "f"] & M
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
F \arrow[dr, "\tilde{f}"] & \\
X \arrow[u, "\mu"] \arrow[r, "f"] & M
\end{tikzcd}$$

Lifting property of free modules. *Let F be a free R-module. If $p : B \to C$ is a surjective R-map, then for every R-map $g : F \to C$, there exists an R-map $h : F \to B$ such that $g = ph$.*

$$\begin{tikzcd}
 & F \arrow[d, "g"] \\
B \arrow[r, "p"] & C
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & F \arrow[d, "g"] \arrow[dl, "h"'] \\
B \arrow[r, "p"] & C
\end{tikzcd}$$

Proof. Let $X \subseteq F$ be a basis of F. Since p is surjective, for each $x \in X$, there exists an element $b_x \in B$ such that $p(b_x) = g(x)$. Define a function $u : X \to B$ by $u(x) = b_x$ for all $x \in X$. Hence, there exists an R-map $h : F \to B$ such that $h(x) = b_x$ for all $x \in X$. So for each $x \in X$, $ph(x) = p(b_x) = g(x)$. By the above proposition, $ph = g$ on F. □

Remark 0.3.

The lifting property is a basis-independent property of free modules.

The lifting property is not equivalent to the definition of a free R-module; there are rings R and R-modules F which are not free, even though they have a lifting h for each p and g as above.

There are rings, such as PIDs and **local** commutative rings, over which every module with the lifting property is free.

Definition 0.4. A commutative ring is **local** if it has a unique maximal ideal.

Examples:

A field k is a local ring with unique maximal ideal (0).

The ring of rational numbers with odd denominators, denoted $\mathbb{Q}_{(2)}$, is a local subring of $\mathbb{Q}$. Its unique maximal ideal $2\mathbb{Q}_{(2)}$ consists of fractions with even numerator and odd denominator.

Definition 0.5. Let $g : M \to C$ and $p : B \to C$ be R-maps. An R-map $h : M \to B$ is a **lifting of g** if $ph = g$.

$$\begin{tikzcd} & M \arrow[d, "g"] \\ B \arrow[r, "p"] & C \end{tikzcd} \qquad \begin{tikzcd} & M \arrow[d, "g"] \arrow[dl, "h"'] \\ B \arrow[r, "p"] & C \end{tikzcd}$$

Definition 0.6. A left R-module P is **projective** if, given a diagram of the form below, where B and C are R-modules, p and g are homomorphisms of R-modules (R-maps), and p is surjective, there is a **lifting** $h : P \to B$ such that $g = ph$.

$$\begin{tikzcd} & P \arrow[d, "g"] \\ B \arrow[r, "p"] & C \end{tikzcd} \qquad \begin{tikzcd} & P \arrow[d, "g"] \arrow[dl, "h"'] \\ B \arrow[r, "p"] & C \end{tikzcd}$$

Definition 0.7. A left R-module E is **injective** if, given a diagram of the form below, where A and B are R-modules, i and f are R-maps, and i is injective, there is an R-map $h : B \to E$ such that $f = hi$.

$$\begin{tikzcd}
E & \\
A \arrow[u, "f"] \arrow[r, "i"] & B
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
E & \\
A \arrow[u, "f"] \arrow[r, "i"] & B \arrow[ul, "h"']
\end{tikzcd}$$

Baer's criterion: An R-module is injective if and only if given a diagram of the form below, where I is a left ideal of R, i is the inclusion map, and f is an R-map, there is an R-map $g : R \to E$ making the completed diagram commute: $f = gi$.

$$\begin{tikzcd}
E & \\
I \arrow[u, "f"] \arrow[r, "i"] & R
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
E & \\
I \arrow[u, "f"] \arrow[r, "i"] & R \arrow[ul, "g"']
\end{tikzcd}$$

Proposition 0.8. *Let R be a domain and Q its fraction field. We show that Q is an injective R-module using Baer's Criterion.*

Proof. Let I be a left ideal of R, and let $f : I \to Q$ be an R-map. We extend f to an R-map $g : R \to Q$.

First observe the following: If $a, b \in I$ are nonzero elements of R, then $af(b) = f(ab) = bf(a)$, and therefore $f(a)/a = f(b)/b$ in Q. Let $c \in Q$ denote the common value of these quotients. Define an R-map $g : R \to Q$ by $g(r) = rc$ for all $r \in R$. Then for all $a \in I$,

$g(a) = ac = af(a)/a = f(a).$

Hence, g extends f, and therefore Q is an injective R-module. □

An **exact sequence** of R-modules is a diagram of the form

$... \to X_0 \xrightarrow{d_0} X_1 \xrightarrow{d_1} X_2 \xrightarrow{d_2} ... \to X_n \xrightarrow{d_n} ...$

where for each $n \in \mathbb{N}$, X_n is an R-module, d_n is an R-map, and for each n, $\mathrm{im} d_n = \ker d_{n+1}$.

