HOMEWORK

Contents

1. Homework 1 (Due: Apr 5)

Problem 1.1. Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by

$$\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}.$$

(1) Prove that this is a group action.
(2) Describe explicitly how the elements (1 2) and (1 2 3) act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

Solution.

(1) Since $\sigma \in S_A$ is bijective, $\sigma \cdot \{a_1, a_2, \cdots, a_k\} = \{\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_k)\}$ is a subset of A with cardinality k so in B.

Since S_A is a group, $\sigma, \tau \in S_A$ implies that $\sigma\tau \in S_A$ and,

$$\sigma(\tau \cdot \{a_1, a_2, \cdots, a_k\}) = \sigma \cdot \{\tau(a_1), \tau(a_2), \cdots, \tau(a_k)\} = \{\sigma\tau(a_1), \sigma\tau(a_2), \cdots, \sigma\tau(a_k)\} = (\sigma\tau) \cdot \{a_1, a_2, \cdots, a_k\}$$

for all $\sigma, \tau \in S_A$ and all $\{a_1, a_2, \cdots, a_k\} \in B$.

Also, $1 = id \in S_A$ with $id \cdot \{a_1, a_2, \cdots, a_k\} = \{a_1, a_2, \cdots, a_k\}$ for all $\{a_1, a_2, \cdots, a_k\} \in B$.

Hence the acting of S_A on B is a group action. ∎

(2)

acting (1,2)	acting (1 2 3)
$\{1,2\} \mapsto \{1,2\}$	$\{1,2\} \mapsto \{2,3\}$
$\{1,3\} \mapsto \{2,3\}$	$\{1,3\} \mapsto \{1,2\}$
$\{1,4\} \mapsto \{2,4\}$	$\{1,4\} \mapsto \{2,4\}$
$\{2,3\} \mapsto \{1,3\}$	$\{2,3\} \mapsto \{1,3\}$
$\{2,4\} \mapsto \{1,4\}$	$\{2,4\} \mapsto \{3,4\}$
$\{3,4\} \mapsto \{3,4\}$	$\{3,4\} \mapsto \{1,4\}$

□

Problem 1.2. Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by $a \sim b$ if and only if $a = hb$ for some $h \in H$ is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the orbit of x under the action of H. The orbits under the action of H partition the set A.)

Solution.

W.T.S $a \sim b$ defined by $a = hb$ for some $h \in H$ is an equiv. relation.

(reflexive) $a \sim a$ by 1_h $\because$ $1_h a = a$

(symmetric) $a \sim b$ if and only if $b \sim a$ by inverse element: $a = h \cdot b \Leftrightarrow b = h^{-1} \cdot a$

(transitive) If $a \sim b$ and $b \sim c$, then $a \sim c$ by group axiom on H: $a = hb$, $b = h'c \to a = h \cdot (h'c) = (hh') \cdot c$, $hh' \in H$.

Hence $\sim$ is the equivalence relation. ∎

□

Problem 1.3. In each of parts (1) to (5) give the number of nonisomorphic abelian groups of the specified order - do not list the groups:

(1) order 100
(2) order 576
(3) order 1155
(4) order 42875
(5) order 2704

Solution.

1.3 $P(n)$ is a partition number of n.

(1) $100 = 2^2 \cdot 5^2$, $P(2) \cdot P(2) = 2 \cdot 2 = 4$.
4.

(2) $576 = 2^6 \cdot 3^2$, $P(6) \cdot P(2) = 11 \cdot 2 = 22$
22.

(3) $1155 = 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1$, $P(1)^4 = 1$.
1.

(4) $42875 = 5^3 \cdot 7^3$, $P(3)^2 = 3^2 = 9$.
9.

(5) $2704 = 2^4 \cdot 13^2$, $P(4) \cdot P(2) = 5 \cdot 2 = 10$
10.

□

Problem 1.4. In each of parts (1) to (5) give the lists of invariant factors for all abelian groups of the specified order:

(1) order 270
(2) order 9801
(3) order 320
(4) order 105
(5) order 44100

Solution.

