MAS511 2020Spring Homework#08

Problem 1

P1(1)

When R is a field, prove that the projective dimensions of all R-modules are 0.

Answer for P1(1)

Let M be an arbitrary R-module. Let $I \subseteq R$ be a left ideal and $g : I \to M$ is a homomorphism. Since R is a field, $I = (0)$ or $I = R$. (By commutativity of R, left ideal is two-sided, and simple as a field.) Suppose that $I = (0)$. Then, $g(0) = 0$. Then, we can extend g to $\tilde{g} : R \to M$ such that $\tilde{g} \equiv 0$. Suppose that $I = R$. Then g is already a function $R \to M$. Then, just take a $\tilde{g} = g$. It's an extension of g. Therefore, for every left ideal $I \subseteq R$, any homomorphisms $g : I \to M$ can be extended to the map $R \to M$. Thus, by Baer's Criterion, M is injective. Therefore, every R-module is injective. This shows that any field is semisimple.

Then, by Wedderburn's Theorem, every R-module is projective. (See Problem 2 (2) $\Rightarrow$ (1))

Let M be an arbitrary R-module. Then, M is projective. Take

$$0 \to M \xrightarrow{\mathrm{Id}_M} M \to 0$$

This is an exact sequence since Id_M is a bijective homomorphism. And since M is projective, it's a projective resolution of M. Therefore, the projective dimensions of M is at most 0. Since projective dimension is laid on $\mathbb{Z}^{\geq 0} \cup \{\infty\}$, $pd_R M = 0$. □

P1(2)

Let R be a PID. Let M be a finitely generated R-module. Prove that M always has a projective resolution of length ≤ 1. (Hint: Theorem A)

Answer for P1(2)

Let M be a finitely generaetd R-module. Then, there is a generator $\mathcal{B} = \{b_1, \cdots, b_n\} \subseteq M$. In other words, for any element m of M, there are $r_1, \cdots, r_n \in R$ such that

$$m = \sum_{k=1}^{n} r_k b_k$$

Then, let $\varphi : R^n \to M$ such that

$$\varphi(r_1, \cdots, r_n) = \sum_{k=1}^{n} r_k b_k$$

Then, it's well-defined and surjective, since $\operatorname{im}\varphi$ takes every possible linear combinations of the basis $\mathcal{B}$ of M.

Note that φ is a homomorphism: Let $\mathbf{r} = (r_1, \cdots, r_n) \in R^n$, $\mathbf{s} = (s_1, \cdots, s_n) \in R^n$ and $a \in R$. Then,

$$\begin{aligned}\varphi(\mathbf{r}+\mathbf{s}) &= \sum_{k=1}^{n}(r_k + s_k)b_k \\ &= \sum_{k=1}^{n}(r_k b_k + s_k b_k) \\ &= \sum_{k=1}^{n} r_k b_k + \sum_{k=1}^{n} s_k b_k = \varphi(\mathbf{r}) + \varphi(\mathbf{s})\end{aligned}$$

$$\begin{aligned}\varphi(a\mathbf{r}) &= \sum_{k=1}^{n}(a r_k)b_k \\ &= a\sum_{k=1}^{n} r_k b_k = a\varphi(\mathbf{r})\end{aligned}$$

This shows that φ is an homomorphism.

Let $K = \ker\varphi$. Then, we know two facts: First, there is a canonical injective homomorhpism ι from K to R^n, which is an identity for every element of K. In this case, $\operatorname{im}\iota = K = \ker\varphi$. Second, since R is PID, R^n is a free R-module of rank n and K is a R-submodule of R^n, K is also free by the Theorem (A).

Then, we can construct an short exact sequence:

$$0 \longrightarrow K \xrightarrow{\iota} R^n \xrightarrow{\varphi} M \longrightarrow 0$$

because ι is injective, $\operatorname{im}\iota = K = \ker\varphi$, and φ is surjective. Since K and R^n are free, they are projective. Thus, $\cdots \to 0 \to K \to R^n \to M$ is a projective resolution of length 1. Thus, the projective dimension of M should be less or equal to 1. □

P1(3)

Give an example of a concrete PID R and a finitely generated R-module M such that $pd_R M$ is precisely 1.

Answer for P1(3)

Since every finitely generated R-module for PID R has a projective dimension 0 or 1, we need to find a PID R and a finitely generated R-modlue which does not have a projective resolution of length 0.

Let R be a PID and M be an arbitrary finitely generaetd R-module. Suppose that $pd_R M = 0$. Then, there is a projective resolution

$$\cdots \to 0 \to N \xrightarrow{\epsilon} M \to 0$$

In this case, ϵ must be injective and surjective. Thus, ϵ is an isomorphism between N and M. Since M's isomorphic image, N, is projective, M should be projective too.

In other words, if M is not projective, $pd_R M > 0$. Therefore, it's enough to find some non-projectiev R-module.

Let $R = \mathbb{Z}$. $\mathbb{Z}$ is an ED thus a PID, but not a field since $2^{-1} \in \mathbb{Q} \setminus \mathbb{Z}$. Let $M = \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$.

$\mathbb{Z}_2$ is not projective. Because, if we take

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "f"] & \mathbb{Z}_2 \arrow[r] & 0 \\
& \mathbb{Z}_2 \arrow[u, "g"] \arrow[ul, dashed, "\tilde{g}"] &
\end{tikzcd}$$

where $f : \mathbb{Z} \to \mathbb{Z}_2$ is a canonical surjection such that $x \mapsto x + 2\mathbb{Z}$, and g is an identity map. If $\mathbb{Z}_2$ is projective, since f is surjective, ther should be a lift $\tilde{g}$ of g such that $g = f \circ \tilde{g}$. Note that $\tilde{g}$ must be a R-module homomorphism. Because module homomorphism maps 0 to 0, $\tilde{g}(0) = 0$. Also,

$$0 = \tilde{g}(0) = \tilde{g}(1 + 1) = \tilde{g}(1) + \tilde{g}(1)$$

However, for $n \in \mathbb{Z}$, $n + n = 0$ iff $n = 0$. Thus, $\tilde{g}(1) = 0$. This shows that there is only one homomorphism from $\mathbb{Z}_2$ to $\mathbb{Z}$, which is a zero map. Thus, $\tilde{g} \equiv 0$. However, in this case $0 = (f \circ \tilde{g})(1) \neq g(1) = 1$. Thus, there cannot be a lift of g by f.