A **short exact sequence** (ses) of R-modules is a diagram of the form

$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$

where A, B, and C are R-modules, f and g are R-maps, and

$\ker f = 0$

$\operatorname{im} f = \ker g$

$\operatorname{im} g = C$

The image of each homomorphism equals the kernel of the next homomorphism.

If there is an R-map $B \xrightarrow{j} A$ such that $jf = 1_A$, or equivalently, if there is an R-map $\rho : C \to B$ such that $g\rho = 1_C$, then we say the short exact sequence **splits**, which implies $B \cong A \oplus C$.

Examples: Given an R-module M, an R-submodule $N \subseteq M$ gives us a short exact sequence where i is the inclusion map and π is the quotient map:

$0 \to N \xrightarrow{i} M \xrightarrow{\pi} M/N \to 0.$

If A, B, and C are R-modules and $B = A \oplus C$, then

$0 \to A \to B \to C \to 0$ is a ses.

Note: If we are given a short exact sequence $0 \to A \to B \to C \to 0$ such that $B \cong A \oplus C$, it does not follow that the ses splits.

Facts and examples

Every R-module is the homomorphic image of a free R-module.

Every free R-module $F = \bigoplus_{i \in I} R_i$, where each R_i is a copy of R, is a projective R-module. The notion of a projective module is an abstraction of free modules defined by the basis-free lifting property of free modules.

$\mathbb{Z}/6\mathbb{Z}$ is a free $\mathbb{Z}/6\mathbb{Z}$-module. Since $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, it follows that $\mathbb{Z}/3\mathbb{Z}$ is a projective $\mathbb{Z}/6\mathbb{Z}$-module. But it is not a free $\mathbb{Z}/6\mathbb{Z}$-module, since it is nonzero and has cardinality less than 6.

If R is a PID, then an R-module M is projective if and only if it is free, and M is injective if and only if it is divisible.

Given a domain R, we say that an R-module M is **divisible** if for all $m \in M$ and all nonzero $r \in R$, there is an element $m' \in M$ such that $m = rm'$.

Since $\mathbb{Q}/\mathbb{Z}$ is a divisible $\mathbb{Z}$-module, it is an injective $\mathbb{Z}$-module.

Kaplansky's theorem for projective modules: If R is a local ring, then every projective R-module is free.

A module is projective if and only if it is a direct summand of a free module.

Direct sums of projective modules and direct summands of projective modules are projective. It is not true that an infinite direct product of projective modules is always projective. If we assume R is commutative, then every direct product of projective R-modules is projective if and only if R is Artinian.

$\prod_{i\in\mathbb{N}} \mathbb{Z}_i$, where $\mathbb{Z}_i = \mathbb{Z}$ for each i, is not a free $\mathbb{Z}$-module, and therefore it is not a projective module since $\mathbb{Z}$ is a PID.

Direct products of injective modules and direct summands of injective modules are injective. It is not true that an infinite direct sum of injective modules is always injective. Given a ring R, every direct sum of injective R-modules is injective if and only if R is Noetherian (Bass-Papp theorem).

For a given field k, every k-vector space V is projective and injective.

Since V has a k-basis, V is a free, and thus projective k-module.
$V \cong \bigoplus_{i\in I} k_i$ for some index set I. Over a Noetherian ring, direct sums of injective modules are injective. Since k is Noetherian and injective as a module over itself, V is an injective k-module.

Theorem. An R-module P is projective if and only if every short exact sequence of R-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ splits.

Proof. ($\Rightarrow$) Suppose P is projective, and we have a short exact sequence as above.

$$\begin{tikzcd}
 & P \arrow[d, "1_P"'] \\
B \arrow[r, "g"] & P
\end{tikzcd}
\qquad
\begin{tikzcd}
 & P \arrow[d, "1_P"'] \arrow[dl, "\rho"'] \\
B \arrow[r, "g"] & P
\end{tikzcd}$$

Since P is projective, there exists an R-map $\rho : P \to B$ such that $1_P = g\rho$. Hence, the short exact sequence splits.

($\Leftarrow$) Suppose every short exact sequence ending with P splits. We show that P is projective. Consider the following diagrams with g surjective:

$$\begin{tikzcd}
 & P \arrow[d, "f"'] \\
B \arrow[r, "g"] & C
\end{tikzcd}
\qquad
\begin{tikzcd}
F \arrow[r, "h"] \arrow[d, "g_o"'] & P \arrow[d, "f"'] \\
B \arrow[r, "g"] & C
\end{tikzcd}$$

There exists a surjective R-map $h : F \to P$, where F is a free module, since every module is the homomorphic image of a free module. The R-map g_o making the right-hand diagram commute exists because F is projective.