(1) $270 = 2 \times 3^3 \times 5 \longrightarrow P(1) \times P(3) \times P(1) = 1 \times 3 \times 1 = 3$

(2) $9801 = 99^2 = 3^4 \times 11^2 \longrightarrow P(4) \times P(2) = 5 \times 2 = 10$

(3) $320 = 2^6 \times 5 \longrightarrow P(6) \times P(1) = 11 \times 1 = 11$

(4) $105 = 3 \times 5 \times 7 \longrightarrow P(1) \times P(1) \times P(1) = 1 \times 1 \times 1 = 1$

(5) $44100 = 210^2 = 2^2 \times 3^2 \times 5^2 \times 7^2 \longrightarrow P(2) \times P(2) \times P(2) \times P(2) = 2 \times 2 \times 2 \times 2 = 16$

Order	invariant factors	
(1) 270	$2 \cdot 3^3 \cdot 5$	$: \mathbb{Z}_{270}$
	$2 \cdot 3^2 \cdot 5,\ 3$	$: \mathbb{Z}_{90} \times \mathbb{Z}_3$
	$2 \cdot 3 \cdot 5,\ 3,\ 3$	$: \mathbb{Z}_{30} \times \mathbb{Z}_3 \times \mathbb{Z}_3$
(2) 9801	$3^4 \cdot 11^2$	$: \mathbb{Z}_{9801}$
	$3^3 \cdot 11^2,\ 3$	$: \mathbb{Z}_{3269} \times \mathbb{Z}_3$
	$3^2 \cdot 11^2,\ 3^2$	$: \mathbb{Z}_{1089} \times \mathbb{Z}_9$
	$3^2 \cdot 11^2,\ 3,\ 3$	$: \mathbb{Z}_{1089} \times \mathbb{Z}_3 \times \mathbb{Z}_3$
	$3 \cdot 11^2,\ 3,\ 3,\ 3$	$: \mathbb{Z}_{363} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
	$3^4 \cdot 11,\ 11$	$: \mathbb{Z}_{891} \times \mathbb{Z}_{11}$
	$3^3 \cdot 11,\ 3 \cdot 11$	$: \mathbb{Z}_{297} \times \mathbb{Z}_{33}$
	$3^2 \cdot 11,\ 3^2 \cdot 11$	$: \mathbb{Z}_{99} \times \mathbb{Z}_{99}$
	$3^2 \cdot 11,\ 3 \cdot 11,\ 3$	$: \mathbb{Z}_{99} \times \mathbb{Z}_{33} \times \mathbb{Z}_3$
	$3 \cdot 11,\ 3 \cdot 11,\ 3,\ 3$	$: \mathbb{Z}_{33} \times \mathbb{Z}_{33} \times \mathbb{Z}_3 \times \mathbb{Z}_3$
(3) 320	$2^6 \cdot 5$	$: \mathbb{Z}_{320}$
	$2^5 \cdot 5,\ 2$	$: \mathbb{Z}_{160} \times \mathbb{Z}_2$
	$2^4 \cdot 5,\ 2^2$	$: \mathbb{Z}_{80} \times \mathbb{Z}_4$
	$2^3 \cdot 5,\ 2^3$	$: \mathbb{Z}_{40} \times \mathbb{Z}_8$
	$2^4 \cdot 5,\ 2,\ 2$	$: \mathbb{Z}_{80} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
	$2^3 \cdot 5,\ 2^2,\ 2$	$: \mathbb{Z}_{40} \times \mathbb{Z}_4 \times \mathbb{Z}_2$