$\mathbb{Z}_2$ is finitely generated. More specifically, the basis of $\mathbb{Z}_2$ is $\{1\}$. ($\because$ Since $\mathbb{Z}_2$ is non-zero, the generating set of $\mathbb{Z}_2$ must contains at least one non-zero element. Since $0 = 0 \cdot 1$, $1 = 1 \cdot 1$, 1 generates every element of $\mathbb{Z}_2$.)

Therefore, the projective dimension of $\mathbb{Z}_2$ as a $\mathbb{Z}$-module must be greater than 0 since $\mathbb{Z}_2$ is not projective, and the projective dimension of $\mathbb{Z}_2$ as a $\mathbb{Z}$-module must be less or equal to 1 since $\mathbb{Z}_2$ is a finitely generated module of PID. Thus, the projection dimension of $\mathbb{Z}_2$ as a $\mathbb{Z}$-module is 1. $\square$

Note that we can easily find a projective resolution of $\mathbb{Z}_2$ of length 1, which is,

$$\cdots \to 0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}_2 \to 0$$

where $f : \mathbb{Z} \to \mathbb{Z}$ is a map such that $x \mapsto 2x$ and $g : \mathbb{Z} \to \mathbb{Z}_2$ is a canonical surjection such that $x \mapsto x + 2\mathbb{Z}$. In this case, f is injective, g is surjective, $\operatorname{im} f = 2\mathbb{Z} = \ker g$. Thus, the above sequence is exact. Also, since $\mathbb{Z}$ is a free $\mathbb{Z}$-module of rank 1, it's projective. Thus the above sequence gives a projective resolution of $\mathbb{Z}_2$.

P1(4)

Let $R = k[y_1, y_2]$. Give an example of a finitely generated R-module M, such that $pd_R M \geq 2$.

Answer for P1(4)

For convinience let's change the indeterminates y_1 and y_2 to x and y. Since k is a field, $k[x]$ is an ED and $k[x, y]$ is a UFD.

$M = k[x, y]/(x, y) \simeq k$.

First, I'll introduce a lemma:

Definition 1. R-module M is torsion free, if for any non-zero element m of M, $rm = 0$ if and only if $r = 0$ for $r \in R$.

Lemma 1. *Let R be an integral domain. Every flat R-module is torsion-free.*

Proof. Suppose that M is flat but not a torsion-free. Then there is a non-zero $m \in M$ and non-zero $r \in R$ such that $rm = 0$.

Note that r is a non-unit. (If not, $m = r^{-1}rm = r^{-1}0 = 0$ and it gives a contradiction.) This shows that if $sm = 0$ for $s \in R$ then $s = 0$ or s is a non-unit.

Let $f : R \to R$ such that $x \mapsto xr$. Then, f is injective, because if $f(x) = f(y)$ for $x, y \in R$, $xr = yr$ and $x = y$ by cancellation law.

Take a exact sequence

$$0 \to R \xrightarrow{f} R \to \operatorname{coker} f \to 0$$

Because M is flat,

$$0 \to R \otimes_R M \xrightarrow{f \otimes_R M} R \otimes_R M \to \operatorname{coker} f \otimes_R M \to 0$$

is exact. It means, $f \otimes_R M = f \otimes \mathrm{Id}_M$ is injective.

Note that $1 \otimes m$ is non-zero. ($\because$ If $1 \otimes m = 0$, there should be some $s \in S^\times$ such that $sm = 0$ so that $1 \otimes m = s^{-1} \otimes sm = s^{-1} \otimes 0 = 0$. However, since s is a unit, sm cannot be zero.)

However, $(f \otimes_R M)(1 \otimes m) = r \otimes m = 1 \otimes rm = 1 \otimes 0$. Thus, $\ker(f \otimes_R M)$ contains a non-zero element $1 \otimes m$. Therefore, $f \otimes_R M$ cannot be injective and it's an contradiction.

Therefore, if M is flat, it must be torsion-free. $\square$

Since R is an ID and every projective R-module is flat, projective R-module is torsion-free.

$M = k[x, y]/(x, y)$ is not projective, because it's not torsion-free. (e.g. $x \cdot \overline{1} = \overline{x} = 0$) Therefore, $pd_R M > 0$. (Because $pd_R M = 0$ then M should be projective. See the Proof of (3).)

Let's show that there cannot be a projective resolution of length 1. Suppose that there is a exact sequence with projective R-modules P, Q:

$$0 \to P \to Q \xrightarrow{f} k[x, y]/(x, y) \to 0$$

where P is non-zero. Then, because the injectivity of $P \to Q$, $P \simeq \operatorname{im}(P \to Q) = \ker f$ and we obtain an exact sequence

$$0 \to \ker f \to Q \xrightarrow{f} k[x, y]/(x, y) \to 0$$

For each $q \in Q$, if there is $r \in Q$ such that $q = xr$, then $f(xr) = xf(r) = \overline{xr} = \overline{0}$. Thus, $q \in \ker f$. In the same way, if there is $r \in Q$ such that $q = yr$, $q \in \ker f$. Thus, $(x, y) \cdot Q = \{pq \mid q \in Q, p \in (x, y)\} \subseteq \ker f$.

Since f is surjective, there is $q \in Q$ such that $f(q) = \overline{1}$. Note that since this q is not in $\ker f$, $xq, yq \in \ker f$ has a special property that there is no $r \in \ker f$ such that $xr = xq$ or $yr = yq$. (It's because, if such r exists, since R is UFD, we can use Cancellation Law to obtain $r = q$. It makes a contradiction since $r \in \ker f$ but $q \notin \ker f$.)