The map $F \xrightarrow{h} P$ gives the short exact sequence $0 \to \ker h \hookrightarrow F \xrightarrow{h} P \to 0$. Since this short exact sequence splits by hypothesis, there exists a map $j : P \to F$ such that $hj = 1_P$. Let $\tilde{f} = g_0 j$. Then $g\tilde{f} = g(g_o j) = (gg_o)j = (fh)j = f(hj) = f$. So P is projective.

□

Theorem 2. An R-module E is injective if and only if every short exact sequence of R-modules $0 \to E \xrightarrow{f} B \xrightarrow{g} C \to 0$ splits.

Proof. ($\Rightarrow$) Suppose E is injective, and that we have a short exact sequence as above.

$$\begin{tikzcd} E & \\ E \arrow[u, "1_E"] \arrow[r, "f"] & B \end{tikzcd} \qquad \begin{tikzcd} E & \\ E \arrow[u, "1_E"] \arrow[r, "f"] & B \arrow[ul, "j"'] \end{tikzcd}$$

Since f is injective, there exists an R-map $j : B \to E$ such that $1_E = jf$. Hence, the short exact sequence splits.

□

Definition. A submodule S of a module M is **superfluous** if, whenever $L \subseteq M$ is a submodule such that $S + L = M$, then $L = M$.

A surjective R-map $f : A \to B$ is **essential** if for every proper submodule $A' \subsetneq A$, $f(A') \subsetneq B$.

A **projective cover** of a module B is an ordered pair (P, φ) where P is projective and $\varphi : P \to B$ is a surjective map with $\ker \varphi$ a superfluous submodule of P.

Equivalently, (φ, P) is a **projective cover** of B if P is projective and φ is an essential surjection.

Definition. Let M and E be R-modules. Then E is called an **essential extension** of M if there is an injective R-map $\alpha : M \to E$ such that for every nonzero R-submodule $S \subseteq E$, $S \cap \alpha(M) \neq 0$.

E is called an **injective hull** or **injective envelope** of M if E is an injective module that is an essential extension of M.

Motivation: Why do we care about projective modules, injective modules, projective covers, and injective hulls?

1) Projective modules are a generalization of free modules. The lifting property that defines projective modules is a characterizing basis-free property of free modules.

Injective modules are the categorical dual of projective modules. Moreover, they are a natural generalization of the set of rational numbers $\mathbb{Q}$ considered as a $\mathbb{Z}$-module in the following ways:

a) If $\mathbb{Q}$ is a submodule of a $\mathbb{Z}$-module M, then $\mathbb{Q}$ is a direct summand of M.

b) If M is a $\mathbb{Z}$-module and N is a submodule of M, then any $\mathbb{Z}$-map $f : N \to \mathbb{Q}$ can be extended to a $\mathbb{Z}$-map $\tilde{f} : M \to \mathbb{Q}$.

2) Projective and injective modules are used in the construction of the derived functors, which are used to study properties of algebraic and projective varieties and topological invariants of manifolds.

3) The injective envelope of a module is a maximal essential extension of the module. Projective covers and injective hulls are used in the study of algebraic varieties.

Note: The projective cover and injective hull of an R-module M are unique up to isomorphism. Hence, we refer to *the* projective cover and injective hull of a module.

For an arbitrary ring R, every R-module has an injective hull. But it is not true that for every ring R, every R-module has a projective cover.

We say that a ring is **left perfect** if every left R-module has a projective cover, and **left semiperfect** (or just semiperfect) if every finitely generated left R-module has a projective cover. A commutative Artinian ring R is (left and right) perfect.

Examples: If P is a projective R-module, then $(P, 1_P)$ is a projective cover of P, since $\{0\}$ is a superfluous submodule of P. Likewise, if E is injective, then $(E, 1_E)$ is an injective hull of E.

The $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ has no projective cover. Suppose $\mathbb{Z}/2\mathbb{Z}$ has a projective cover (F, φ), $\varphi : F \to \mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, F is a free abelian group. Let $x \in F$ be a basis element such that $\varphi(x) = 1$. $F = \varphi^{-1}(\mathbb{Z}/2\mathbb{Z}) = \varphi^{-1}(\varphi((3x))) = \ker\varphi + (3x)$. Since $\ker\varphi$ is superfluous in F, $(3x) = F$. But this is a contradiction, since $x \notin (3x)$.