	$2^2 \cdot 5,\ 2^2,\ 2^2$	$: \mathbb{Z}_{20} \times \mathbb{Z}_4 \times \mathbb{Z}_4$
	$2^3 \cdot 5,\ 2,\ 2,\ 2$	$: \mathbb{Z}_{40} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
	$2^2 \cdot 5,\ 2^2,\ 2,\ 2$	$: \mathbb{Z}_{20} \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
	$2^2 \cdot 5,\ 2,\ 2,\ 2,\ 2$	$: \mathbb{Z}_{20} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
	$2 \cdot 5,\ 2,\ 2,\ 2,\ 2,\ 2$	$: \mathbb{Z}_{10} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Order	invariant factors	
(4) 105	$3 \cdot 5 \cdot 7$	$: \mathbb{Z}_{105}$
(5) 44100	$2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2$	$: \mathbb{Z}_{44100}$
	$2 \cdot 3^2 \cdot 5^2 \cdot 7^2,\ 2$	$: \mathbb{Z}_{22050} \times \mathbb{Z}_2$
	$2^2 \cdot 3 \cdot 5^2 \cdot 7^2,\ 3$	$: \mathbb{Z}_{14700} \times \mathbb{Z}_3$
	$2^2 \cdot 3^2 \cdot 5 \cdot 7^2,\ 5$	$: \mathbb{Z}_{8820} \times \mathbb{Z}_5$
	$2^2 \cdot 3^2 \cdot 5^2 \cdot 7,\ 7$	$: \mathbb{Z}_{6300} \times \mathbb{Z}_7$
	$2 \cdot 3 \cdot 5^2 \cdot 7^2,\ 2 \cdot 3$	$: \mathbb{Z}_{7350} \times \mathbb{Z}_6$
	$2 \cdot 3^2 \cdot 5 \cdot 7^2,\ 2 \cdot 5$	$: \mathbb{Z}_{4410} \times \mathbb{Z}_{10}$
	$2 \cdot 3^2 \cdot 5^2 \cdot 7,\ 2 \cdot 7$	$: \mathbb{Z}_{3150} \times \mathbb{Z}_{14}$
	$2^2 \cdot 3 \cdot 5 \cdot 7^2,\ 3 \cdot 5$	$: \mathbb{Z}_{2940} \times \mathbb{Z}_{15}$
	$2^2 \cdot 3 \cdot 5^2 \cdot 7,\ 3 \cdot 7$	$: \mathbb{Z}_{2100} \times \mathbb{Z}_{21}$
	$2^2 \cdot 3^2 \cdot 5 \cdot 7,\ 5 \cdot 7$	$: \mathbb{Z}_{1260} \times \mathbb{Z}_{35}$
	$2 \cdot 3 \cdot 5 \cdot 7^2,\ 2 \cdot 3 \cdot 5$	$: \mathbb{Z}_{1470} \times \mathbb{Z}_{30}$
	$2 \cdot 3 \cdot 5^2 \cdot 7,\ 2 \cdot 3 \cdot 7$	$: \mathbb{Z}_{1050} \times \mathbb{Z}_{42}$
	$2 \cdot 3^2 \cdot 5 \cdot 7,\ 2 \cdot 5 \cdot 7$	$: \mathbb{Z}_{630} \times \mathbb{Z}_{70}$
	$2^2 \cdot 3 \cdot 5 \cdot 7,\ 3 \cdot 5 \cdot 7$	$: \mathbb{Z}_{420} \times \mathbb{Z}_{105}$
	$2 \cdot 3 \cdot 5 \cdot 7,\ 2 \cdot 3 \cdot 5 \cdot 7$	$: \mathbb{Z}_{210} \times \mathbb{Z}_{210}$