Then, make a exact sequence:

$$0 \to (x, y) \xrightarrow{g} k[x, y] = R \xrightarrow{h} k[x, y]/(x, y) \to 0$$

where g is an injection, and h is a canonical surjection. Then, apply $- \otimes_R \ker f$ functor.

$$0 \to (x, y) \otimes_R \ker f \xrightarrow{g \otimes_R \ker f} k[x, y] \otimes_R \ker f \xrightarrow{h \otimes_R \ker f} k[x, y]/(x, y) \otimes_R \ker f \to 0$$

Since $\ker f$ is projective, thus flat, the above sequence must exact.

Note that $x \otimes (y \cdot q) \neq y \otimes (x \cdot q)$ in $(x, y) \otimes_R \ker f$. Because there are no other representation of $x \otimes (yq)$. In other words, for a single tensor product term, there are only one equivalence relation such that $ar \otimes b = a \otimes rb$ for $r \in R$. However, for $x \otimes (yq)$, If $x = ar$ where $a \in (x, y)$, since the degree of a must be greater than 0, $\deg r$ must be 0. Thus, in this case, only the element of k can be passed from left to right. Also, since q is not in $\ker f$, polynomial with degree greater than 0 cannot be passed from right to left. Thus, we cannot make any common terms between $x \otimes (y \cdot q)$ and $y \otimes (x \cdot q)$. And they cannot be equal.

However,

$$\begin{aligned}(g \otimes_R \ker f)(x \otimes (y \cdot q) - y \otimes (x \cdot q)) &= x \otimes (y \cdot q) - y \otimes (x \cdot q) \\ &= 1 \otimes (xy \cdot q) - 1 \otimes (yx \cdot q) \\ &= 1 \otimes (xy \cdot q) - 1 \otimes (xy \cdot q) \\ &= 0 \otimes (xy \cdot q) = 0\end{aligned}$$

This shows that $\ker(g \otimes_R \ker f)$ contains a non-zero element $x \otimes (y \cdot q) - y \otimes (x \cdot q)$ Thus, $g \otimes_R \ker f$ is not injective. But it's a contradiction, because $g \otimes_R \ker f$ is injective by the flatness of $\ker f$.

Therefore, $\ker f$ cannot be projective, and P cannot be projective too.

Therefore, the length of any projective resolution of $k[x, y]/(x, y)$ over $k[x, y]$ must be at least 2 (or infinity). $\square$

Problem 2

Prove below:

Theorem 1. *(Wedderburn-Artin)*

Let R be a ring with unity. Then TFAE:

(1) Every R-module is projective.

(2) Every R-module is injective.

(3) Every R-module is completely reducible.

(4) The ring R considered as a left R-module is a direct sum $R = L_1 \oplus \cdots \oplus L_n$ of simple R-modules L_i, with $L_i = Re_i$, such that $e_ie_j = \delta_{ij}e_i$ and $\sum e_i = 1$.

(5) As rings, R is isomorphic to $R_1 \times \cdots \times R_r$ where $R_j = M_{n_j}(D_j)$, for some division ring D_j. The integer r, n_j and the ring D_j are unique.

$M_n(R)$ is a matrix algebra for the ring R.

Proof

First, let's introduce slightly different statement of Wedderburn-Artin Theorem (4):

Theorem 2. *Continue from Wedderburn-Artin:*

(4-1) The ring R considered as a left R-module is a direct sum $R = L_1 \oplus \cdots \oplus L_n$ of simple R-modules L_i, with $L_i = Re_i$, such that e_i is non-zero idempotent, $e_ie_j = \delta_{ij}e_i$ and $\sum e_i = 1$. The integer n is unique, and L_i is unique up to reordering.

Proof direction:

- (1) $\Leftrightarrow$ (2)
- (1), (2) $\Leftrightarrow$ (3)
- (3) $\Leftrightarrow$ Existency of (4-1)
- (4) $\Leftrightarrow$ Existency of (4-1)
- Existency of (4-1) $\Leftrightarrow$ Existency of (5)
- Uniqueness of (5)

(1) $\Rightarrow$ (2)

Suppose all R-modules are projective. Let I be an arbitrary R-module.

Take an exact sequence $0 \to I \to M \to N \to 0$. Since every R-modules are projective, N is projective. Thus, the exact sequence is split. Therefore, every exact sequence $0 \to I \to M \to N \to 0$ are split.

Therefore, I is injective. $\square$

(2) ⇒ (1)

Suppose all R-modules are injective. Let P be an arbitrary R-module.

Take an exact sequence $0 \to M \to N \to P \to 0$. Since every R-modules are injective, M is injective. Thus, the exact sequence is split. Therefore, every exact sequence $0 \to M \to N \to P \to 0$ are split.

Therefore, P is projective. □

(1), (2) ⇒ (3)

Suppose all R-modules are projective and injective.

Note that for this R, R-module is irreducible if and only if it's indecomposable. Irreducible ⇒ indecomposible is trivial. If R-module M is reducible, Then, there is non-zero proper submodule $N \subsetneq M$. Then, take N/M and make a exact sequence: $0 \to N \to M \to M/N \to 0$. Since every R-modules are injective, N is injective and the above short exact sequence splits. Thus, $M = N \oplus M/N$. This shows that M is decomposible.

Also, above process show that if we take any non-zero proper submodule N of M, there is a direct summand N' such that $M = N \oplus N'$. As we know that $M/0 = M$ and $M = M \oplus 0 = 0 \oplus M$, every R-module's R-submodule is a direct summand.