Let $R = k[x]$, where k is a field, and let $M = R/(x)$. M has no projective cover. Indeed, suppose (φ, P) is a projective cover of M, $\varphi : P \to M$. Since $k[x]$ is a PID, P is a free R-module. So $(1-x)P \subsetneq P$, but $\varphi((1-x)P) = M$, which contradicts the fact that φ is an essential surjection.

Note that $\mathbb{Z}$ and $k[x]$ are not Artinian.

Theorem. If R is a domain, then its fraction field Q is the injective envelope of R.

Proof. We know that Q is an injective R-module. It remains for us to show that Q is an essential extension of R. We map R injectively into Q via the R-map φ defined by $\varphi : r \to r/1$ for each $r \in R$, and we identify $\varphi(R)$ with R.

Suppose S is a nonzero R-submodule of Q, and let $r/s \in S$ be nonzero. Then r and s are nonzero elements of R. Since S is an R-module, $s(r/s) = r/1 \in S \cap R$, and therefore $S \cap R$ is nonzero.

Hence, Q is an injective R-module that is an essential extension of R, and thus Q is the injective envelope of R.

□

Examples. By the above theorem, $\mathbb{Q}$ is the injective envelope of $\mathbb{Z}$, and given a field k, $k(x)$ is the injective envelope of $k[x]$.

Let $R = k[x]$, and consider the ring of Laurent polynomials $k[x, x^{-1}]$ as an R-module. $k[x, x^{-1}]$ is the set of all k-linear combinations of integer powers of x.

It is clear that $k[x]$ is an R-submodule of $k[x, x^{-1}]$, and therefore we can form the quotient module $E = k[x, x^{-1}]/k[x]$.

The R-module structure on E is dictated by

$$x^a x^{-c} = \begin{cases} x^{a-c} & \text{if } a < c, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

We claim that E is the injective envelope of $R/xR = k[x]/(x)$, whose nonzero elements are equivalence classes of nonzero elements of k. Hence, as sets, we identify R/xR with k.

Since $R = k[x]$ is a PID, and E is a divisible R-module, E is an injective R-module.

To see that E is an essential extension of R/xR, consider the injective R-map $\varphi : k \to E$ defined by $\varphi : 1 \to 1/x$. If S is a nonzero R-submodule of E, then we can multiply a nonzero element of S by x raised to a sufficiently large integer power to obtain an element in the image of φ.

Hence, E is the injective envelope of R/xR.

Indecomposable Decompositions of Injective Modules over Noetherian Rings

In his 1958 paper *Injective Modules over Noetherian rings*, Eben Matlis gave a comprehensive description of injective modules over a Noetherian ring R. In the case R is commutative, he proved that indecomposable injective R-modules are precisely the injective envelopes of the modules $R/\mathfrak{p}$, for prime ideals $\mathfrak{p}$ in R.

We look at some results from this paper.

Definition. Let R be a ring. Given an R-module M and an R-submodule S of M, we say that S is a **direct summand** of M if there is an R-submodule T of M such that $M = S \oplus T$.

An R-module M is **indecomposable** if its only direct summands are 0 and M.

Examples. Every simple module is indecomposable. $\mathbb{Z}/6\mathbb{Z}$ is not an indecomposable abelian group, as $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. In fact, an abelian group is indecomposable if and only if it is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/p^n\mathbb{Z}$, where p is a prime integer and $n \in \mathbb{N}$.

Theorem. Suppose R is Noetherian, and let $\{M_i\}$ be a family of R-modules. Then $E(\bigoplus_i M_i) \cong \bigoplus_i E(M_i)$. This is proved by showing that the injective module $\bigoplus_i E(M_i)$ is an essential extension of $\bigoplus_i M_i$.

Definition. A left ideal J of a ring R is **irreducible** if there do not exist left ideals K and L of R, properly containing J, such that $K \cap L = J$.
If R is a PID, then an ideal $(a) \subseteq R$ is irreducible if and only if a is an irreducible element of R.

Example. (4) is an irreducible ideal of $\mathbb{Z}$. Indeed, suppose there are ideals (a) and (b) of $\mathbb{Z}$ such that $(4) = (a) \cap (b)$. Then $4 \in (a)$ and $4 \in (b)$, so $a|4$ and $b|4$. Hence, $a = 1, 2$, or 4, and $b = 1, 2$ or 4. If $a = 1$, then $(a) = \mathbb{Z}$, and $(4) = (b)$. Likewise, $a = 2 \Rightarrow (4) = (b)$. We conclude that $(a) = (4)$ or $(b) = (4)$, so (4) is an irreducible ideal.

Theorem. A module E over a ring R is an indecomposable, injective module if and only if $E \cong E(R/J)$, where J is an irreducible left ideal of R.