$\square$

Problem 1.5. In each of parts (1) to (5) give the lists of elementary divisors for all abelian groups of the specified order and then match each list with the corresponding list of invariant factors found in the preceding problem:

(1) order 270
(2) order 9801
(3) order 320
(4) order 105
(5) order 44100

Solution.

(1) $270 = 2\times 3^3\times 5$
(2) $9801 = 3^4\times 11^2$
(3) $320 = 2^6\times 5$
(4) $105 = 3\times 5\times 7$
(5) $44100 = 2^2\times 3^2\times 5^2\times 7^2$

Order	elementary divisors			invariant factors
(1) 270	$2, 3^3, 5$	$: \mathbb{Z}_{27}\times\mathbb{Z}_5\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{270}$	$: 2\cdot 3^3\cdot 5$
	$2, 3^2, 5, 3$	$: \mathbb{Z}_9\times\mathbb{Z}_5\times\mathbb{Z}_3\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{90}\times\mathbb{Z}_3$	$: 2\cdot 3^2\cdot 5,\ 3$
	$2, 3, 5, 3, 3$	$: \mathbb{Z}_5\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{30}\times\mathbb{Z}_3\times\mathbb{Z}_3$	$: 2\cdot 3\cdot 5,\ 3,\ 3$
(2) 9801	$3^4, 11^2$	$: \mathbb{Z}_{121}\times\mathbb{Z}_{81}$	$\cong \mathbb{Z}_{9801}$	$: 3^4\cdot 11^2$
	$3^3, 3, 11^2$	$: \mathbb{Z}_{121}\times\mathbb{Z}_{27}\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{3267}\times\mathbb{Z}_3$	$: 3^3\cdot 11^2,\ 3$
	$3^2, 3^2, 11^2$	$: \mathbb{Z}_{121}\times\mathbb{Z}_9\times\mathbb{Z}_9$	$\cong \mathbb{Z}_{1089}\times\mathbb{Z}_9$	$: 3^2\cdot 11^2,\ 3^2$
	$3^2, 3, 3, 11^2$	$: \mathbb{Z}_{121}\times\mathbb{Z}_9\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{1089}\times\mathbb{Z}_3\times\mathbb{Z}_3$	$: 3^2\cdot 11^2,\ 3,\ 3$
	$3, 3, 3, 3, 11^2$	$: \mathbb{Z}_{121}\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{363}\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3$	$: 3\cdot 11^2,\ 3,\ 3,\ 3$
	$3^4, 11, 11$	$: \mathbb{Z}_{81}\times\mathbb{Z}_{11}\times\mathbb{Z}_{11}$	$\cong \mathbb{Z}_{891}\times\mathbb{Z}_{11}$	$: 3^4\cdot 11,\ 11$
	$3^3, 3, 11, 11$	$: \mathbb{Z}_{27}\times\mathbb{Z}_{11}\times\mathbb{Z}_{11}\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{297}\times\mathbb{Z}_{33}$	$: 3^3\cdot 11,\ 3\cdot 11$
	$3^2, 3^2, 11, 11$	$: \mathbb{Z}_{11}\times\mathbb{Z}_{11}\times\mathbb{Z}_9\times\mathbb{Z}_9$	$\cong \mathbb{Z}_{99}\times\mathbb{Z}_{99}$	$: 3^2\cdot 11,\ 3^2\cdot 11$
	$3^2, 3, 3, 11, 11$	$: \mathbb{Z}_{11}\times\mathbb{Z}_{11}\times\mathbb{Z}_9\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{99}\times\mathbb{Z}_{33}\times\mathbb{Z}_3$	$: 3^2\cdot 11,\ 3\cdot 11,\ 3$
	$3, 3, 3, 3, 11, 11$	$: \mathbb{Z}_{11}\times\mathbb{Z}_{11}\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{33}\times\mathbb{Z}_{33}\times\mathbb{Z}_3\times\mathbb{Z}_3$	$: 3\cdot 11,\ 3\cdot 11,\ 3,\ 3$
(3) 320	$2^6, 5$	$: \mathbb{Z}_{64}\times\mathbb{Z}_5$	$\cong \mathbb{Z}_{320}$	$: 2^6\cdot 5$
	$2^5, 2, 5$	$: \mathbb{Z}_{32}\times\mathbb{Z}_5\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{160}\times\mathbb{Z}_2$	$: 2^5\cdot 5,\ 2$
	$2^4, 2^2, 5$	$: \mathbb{Z}_{16}\times\mathbb{Z}_5\times\mathbb{Z}_4$	$\cong \mathbb{Z}_{80}\times\mathbb{Z}_4$	$: 2^4\cdot 5,\ 2^2$
	$2^3, 2^3, 5$	$: \mathbb{Z}_8\times\mathbb{Z}_8\times\mathbb{Z}_5$	$\cong \mathbb{Z}_{40}\times\mathbb{Z}_8$	$: 2^3\cdot 5,\ 2^3$
	$2^4, 2, 2, 5$	$: \mathbb{Z}_{16}\times\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{80}\times\mathbb{Z}_2\times\mathbb{Z}_2$	$: 2^4\cdot 5,\ 2,\ 2$
	$2^3, 2^2, 2, 5$	$: \mathbb{Z}_8\times\mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{40}\times\mathbb{Z}_4\times\mathbb{Z}_2$	$: 2^3\cdot 5,\ 2^2,\ 2$
	$2^2, 2^2, 2^2, 5$	$: \mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_4$	$\cong \mathbb{Z}_{20}\times\mathbb{Z}_4\times\mathbb{Z}_4$	$: 2^2\cdot 5,\ 2^2,\ 2^2$