Note that for any R-module M, there is an irreducible submodule of M. First, let $M = Rx$ for some $x \in R$. Then, every submodule of M is an ideal of R. In this case, there is a maximal right ideal of Rx, N, by taking the union of all ideal of Rx which does not contain x. Then, $M = N \oplus N'$ for some R-module N'. If N' is reducible, there is a submodule S, S' of N' such that $N' = S \oplus S'$. Then, x must be contained in exactly one of S or S'. WLOG let's assumed that $x \in S$. Then, $x \notin S'$. Then, $S' \cup N$ is larger than N, which does not contain x. Thus, it violates the maximality of N. Therefore, N' must irreducible. For arbitrary R-module M, because M is proective, M is a direct summand of some free R-module $\bigoplus_\Lambda R$. Thus, M is isomorphic to some direct sum of ideals of R. If M is non-zero reducible, there is some $\alpha \in \Lambda$ such that the α-th entry of the isomorphic image of M is the non-zero ideal of R. Then, it has an irreducible submodule N. Then, the inverse image of N into M is an irreducible submodule.

Let S be a sum of every irreducible submodules of M. Then, there is a R-submodule S' of M such that $M = S \oplus S'$. (S' may be zero.) Suppose that $S' \neq 0$. If S' is irreducible, it's a contradiction because it should be in S. Then, S' should contain an irreducible submodule direct summand. But this also makes a contradiction since every irreducible submodule should be in S. Thus, S' must be 0 and $M = S$. Thus, M is a sum of some irreducible submodules. Let $M = \sum_{\alpha \in \Lambda} M_\alpha$

Then, for some index subset $S \subseteq \Lambda$, $\sum_{\alpha \in S} M_\alpha$ can be a direct sum $\bigoplus_{\alpha \in S} M_\alpha$ (if M_α are disjoint except 0...) For this kind of sums, which are direct sums, we can give a partial order $\subseteq$, which is the set inclusion relation. Then, if we pick any chains of $\subseteq$, by taking union of all items, we have a maximum element, and the element also a direct sum. (Because, if $\sum_{\alpha \in S} M_\alpha$ is maximum, for any M_a, M_b for $a, b \in S$, there is a element $\sum_{\alpha \in T} M_\alpha$ in the chain such that $S \subseteq T$ and $a, b \in T$. Thus, M_a and M_b should be disjoint except 0.) Since M has at elast one irreducible submodule, which can be considered as a direct sum of irreducible submodules, by Zorn's Lemma, there is a maximal element. Let $M' = \sum_{\alpha \in \Gamma} M_\alpha = \bigoplus_{\alpha \in \Gamma} M_\alpha$ be the maximal element in M. If $M = M'$ we are done. And suppose that $M' \neq M$. (i.e. $M'' \neq 0$) As we showed above, there is R-module M'' such that $M = M' \oplus M''$. If M'' is irreducible, then M is a direct sum of a direct sum of irreducible modules, M', and a irreducible module M''. Thus M is a direct sum of irreducible modules. If M'' is reducible, there is a irreducible submoddule $M''' \subseteq M''$. However, since M''' and M' are disjoint except 0, $M' + M''' = M' \oplus M'''$. It violtaes the maximality of M'.

Therefore, M is a direct sum of irreducible modules. It means M is completely reducible. $\square$

(3) ⇒ (1), (2)

Suppose all R-modules are completely reducible.

Let's take an arbitrary exact sequence

$$0 \to K \xrightarrow{f} L \xrightarrow{g} M \to 0$$

Since each K, L, M are completely reducible, there are some irreducible R-modules $\{K_\alpha\}_{\alpha\in\Gamma}, \{L_\alpha\}_{\alpha\in\Lambda}, \{M_\alpha\}_{\alpha\in\Omega}$ such that $K = \bigoplus_{\alpha\in\Gamma} K_\alpha$, $L = \bigoplus_{\alpha\in\Lambda} L_\alpha$, $M = \bigoplus_{\alpha\in\Omega} M_\alpha$. Then, the below is exact:

$$0 \to \bigoplus_{\alpha\in\Gamma} K_\alpha \xrightarrow{f} \bigoplus_{\alpha\in\Lambda} L_\alpha \xrightarrow{g} \bigoplus_{\alpha\in\Omega} M_\alpha \to 0$$

Let's think about submodules of L. Since each L_α are irreducible, only submodules of L_α is 0 or L_α. Let $\pi_\alpha : L \to L_\alpha$ be a canonical projection. Suppose that there is some submodule $L' \subseteq L$. Then, $\pi_\alpha(L')$ must be a submodule, since π_α is a homomorphism. Thus, there are only two choices about $\pi_\alpha(L')$: $\pi_\alpha(L') = L_\alpha$ or $\pi_\alpha(L') = 0$. Thus, L' must be a form of $L' \simeq \bigoplus_{\alpha\in\Lambda'} L_\alpha$ where $\Lambda' \subseteq \Lambda$.

Note that $\operatorname{im} f$ is an isomorphic image of K since f is injective. In addition, $\operatorname{im} f \subseteq L$. It means, there is a subset $S \subseteq \Lambda$ such that $\operatorname{im} f \simeq \bigoplus_{\alpha\in S} L_\alpha$. And, $K \simeq \bigoplus_{\alpha\in S} L_\alpha$. Let $\varphi : \bigoplus_{\alpha\in S} L_\alpha \to K$ be an inverse of f.

Also, we can make a projection $\pi : L \to \operatorname{im} f$ such that: $\pi(\mathbf{a}) = \mathbf{a}'$ where the α-th entry of $\mathbf{a}'$ is the α-th entry of $\mathbf{a}$ if $\alpha \in S$, otherwise α-th entry of $\mathbf{a}'$ is zero.

Thus, $\varphi \circ \pi$ give a homomorphism from L to K. And since $\operatorname{Cod}(\pi) = \operatorname{im} f$, $\pi \circ f = f$ and $\varphi \circ \pi \circ f = \varphi \circ f = \mathrm{Id}_K$. Therefore, $0 \to K \to L \to M \to 0$ splits.

Since $0 \to K \to L \to M \to 0$ was chosen arbitrarily, every exact sequence of R-modules splits. If we fix K and just change L, M, we obtain the result that K is injective. If we fix M and just changed K, L, we obtain the result that M is projective.