Theorem. If R is a left-Noetherian ring, then every injective R-module has a decomposition as a direct sum of indecomposable, injective R-modules.

This means that, given an R-module E, there is a collection of indecomposable R-modules $\{E_i\}_{i \in I}$ such that

$E \cong \bigoplus_{i \in I} E_i$.

Moreover, the indecomposable, injective direct summands in this decomposition are unique up to isomorphism and permutation of the indices.

Definition. Given an R-modules M, $\mathrm{Hom}_R(M, M)$ denotes the set of all R-homomorphisms from M to itself. We call such homomorphisms **endomorphisms**. $\mathrm{Hom}_R(M, M)$ is a ring with respect to pointwise addition, and multiplication given by composition of functions. That is, for $f, g \in \mathrm{Hom}_R(M, M)$, and $x \in M$,

$(f + g)(x) := f(x) + g(x)$, and
$(fg)(x) := f(g(x))$.

Definition. A ring R is a **local ring** if the set of non-units of R forms a two-sided ideal. If R is commutative, this is equivalent to R having a unique maximal ideal. It is known that a local ring contains no **idempotent** elements other than 0 and 1. $r \in R$ is an **idempotent** if $r^2 = r$.

Fact: If E is an indecomposable injective module, then for any nonzero submodules S and T of E, $S \cap T \neq 0$.

Theorem. Let E be an injective module over a ring R, and $H = \mathrm{Hom}_R(E, E)$. Then H is a local ring if and only if E is indecomposable.

Proof. ($\Rightarrow$) We prove the contrapositive. Suppose E is not indecomposable. Then E has nonzero submodules M and N such that $E = M \oplus N$. Define $p : M \oplus N \to M \oplus N$ by $p(m, n) = (m, 0)$ for all $(m, n) \in M \oplus N$ (projection onto the first summand). It is clear that p is an R-map. And for $(m, n) \in M \oplus N$,

$p^2(m, n) = p(p(m, n)) = p(m, 0) = (m, 0) = p(m, n)$. So $p^2 = p$. That is, p is an idempotent that is not the identity map or the zero map. Hence, H is not a local ring.

($\Leftarrow$) Now assume that E is indecomposable. If $f \in H$ is a unit, then clearly $\ker f = 0$. If $\ker f = 0$, then we have a short exact sequence

$0 \longrightarrow E \xrightarrow{f} E \xrightarrow{\pi} \mathrm{coker} f \longrightarrow 0$. Since E is injective, this short exact sequence splits, and therefore $E \cong E \oplus \mathrm{coker} f$. Since E is indecomposable, and E is nonzero, it follows that $\mathrm{coker} E = 0$, and therefore $\mathrm{im} E = E$, so f is a unit in H.

We have shown that $f \in H$ is a unit (invertible) if and only if $\ker f = 0$.

Now we show that the set of non-units of H forms a two-sided ideal I. Let g and h be non-units of H. Then $\ker g \neq 0$ and $\ker h \neq 0$. Thus, by the above fact, $\ker g \cap \ker h \neq 0$. Since $\ker g \cap \ker h \subseteq \ker(g + h)$, $\ker(g + h) \neq 0$, and therefore $g + h$ is a non-unit.

By considering cases, one can show that for each $f \in H$ and for each non-unit $g \in H$, fg is a non-unit, and gf is a non-unit. Hence, the set of non-units of H forms a two-sided ideal, and we conclude that H is a local ring. □

Definition. If I is an ideal in a commutative ring R, then the **radical** of I, denoted $\sqrt{I}$, is

$\sqrt{I} := \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$.

Definition. A proper ideal I of a commutative ring R is called **primary** if whenever x,$y \in I$, then $x \in I$ or $y^n \in I$ for some positive integer n. If I is primary, then $\sqrt{I}$ is a prime ideal. If $\sqrt{I} = \mathfrak{p}$, then we say that I is $\mathfrak{p}$-primary.

Theorem. A module E over a ring R is an indecomposable, injective module if and only if $E \cong E(R/I)$, where I is an irreducible left ideal of R.

Fact: If R is Noetherian, then an irreducible ideal $I \subseteq R$ is primary. If R is a PID, then an ideal is irreducible if and only if it is primary.

Theorem. Let R be a commutative Noetherian ring. There is a one-to-one correspondence between the prime ideals of R and the indecomposable, injective R-modules, given by $\mathfrak{p} \leftrightarrow E(R/\mathfrak{p})$, for $\mathfrak{p}$ a prime ideal of R ($\mathfrak{p} \in \text{Spec}R$). If I is an irreducible $\mathfrak{p}$-primary ideal, then $E(R/I) \cong E(R/\mathfrak{p})$.