	$2^3, 2, 2, 2, 5$	$: \mathbb{Z}_8\times\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{40}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$: 2^3\cdot 5,\ 2,\ 2,\ 2$
	$2^2, 2^2, 2, 2, 5$	$: \mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{20}\times\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2$	$: 2^2\cdot 5,\ 2^2,\ 2,\ 2$
	$2^2, 2, 2, 2, 2, 5$	$: \mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{20}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$: 2^2\cdot 5,\ 2,\ 2,\ 2,\ 2$
	$2, 2, 2, 2, 2, 2, 5$	$: \mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{10}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	$: 2\cdot 5,\ 2,\ 2,\ 2,\ 2,\ 2$
(4) 105	$3, 5, 7$	$: \mathbb{Z}_7\times\mathbb{Z}_5\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{105}$	$: 3\cdot 5\cdot 7$
(5) 44100	$2^2, 3^2, 5^2, 7^2$	$: \mathbb{Z}_{49}\times\mathbb{Z}_{25}\times\mathbb{Z}_9\times\mathbb{Z}_4$	$\cong \mathbb{Z}_{44100}$	$: 2^2\cdot 3^2\cdot 5^2\cdot 7^2$
	$2, 3^2, 5^2, 7^2, 2$	$: \mathbb{Z}_{49}\times\mathbb{Z}_{25}\times\mathbb{Z}_9\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{22050}\times\mathbb{Z}_2$	$: 2\cdot 3^2\cdot 5^2\cdot 7^2,\ 2$
	$2^2, 3, 5^2, 7^2, 3$	$: \mathbb{Z}_{49}\times\mathbb{Z}_{25}\times\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{14700}\times\mathbb{Z}_3$	$: 2^2\cdot 3\cdot 5^2\cdot 7^2,\ 3$
	$2^2, 3^2, 5, 7^2, 5$	$: \mathbb{Z}_{49}\times\mathbb{Z}_9\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_4$	$\cong \mathbb{Z}_{8820}\times\mathbb{Z}_5$	$: 2^2\cdot 3^2\cdot 5\cdot 7^2,\ 5$
	$2^2, 3^2, 5^2, 7, 7$	$: \mathbb{Z}_{25}\times\mathbb{Z}_9\times\mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_4$	$\cong \mathbb{Z}_{6300}\times\mathbb{Z}_7$	$: 2^2\cdot 3^2\cdot 5^2\cdot 7,\ 7$
	$2, 3, 5^2, 7^2, 2, 3$	$: \mathbb{Z}_{49}\times\mathbb{Z}_{25}\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{4350}\times\mathbb{Z}_6$	$: 2\cdot 3\cdot 5^2\cdot 7^2,\ 2\cdot 3$
	$2, 3^2, 5, 7^2, 2, 5$	$: \mathbb{Z}_{49}\times\mathbb{Z}_9\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{4410}\times\mathbb{Z}_{10}$	$: 2\cdot 3^2\cdot 5\cdot 7^2,\ 2\cdot 5$
	$2, 3^2, 5^2, 7, 2, 7$	$: \mathbb{Z}_{25}\times\mathbb{Z}_9\times\mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{3150}\times\mathbb{Z}_{14}$	$: 2\cdot 3^2\cdot 5^2\cdot 7,\ 2\cdot 7$
	$2^2, 3, 5, 7^2, 3, 5$	$: \mathbb{Z}_{49}\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{2940}\times\mathbb{Z}_{15}$	$: 2^2\cdot 3\cdot 5\cdot 7^2,\ 3\cdot 5$
	$2^2, 3, 5^2, 7, 3, 7$	$: \mathbb{Z}_{25}\times\mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{2100}\times\mathbb{Z}_{21}$	$: 2^2\cdot 3\cdot 5^2\cdot 7,\ 3\cdot 7$
	$2^2, 3^2, 5, 7, 5, 7$	$: \mathbb{Z}_9\times\mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_4$	$\cong \mathbb{Z}_{1260}\times\mathbb{Z}_{35}$	$: 2^2\cdot 3^2\cdot 5\cdot 7,\ 5\cdot 7$
	$2, 3, 5, 7^2, 2, 3, 5$	$: \mathbb{Z}_{49}\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{1470}\times\mathbb{Z}_{30}$	$: 2\cdot 3\cdot 5\cdot 7^2,\ 2\cdot 3\cdot 5$
	$2, 3, 5^2, 7, 2, 3, 7$	$: \mathbb{Z}_{25}\times\mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{1050}\times\mathbb{Z}_{42}$	$: 2\cdot 3\cdot 5^2\cdot 7,\ 2\cdot 3\cdot 7$
	$2, 3^2, 5, 7, 2, 5, 7$	$: \mathbb{Z}_9\times\mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{630}\times\mathbb{Z}_{70}$	$: 2\cdot 3^2\cdot 5\cdot 7,\ 2\cdot 5\cdot 7$
	$2^2, 3, 5, 7, 3, 5, 7$	$: \mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_3$	$\cong \mathbb{Z}_{420}\times\mathbb{Z}_{105}$	$: 2^2\cdot 3\cdot 5\cdot 7,\ 3\cdot 5\cdot 7$
	$2, 3, 5, 7, 2, 3, 5, 7$	$: \mathbb{Z}_7\times\mathbb{Z}_7\times\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_2$	$\cong \mathbb{Z}_{210}\times\mathbb{Z}_{210}$	$: 2\cdot 3\cdot 5\cdot 7,\ 2\cdot 3\cdot 5\cdot 7$