Thus, it shows that every R-module is injective and projective. $\square$

(3) ⇒ Existency of (4-1)

Suppose that every R-module is completely reducible.

Then, R as a left R-module is also completely reducible. Then, there are irreducible R-modules $\{R_\alpha\}_{\alpha\in\Lambda}$ such that

$$R = \bigoplus_{\alpha\in\Lambda} R_\alpha$$

Since $1 \in R$, there is some finite subset S of Λ and $\{r_\alpha\}_{\alpha\in\Lambda}$ where $r_\alpha \neq 0$ iff $\alpha \in S$,

$$1 = \bigoplus_{\alpha\in\Lambda} r_\alpha$$

Note that an ideal $R \cdot 1$ is R. Therefore,

$$R = R \cdot 1 = \bigoplus_{\alpha\in\Lambda} R'_\alpha \simeq \bigoplus_{\alpha\in S} R_\alpha$$

where $R'_\alpha = R \cdot r_\alpha$ if $\alpha \in S$, and $R'_\alpha = 0$ otherwise. Since S is a finite set, for $n = |S|$, we can reindex

S into $\{1, \cdots, n\}$. Then, we obtain

$$R = \bigoplus_{k=1}^{n} R_k = R_1 \oplus \cdots \oplus R_k$$

Thus, R can be expressed as a finite direct sum of some R-submodules of R.

Note that since each R_k is closed under a multiplication by R, they are left ideals of R. Also, since R_k is irreducible, there is no proper non-zero R-submodule of R_k for each k. It means, each R_k are minimal (simple?) left ideal.

Note that every minimal left ideal I of R is a left principal ideal. Because, if not, for any $x \in I \setminus \{0\}$, Rx is a left ideal of R. Since $x \neq 0$, $Rx \neq \{0\}$ ($\because$ Rx must contains $1 \cdot x = x$) Thus $Rx = I$. Note that since x is chosen arbitrarily, I can be expressed for any non-zero $x \in I$ as Rx.

Let $(r_1, \cdots, r_n)$ be the image of 1_R into the $\bigoplus_{k=1}^{n} R_k$. Because of the construction of index set S, every r_k must be non-zero. Thus, $R_k = Rr_k$ for each k. Also, the direct sum of r_k is 1.

Then,

$$r_k \cdot (r_1, \cdots, r_n) = (0, \cdots, 0, r_k, 0, \cdots 0)$$

must holds, because $(r_1, \cdots, r_n)$ is an identity. Thus, $r_k r_j = \delta_{jk} r_k$.

Therefore, if we take $e_k = r_k$ and $L_k = Re_k$, $R = L_1 \oplus \cdots \oplus L_n$, each L_k are simple, $e_i e_j = \delta_{ij} e_i$ and $\sum e_i = 0$ holds. □

Existency of (4-1) ⇒ (3)

Note that (4-1) means R as a left R-module is completely reducible.

Let M be an arbitrary left R-module. Then, there is a generating set $\mathcal{B} = \{b_\alpha\}_{\alpha \in \Lambda}$ of M. Then, there is a homomorphism $\varphi : \bigoplus_\Lambda R \to M$ such that

$$\varphi((r_\alpha)_{\alpha \in \Lambda}) = \bigoplus_{\alpha \in \Lambda} r_\alpha b_\alpha$$

Then, the image of φ is M. Therefore, M is isomorphic to the submodule of $\bigoplus_\Lambda R$.

Since R is a direct sum of simple R-submodules, $\bigoplus_\Lambda R$ is also a direct sum of simple R-submodules.

Since a submodule of a direct sum of simple R-submodules is a direct sum of simple R-submodules, M is isomorphic to some direct sum of simple R-submodules. (See the proof of (3) ⇒ (1), (2).)

Thus M is a direct sum of R-submodules.

Since M is chosen arbitrarily, every R-modules are completely reducible. □

(4) ⇒ Existency of (4-1)

Note that $e_i e_j = \delta_{ij} e_i$ shows that e_i is idempotent. Then, there are two possibility: $e_i = 0$ or not. If $e_i = 0$, then $Re_i = 0$. Thus, even if we remove L_i from the direct sum $\bigoplus_{i=1}^{n} L_i$, it is still R. Also, subtracting by e_i, which is zero, from $\sum e_i = 1$ does not change the sum. Therefore,

$$R = \bigoplus_{k=1}^{i-1} Re_k \oplus \bigoplus_{k=i+1}^{n} Re_k$$

and $\sum_{k \neq i} e_k = 1$

Since there are only finite number of e_k, just find all e_k which is zero and omit them. Then, after reordering, we obtain new $n' \le n$, non-zero idempotent $\{e'_k\}_{k=1}^{n'} \subseteq \{e_1, \cdots, e_n\}$ such that

$$R = \bigoplus_{k=1}^{n'} Re'_k$$

, $e'_i e'_j = \delta_{ij} e'_i$ and $\sum e'_i = 1$. $\square$

Existency of (4-1) $\Rightarrow$ (4)

This is trivial since the statement (4-1) is stronger than one of (4). $\square$

Existency of (4-1) $\Rightarrow$ Existency of (5)

Let's begin with some notes.

First, $e_k R e_k$ is a division ring for each k. To show this fact, it's enough to show that $e_k R e_k$ contains units of every non-zero elements. First $e_k = e_k^2 = e_k 1 e_k$ is an identity of $e_k R e_k$. ($\because$ $e_k a e_k e_k 1 e_k = e_k a e_k^3 = e_k a e_k$ and $e_k 1 e_k e_k a e_k = e_k^3 a e_k = e_k a e_k$ for any $a \in R$.) Let $e_k a e_k \in e_k R e_k$ be a non-zero element. Then, $R(e_k a e_k)$ is an ideal contained in Re_k. ($\because$ For any $r \in R$, $re_k a e_k \in R(e_k a e_k)$ and since $re_k a \in R$ $(re_k a)e_k \in Re_k$.) However, since Re_k is simple, $Re_k a e_k$ is 0 or Re_k. But since the non-zero element $e_k a e_k = 1 \cdot e_k a e_k$ is in $Re_k a e_k$, $Re_k a e_k$ is non-zero. Thus, $Re_k a e_k = Re_k$. Then, there is $r \in R$ such that $re_k a e_k = e_k$. Then, because $e_k^2 = e_k$, $(e_k r e_k)(e_k a e_k) = e_k r e_k a e_k = e_k^2 = e_k$. Thus, $e_k r e_k$ is the inverse of $e_k a e_k$ in $e_k R e_k$.