Examples. For every prime number p, $E(\mathbb{Z}/p\mathbb{Z})$ is an indecomposable, injective $\mathbb{Z}$-module.

Suppose R is a PID and M is a finitely generated R-module. By the structure theorem for finitely generated modules over a PID,
$M \cong \bigoplus_{i=1}^{n} R/\mathfrak{q}_i$, where each $\mathfrak{q}_i$ is a primary ideal and $n \in \mathbb{N}$. Hence,

$E(M) \cong \bigoplus_{i=1}^{n} E(R/\mathfrak{q}_i)$, where each $E(R/\mathfrak{q}_i)$ is an indecomposable injective module. This is the unique decomposition of the injective envelope of M as a finite direct sum of indecomposable injective modules.

We know that if R is a left-Noetherian ring, then every injective R-module can be written as a direct sum of indecomposable, injective R-modules. Thus, if R is a commutative Noetherian ring, then an injective R-module E can be written as

$E \cong \bigoplus_{\mathfrak{p} \in \text{Spec}R} E(R/\mathfrak{p})^{\mu_{\mathfrak{p}}}$, where for each $\mathfrak{p} \in \text{Spec}R$,

$E(R/\mathfrak{p})^{\mu_{\mathfrak{p}}} = \bigoplus_{i \in I} E(R/\mathfrak{p})_i$, where $|I| = \mu_{\mathfrak{p}}$, and $E(R/\mathfrak{p})_i = E(R/\mathfrak{p})$ for each i.
Each $\mu_{\mathfrak{p}}$ is uniquely determined by E and $\mathfrak{p}$. Hence, the necessary data for writing our indecomposable decomposition of E is contained entirely in the cardinal numbers $\mu_{\mathfrak{p}}$, for $\mathfrak{p} \in \text{Spec}R$.

Indecomposable Decompositions of
Projective Modules over Artinian Rings

Theorem. Let R be a perfect ring and let P be a nonzero projective R-module. Then P is indecomposable if and only if $P \cong P_R(S)$, for some simple R-module S.

Assume R is commutative. Recall that the simple R-modules are precisely the R-modules $R/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal of R.

Lemma. Let R be a commutative Artinian ring. Then every prime ideal is maximal. Thus, an ideal of R is prime if and only if it is maximal. Moreover, R has only finitely many prime ideals.

Proof. Let $\mathfrak{p} \subseteq R$ be a prime ideal. Choose $x \in R \backslash \mathfrak{p}$. We obtain a decreasing sequence of ideals

$... \subseteq (x^3) \subseteq (x^2) \subseteq (x) \subseteq R$

Since R is Artinian, the sequence stabilizes. So there is a positive integer n such that $(x^n) = (x^{n+1})$, and thus there is an element $a \in R$ such that $x^n = ax^{n+1}$. Hence, $(1 - ax)x^n = 0 \in \mathfrak{p}$. Thus, $1 - ax \in \mathfrak{p}$ or $x \in \mathfrak{p}$. Since $x \notin \mathfrak{p}$, $x^n \notin \mathfrak{p}$, and therefore $1 - ax \in \mathfrak{p}$. Thus, there exists some $y \in \mathfrak{p}$ such that $1 - ax = y$, so $1 = y + ax$. Thus, $R = \mathfrak{p} + (x)$. So if $I \subseteq R$ is an ideal such that $\mathfrak{p} \subsetneq I \subseteq R$, then choosing $x \in I \backslash P$, we have $R = \mathfrak{p} + (x) \subseteq I \subseteq R$, so $I = R$. Therefore $\mathfrak{p}$ is maximal.

Let $S = \{\prod_{i=1}^{n} \mathfrak{p}_i : \mathfrak{p}_i \in \mathrm{Spec}R$ for $i = 1, ..., n$, and $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$ $\}$. This is a nonempty collection of ideals in R, and since R is Artinian, S has a minimal element $J = \prod_{i=1}^{n} \mathfrak{p}_i = \bigcap_{i=1}^{n} \mathfrak{p}_i$. Let $\mathfrak{p} \in \mathrm{Spec}R$. Then $J = \mathfrak{p}J \subseteq \mathfrak{p}$. Hence, $\mathfrak{p}$ contains $\mathfrak{p}_j$ for some j, and thus equals $\mathfrak{p}_j$, since all primes are maximal.

Hence, $\mathrm{Spec}R = \{\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_n\}$. □

Theorem. Let R be a commutative Artinian ring and let P be a projective R-module. Then

$P \cong \prod_{\mathfrak{p} \in \mathrm{Spec}R} P(R/\mathfrak{p})^{\pi(\mathfrak{p},P)}$, where for each $\mathfrak{p}$,

$P(R/\mathfrak{p})^{\pi(\mathfrak{p},P)} = \bigoplus_{i \in I} P_i(R/\mathfrak{p})$, where for each i, $P_i(R/\mathfrak{p}) \cong P(R/\mathfrak{p})$ and $|I| = \pi(\mathfrak{p}, P)$.