$(Re_k)e_k(Re_k) = Re_k$. First, since $(Re_k)e_k \subseteq R$ and Re_k is a left ideal, $(Re_k)e_k(Re_k) \subseteq Re_k$. Since Re_k is simple, $(Re_k)e_k(Re_k)$ is 0 or Re_k. Since $(e_k e_k)e_k(e_k e_k) = e_k^5 = e_k$, which is non-zero, is in $(Re_k)e_k(Re_k)$, $(Re_k)e_k(Re_k)$ is non-zero. Thus, $(Re_k)e_k(Re_k) = Re_k$. Since every element of $(Re_k)e_k(Re_k)$ is a finite sum of $(a_i e_k)e_k(b_i e_k)$ for $a_i, b_i \in R$, there is $n_k \in \mathbb{N}$ and $a_i, b_i \in R$ such that

$$1 = \sum_{i=1}^{n_k} (a_i e_k) e_k (b_i e_k) = \sum_{i=1}^{n_k} a_i e_k b_i e_k$$

Note that for any division ring D, every module M over D is free. This can be shown as follows: since D is a simple ring, as the proof of Problem 1(1), we can show that every D-module is injective using Baer's Criterion. Then, by (1) $\Leftrightarrow$ (2), we obtain every D-module is projective. Thus, for any D-module M, it's a direct summand of $\bigoplus_\Lambda D$. However, since D is simple, the only possible submodule of $\bigoplus_\Lambda D$ is another free D-module $\bigoplus_\Gamma D$. ($\because$ each entry of the submodule of M must be a submodule of D, but there are only two possible submodule of D one is 0 and the other one is D.) Thus, M must be some free D-module. This implies that we can say about basis for D-module.

Re_k is a finitely generated right $e_k R e_k$-module. First, since Re_k is an ideal, it's an abelian group. Let $e_k R e_k$ acts on the left side of Re_k as:

$$(re_k) \cdot (e_k s e_k) = (re_k)(e_k s e_k) = (re_k s)e_k$$

Since $re_k s$ is in R, it's in Re_k. Thus the action is closed. Since it's an action between rings, it satisfies all properties of module. Also, for arbitrary $r \in R$,

$$re_k = \left(\sum_{i=1}^{m_k} a_i e_k b_i e_k \right) re_k = \sum_{i=1}^{m_k} a_i (e_k (b_i e_k r) e_k)$$

Since $b_i r \in R$, $e_k b_i e_k r e_k \in e_k R e_k$. Thus, $\mathcal{A}_k = \{a_i\}_{i=1}^{m_k}$ generates every element of Re_k. Thus, Re_k is finitely generated, such that $Re_k \simeq (e_k R e_k)^{m_k}$.

In this case, we can reduce the number of n_k as small as possible to obtain $\mathcal{A}_k$ which is a basis of Re_k.

What we want to say is $Re_k \simeq M_{n_k}(e_kRe_k)$.

Note that $M_{n_k}(e_kRe_k) \simeq \mathrm{Hom}_{e_kRe_k}(Re_k, Re_k)$. It's because Re_k is n-dimensional module over e_kRe_k.

Since Re_k is simple, by Schur's Lemma, $\mathrm{Hom}_R(Re_k, Re_k)$ is a division ring. Then, take $f \in \mathrm{Hom}_R(Re_k, Re_k)$. There is $f(e_k) = ae_k$ for some $a \in R$. Then, $f(re_k) = rf(e_k) = rae_k$. This shows that $\mathrm{Hom}_R(Re_k, Re_k)$ is determined that where e_k is mapped to.

Make a homomorphism $F : \mathrm{Hom}_R(Re_k, Re_k) \to e_kRe_k$ such that $F(f) = e_kf(e_k)$. Since both $\mathrm{Hom}_R(Re_k, Re_k)$ and e_kRe_k are simple as division ring, and F is non-zero map since Re_k contains at least one non-zero element a and it makes a homomorphism $e_k \mapsto ae_k$, which is non-zero map, F is an isomorphism. Thus, $e_kRe_k \simeq \mathrm{Hom}_R(Re_k, Re_k)$.

Make a homomorphism $G : Re_k \to \mathrm{Hom}_{e_kRe_k}(Re_k, Re_k)$ such that $G(re_k) : ae_k \mapsto re_kae_k$. This is injective since if $G(re_k) \equiv 0$, $G(re_k)(e_k) = re_ke_k = re_k = 0$, and $\ker G$ is zero. Also, for some $f \in \mathrm{Hom}_{e_kRe_k}(Re_k, Re_k)$,

$$
\begin{aligned}
f(ce_k) = f(1 \cdot ce_k) &= f(\sum_{i=1}^{n_k} a_ie_kb_ie_kce_k) \\
&= \sum_{i=1}^{n_k} f(a_ie_kb_ie_kce_k) \\
&= \sum_{i=1}^{n_k} f(a_ie_k)e_kb_ie_kce_k \\
&= \left(\sum_{i=1}^{n_k} f(a_ie_k)e_kb_ie_k\right) ce_k
\end{aligned}
$$

for arbitrary $c \in R$. Thus, if we take $r = \sum_{i=1}^{n_k} f(a_ie_k)e_kb_ie_k$, $G(re_k) = f$. Therefore, G is an isomorphism. This shows that $Re_k \simeq \mathrm{Hom}_{e_kRe_k}(Re_k, Re_k)$.

Therefore, for each k, $Re_k \simeq \mathrm{Hom}_{e_kRe_k}(Re_k, Re_k) \simeq M_{n_k}(e_kRe_k)$.

Then, just take r be a number of direct sumamnds in $(4-1)$, $n_k = \dim_{e_kRe_k}(Re_k)$, $D_k = e_kRe_k$. And since we show that $L_k = Re_k \simeq M_{n_k}(e_kRe_k)$ and the finitely many direct sum is just a cartesian product, we obtain

$$
\begin{aligned}
R &= L_1 \oplus \cdots \oplus L_n \\
&= M_1(D_1) \times \cdots \times M_r(D_r)
\end{aligned}
$$

□

Existency of(5) ⇒ Existency of (4-1)

Let $R \simeq R_1 \times \cdots \times R_r$ where $R_j = M_{n_j}(D_j)$ for some division rings D_j. Since it's a finite product, $R_1 \times \cdots \times R_r = R_1 \oplus \cdots \oplus R_r$.

Each $M_{n_k}(D_k)$ is simple. It's because, if an ideal of $M_{n_k}(D_k)$ contains a non-zero matrix, it must be $M_{n_k}(D_k)$. Let's show it. First, let $e_{i,j}$ be a matrix of $M_{n_k}(D_k)$ such that only i-th row j-th column entry is 1 and all other entries are zero. Let's pick any non-zero matrix $m \in M_{n_k}(D_k)$. Then m must contains a non-zero entry at i-th row, j-th column entry for some $i, j \in \{1, \cdots, n\}$. Let the entry be u. Since $M_{n_k}(D_k)$ is a division ring, there is $u^{-1} \in M_{n_k}(D_k)$. Then, $(u^{-1}e_{x,i})m = e_{x,j}$ and $m(u^{-1}e_{j,x}) = e_{i,x}$. Then, if an ideal of $M_{n_k}(D_k)$ contains m, it contains $e_{i,x}, e_{x,j}$ for every x.

Also, if we take $e_{y,i}$ for some y, we obtain $e_{y,x} = e_{y,i}e_{i,x}$. Thus, the ideal contains all $e_{y,x}$ for every $y, x \in \{1, \cdots, n\}$. Then, for $(a_{i,j})_{i,j\in\{1,\cdots,n_k\}} \in M_{n_k}(D_k)$,

$$(a_{i,j})_{i,j\in\{1,\cdots,n_k\}} = \sum_{i=1}^{n_k}\sum_{j=1}^{n_k} a_{i,j}e_{i,j}$$

Thus, the ideal is $M_{n_k}(D_k)$. Therefore, $M_{n_k}(D_k)$ has only two ideal: zero or itself. it shows $M_{n_k}(D_k)$ is simple.

Let $R' = R'_1 \oplus \cdots \oplus R'_r$ where $R'_k = 0 \times \cdots \times 0 \times R_k \times 0 \times \cdots \times 0$. Then, $R'_k \simeq R_k$ and $R \simeq R'$.

Then, the left product of R to R'_k is same as R_k to R'_k, because every entry of R'_k are zero except k-th one,

$$\begin{aligned}(a_1, \cdots, a_r) \cdot (0, \cdots, 0, b_k, 0, \cdots, 0) &= (a_1 \cdot 0, \cdots, a_{k-1} \cdot 0, a_k \cdot b_k, a_{k+1} \cdot 0, \cdots, a_r \cdot 0) \\ &= (0, \cdots, 0, a_k \cdot b_k, 0, \cdots, 0)\end{aligned}$$

Thus if there is an ideal I contained in R'_k, since R'_k is simple, I is isomorphic to 0 or R'_k which are only possible ideals of R_k. Therefore, each R_k is simple.

Let $e_k \in R'$ such that all entries are zero except k-th entry which is 1. First, multiplication by e_k is a projection to R'_k. Thus, $R'_k = R' \cdot e_k$. $e_j \cdot e_k = \delta_{jk}e_j$. It's because, if $j = k$, zero entries are multiplicated with zero-valued entries and the one-valued entry, at j-th, is multiplicated wiht one-valued entries, and if $j \neq k$, then each one-valued entries are vanished since they are multiplicated with some zero-valued entries. Also, note that the multiplicative identity of finite direct sum of rings with unity is $(1, 1, \cdots, 1)$. Thus, $(1, 1, \cdots, 1) = \sum_{k=1}^{r} e_k = 1_R$.

Therefore, $R = \bigoplus_{k=1}^{r} Re_k$ where $e_je_k = \delta_{j,k}e_j$, $\sum_{j=1}^{r} e_j = 1_R$.

□

Uniqueness of (4-1)

First, instead of the result of (5), let's show some uniqueness of the result of (4).

Suppose that there are two distinct set of simple $L_i = Re_i$ for each $i = 1, \cdots, n$ and simple $L'_i = Re'_i$ for each $i = 1, \cdots, n'$ which satisfies all properties given in (4). (i.e. $R = \bigoplus_{i=1}^{n} L_i = \bigoplus_{i=1}^{n'} L'_i$, $e_ie_j = \delta_{ij}e_i$, $e'_ie'_j = \delta_{ij}e'_i$, $\sum e_i = \sum e'_i = 1$.)