Injective Modules over Prüfer Rings

Definition. Let R be an integral domain, and let Q be its quotient field. R is a subring of Q under the injective ring homomorphism $\varphi : R \to Q$ given by $\varphi(r) = \frac{r}{1}$. A **fractional ideal** of R is an R-submodule I of Q such that there exists a nonzero ring element $r \in R$ such that $rI \subseteq R \subseteq Q$.

A fractional ideal I is **invertible** if there is a fractional ideal J such that $IJ = R$, where $IJ = \{\sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J\}$.

Definition. A **Prüfer domain** is an integral domain R in which every finitely generated nonzero ideal is invertible (The finitely generated nonzero ideals of R form a multiplicative group).

Examples of Prüfer domains. The ring of entire functions on the complex plane, and the ring of **integer-valued polynomials** with rational coefficients.

An integer-valued polynomail $P \in \mathbb{Q}[x]$ satisfies $P(n) \in \mathbb{Z}$ for every $n \in \mathbb{Z}$ e.g. $\frac{1}{2}x(x+1)$.

Univariate polynomial rings over **von Neumann regular** rings are Bézout domains (the sum of two principal ideals is principal), and thus Prüfer domains. A ring R is von Neumann regular if for all $a \in R$, there exists a (generalized inverse) $x \in R$ such that $a = axa$.

Conversely, if $R[x]$ is a Prüfer ring, then R is von-Neumann regular.

$\mathbb{Z}[x]$ and $\mathbb{Z}_4[x]$ are not Prüfer domains because $\mathbb{Z}$ and $\mathbb{Z}_4$ are not von-Neumann regular ($2 \in \mathbb{Z}_4$ does not have a generalized inverse).

Definition. A **valuation ring** R is an integral domain in which every two elements have a greatest common divisor which is equal to one of them. Equivalently, a valuation ring is a local Prüfer ring.

Given $a, b \in R$, a **greatest common divisor** of a and b is an element $d \in R$ such that $d|a$ and $d|b$ (there exist $x, y \in R$ such that $a = xd$ and $b = yd$), and any $r \in R$ that divides both a and b also divides d.

Examples of valuation rings. Any field. The ring of meromorphic functions on the complex plane.

$\mathbb{C}[x]$ is a Prüfer domain that is not a valuation ring, since it is not local.

Fact: The ideals of a valuation ring R are totally ordered by inclusion. Hence, for each pair of ideals $I, J \subseteq R$, $I \subseteq J$ or $J \subseteq I$.

Proof. Let $I, J \subseteq R$, and suppose $I \nsubseteq J$. Let $x \in I \backslash J$, $y \in J$, and $d = \gcd(x, y)$. $d = x$ or $d = y$. If $d = x$, then $x|y$, so $y = tx$ for some $t \in R$, and therefore $y \in I$. If $d = y$, then $y|x$, so $x = sy$ for some $s \in R$, and therefore $x \in J$, a contradiction. Hence, $d = x$, and $J \subseteq I$. □

Fact: If R is a valuation ring with quotient field Q, and if S is a proper R-submodule of Q, then there is a nonzero element $a \in R$ such that aS is an ideal of R.

Proposition. Let R be a valuation ring with quotient field Q. Then

1) $E_R(R/I)$ is an indecomposable, injective R-module for every ideal I of R, and every indecomposable, injective R-module is of this form.

2) If I is a proper ideal of R, then $E_R(R/I) \cong E_R(Q/I)$.

3) If I and J are proper ideals of R, then $E_R(R/I) \cong E_R(R/J)$ if and only if $I \cong J$.

Proof. 1) Let I be an ideal of R, and suppose that there exist ideals J and K of R such that $I = J \cap K$. Since R is a valuation ring, its ideals are totally ordered, and thus $J \subset K$ or $K \subset J$. WLOG, say $J \subset K$. Then $I = J$, so I is irreducible. We know that an R-module is an indecomposable, injective R-module iff it is isomorphic to the injective envelope of R/J, where J is an irreducible ideal. Since every ideal is irreducible, we obtain the desired result.