Just take a product with e_k for some k. Then we obtain

$$\begin{aligned}Re_k &= \bigoplus_{i=1}^{n} Re_ie_k \\ &= \bigoplus_{i=1}^{n'} Re'_ie_k\end{aligned}$$

Note that $R(e'_ie_k)$ is a left principal ideal and since Re'_i is simple and $Re'_ie_k \subseteq Re'_i$, Re'_ie_k is 0 or Re'_i for each i. However, if two of Re'_ie_k is non-zero for the fixed k, then, Re_k, which is simple too, can be expressed as the direct sum of more than one non-zero modules. Thus it's a contradiction. Therefore, for each k, at most one of Re'_ie_k can be non-zero, i.e. $Re'_ie_k = Re_k$. $\cdots$(a)

Also, suppose that if every Re'_ie_k is zero for each i. then, we obtain $Re_k = 0$. But since Re_k is not zero (because at least it contains an idempotent element e_k), it's a contradiction. Thus, for each k, at least one of Re'_ie_k must be non-zero, i.e. $Re'_ie_k = Re_k$. $\cdots$(b)

Therefore to satisfy (a) and (b), n must be equal to n'. (If $n > n'$, to satisfy (b), for each k, there exists i such that $Re'_ie_k = Re_k$. However, since $n > n'$, by Pigeonhole Principle, there are two k, k' such that $Re'_i e_k = Re_k$ and $Re'_i e'_k = Re'_k$ for some i. This violates (a). If $n < n'$, switch (L_*, n, e_*) and (L'_*, n', e'_*) to obtain the case of $n > n'$, since the equivalence is symmetric, then, as we showed above, it violates (a). Thus, the previous (L_*, n, e_*) and (L'_*, n', e'_*) $n < n'$ is impossible.) Also, there must be a ono-to-one correspondence between $k \in \{1, \cdots, n\}$ and $i \in \{1, \cdots, n'\}$ such that $Re'_i e_k = Re_k$.

Let $k \in \{1, \cdots, n\}$ and $i \in \{1, \cdots, n'\}$ such that $Re'_i e_k = Re_k$. Then, since $e_k \in Re_k$, $e_k \in Re'_i e_k \subseteq Re'_i$ too. But as we showed in the proof of (3)⇒(4), minimal ideal I can be expressed as Rx for any non-zero element x of I. Since e_k is non-zero, $Re'_i = Re_k$.

Therefore, this shows that $n = n'$ and there is some permutation $\pi \in S_n$ such that $L_i = L'_{\pi(i)}$ for $i = 1, \cdots, n$. □

Uniqueness of (5)

Let's use the uniqueness of (4-1) and construction between (4-1) and (5) we shown above.

Suppose that there are two set of (r, n_*, R_*, D_*) and (r', n'_*, R'_*, D'_*) such that $R_k = M_{n_k}(D_k)$, $R'_k = M_{n'_k}(D'_k)$ and
$$R \simeq R_1 \times \cdots \times R_r \simeq R'_1 \times \cdots \times R_{r'}$$

First, in the construction from (5) to (4-1), n in (4-1) is equal to r. (i.e. the number of term in the product of (5) is equal to the number or direct summands of (4-1).) Thus, there is $e_1, \cdots, e_r$ and $e'_1, \cdots, e'_{r'}$ in R such that

$$R = Re_1 \oplus \cdots \oplus Re_r = Re'_1 \oplus \cdots \oplus Re'_{r'}$$

and each e_* and e'_* satisfies all conditions in (4-1). Then, by the uniqueness of (4-1), $r = r'$ and there is some permutation $\pi \in S_r$ such that $Re_k = Re'_{\pi(k)}$ for every $k = 1, \cdots, r$.

First, since $n = r$, $n' = r'$ by the construction (5) to (4-1), and $r = r'$ by the uniqueness of (4-1), $n = n' = r = r'$ must holds.

Next, in the construction (5) to (4-1), each $M_{n_k}(D_k)$ is correspond to Re_k. In the same way, each $M_{n'_k}(D'_k)$ is correspond to Re'_k. Since $Re_k = Re'_{\pi(k)}$, by reordering n'_*, D'_*, e'_* using π, we obtain $Re_k = Re'_k$ for each k. Note that Re_k is constructed so that $M_{n_k}(D_k)$ is isomorphic to Re_k. Thus,

$$M_{n_k}(D_k) \simeq Re_k = Re'_k \simeq M_{n'_k}(D'_k)$$

Therefore, at this point, we know that $n = n'$ and each $M_{n_k}(D_k)$ is unique up to up to isomorphism after reordering.

The last thing what we need to show is,n $n_k = n'_{\pi(k)}$ and $D_k \simeq D'_{\pi(k)}$ holds for each k where $\pi \in S_n$ is a permutation such that $M_{n_k}(D_k) \simeq M_{n'_{\pi(k)}}(D'_{\pi(k)})$.

Suppose that D, D' be division rings, $n, n' \in \mathbb{N}$ and $R = M_n(D), R' = M_{n'}(D')$, such that $R \simeq R'$.

Then, by the theorem in the lecture, R

Let $e_{i,j}$ be an matrix of R such that every entry are zero except the i-th row j-th column entry which is valued by 1. In the same way, let $f_{i,j}$ be an matrix of R' such that all entries are valued by zero except (i, j)-entry which is valued by 1.

Let $\varphi : R \to R'$ be an isomorphism between R and R'.

Also, since

$$\begin{aligned} Z(D) \simeq \{\alpha I \mid \alpha \in Z(D)\} &\simeq Z(R) \\ &\simeq Z(R') \simeq Z(D') \end{aligned}$$

then, for $k = Z(D)$, φ is a k-module isomorphism. (Note that since $cM = (cI)M$ for $c \in k$ and matrix M, scalar multiplication can be considered as a matrix multiplication, and φ is a ring homomorphism for matrices. Thus, each R and R' can be considered as a k-module.)

Suppose that $n' > n$. Note that $\mathcal{B} = \{e_{i,j}\}$ is a basis of $R = M_n(D)$ as a k-module. Then, isomorphic image of $\mathcal{B}$ by φ should be a basis of R'. However, since $|\mathcal{B}| = n^2 < n'^2$. Thus, it cannot be a basis of R'. In the same way, $n' < n$ cannot hold. Thus $n = n'$.

Then, $M_n(D) \simeq M_{n'}(D') = M_n(D')$. Therefore $D \simeq D'$.

This shows that $n_k = n'_k$ and $D_k = D'_k$ for each k. $\square$