2) First we show that $E(Q/I)$ is indecomposable. It suffices to show that Q/I contains no nonzero R-submodules A and B such that $A \cap B = 0$. Let $A = S/I$ and $B = T/I$ be nonzero R-submodules of Q/I such that $A \cap B = 0$, where S and T are R-submodules of Q. If $S = Q$ or $T = Q$, then $A \cap B$ is nonzero. Hence, we may assume that S and T are proper R-submodules of Q. So there exists an element $a \neq 0$ in R such that aS and aT are ideals in R. We have the following isomorphisms of R-modules: $S/I \cong aS/aI$ and $T/I \cong aT/aI$, and thus aS/aI and aT/aI have zero intersection. Hence, $aS \cap aT = aI$. Since I is irreducible and $I \cong aI$, aI is irreducible. So either $aS = aI$ or $aT = aI$. This contradicts our assumption that A and B are nonzero R-modules, and therefore $E(Q/I)$ is indecomposable. Since R/I is a nonzero submodule of $E(Q/I)$, $E(Q/I)$ is the injective envelope of R/I.

3) Suppose I and J are isomorphic as R-modules via R-map $\varphi : I \to J$. We may assume that I and J are nonzero. Let a be a nonzero element of I. Then $\varphi(a)I = \varphi(aI) = a\varphi(I) = aJ$. Hence, letting $q = a/\varphi(a)$ in Q, we have $I = qJ$ in Q, and so as R-modules, $Q/I = Q/qJ \cong Q/J$, so $E(Q/I) \cong E(Q/J)$, and by 2), $E(R/I) \cong E(R/J)$. The converse is straightforward. □

Corollary: If S and T are R-submodules of Q, then $Q/S \cong Q/T$ if and only if $S \cong T$.

Corollary: If M is an injective R-module, then any element of M is contained in an indecomposable, injective direct summand of M.

proof: Let $x \in M$. Since Rx is cyclic, there is an ideal I of R such that $Rx \cong R/I$. Hence,
$E(Rx)$ is indecomposable and $E(Rx) \subset M$, by the minimality of the injective envelope of a module. Since $E(Rx)$ is an injective submodule of M, it is a direct summand of M.

Thus, if B is a finitely generated R-module, then $E(B)$ is a finite direct sum of indecomposable, injective R-modules. We saw that this is also the case for finitely generated modules over PIDs.

proof: Since R is a valuation ring, every finitely generated R-module is cyclic, and thus of the form R/I for some ideal I of R. Thus by Prop 1, $E(B)$ is an indecomposable, injective R-module.

Definition: Given a module M, a submodule $N \subseteq M$, and elements $x, y \in M$, we write $x \equiv y \pmod{N}$ if $x - y \in N$.

Let M be an R-module, and let $\{(M_\alpha, x_\alpha)\}_{\alpha \in A}$ be a collection of pairs of submodules and elements of M. We obtain a **set of congruences** with variable $x \in M$:

$x \equiv x_\alpha \pmod{M_\alpha}, \qquad \alpha \in A.$

A set of congruences is **finitely solvable** if for
every finite collection of inidces $\{\alpha_k\}_{k=1}^n$, there exist elements $\{y_k\}_{k=1}^n$ such that

$y_k \equiv x_{\alpha_k} \pmod{M_{\alpha_k}}$ for $k = 1, 2, ..., n$.

Definition: Let M be a module over a commutative ring R. M is linearly compact if every finitely solvable set of congruences

$x \equiv x_\alpha \pmod{M_\alpha}, \qquad \alpha \in A$

(where $x_\alpha \in M$, M_α are submodules of M),

has a simultaneous solution.

M is **semi-compact** if the above congruence condition holds whenever the submodules M_α are annihilators of ideals of R; that is, for each α, there exists an ideal $I_\alpha \subseteq R$ such that $M_\alpha = \{x \in M : xI_\alpha = 0\}$.

Proposition: Let C be an injective module over a commutative ring. Then C is semi-compact.

Proof. Let $x \equiv x_\alpha \pmod{C_\alpha}$ be a finitely solvable set of congruences, where $x_\alpha \in C$, and each submodule $C_\alpha \subseteq C$ is the annihilator in C of an ideal I_α in R. Let I be the ideal in R generated by all of the I_α's.

Let $a \in I$. There are finitely many indices $\alpha_1, ..., \alpha_n$ such that $a \in I_{\alpha_1} + I_{\alpha_2} + ... + I_{\alpha_n}$. Since the set of congruences is finitely solvable, there is an element $y \in C$ such that $y \equiv x_{\alpha_k} \pmod{C_{\alpha_k}}$ for $k = 1, ..., n$.

Define an R-map $f : I \to C$ by $f(a) = ay$ for $a \in I$.

Let us verify that f is a well-defined function. Let $a \in I$ be as above, and suppose we have a second collections of indices $\beta_1, ..., \beta_m$ such that $a \in I_{\beta_1} + I_{\beta_2} + ... + I_{\beta_m}$. □