□

Problem 1.6. Let R be a ring with identity and let S be a subring of R containing the identity. Prove that if u is a unit in S then u is a unit in R. Show by example that the converse is false.

Solution.

If u is a unit in S, then by the definition,
$\exists\, v \in S$, s.t $uv = vu = 1$. Since $u, v \in S$ and S is a subset of R, we have $u, v \in R$. Thus for $u \in R$, $\exists\, v \in R$, s.t $uv = vu = 1$, which means u is a unit in R.

Converse: If u is a unit in R then u is a unit in S.

Consider the ring $R = \mathbb{Q}$ with identity 1. $S = \mathbb{Z}$ is a subring of $\mathbb{Q}$ containing the identity 1.

Notice 2 is a unit in R, but it is not a unit in S since $\mathbb{Z}^\times = \{\pm 1\}$. $\Rightarrow$ The converse is false.

□

Problem 1.7. Let R be a ring with $1 \neq 0$.

(1) Prove that if a is a zero divisor, then it is not a unit.
(2) Prove that if $ab = ac$ and $a \neq 0$ is not a zero divisor, then $b = c$.

Solution.

(1) Since a is a zero divisor, $\exists\, b \in R \setminus \{0\}$ s.t. $ab = 0$ or $ba = 0$, WOLG $ab = 0$.
Sps that a is a unit i.e. $\exists\, a^{-1} \in R$ s.t $aa^{-1} = a^{-1}a = 1$
$ab = 0 \Rightarrow \underset{(a^{-1}a)b}{\underset{\parallel}{a^{-1}(ab)}} = a^{-1}0 = 0$ so that $b = 0$. However, $b \neq 0$.
Therefore a is not a unit.

(2) $ab = ac \Rightarrow ab - ac = 0$ by distributive law.
$a(b-c) = 0$ Since a is not a zero divisor.
$b - c = 0 \Rightarrow b = c$.

□

Problem 1.8. Assume R is commutative with $1 \neq 0$. Prove that if P is a prime ideal of R and P contains no zero divisors then R is an integral domain.

Solution.

Sps that R is not an integral domain. i.e. $\exists\, a, b \in R$ s.t $ab = 0$ ... (*)
$\neq 0$

Since P is an abelian group in addition, $0 \in P$. and $ab = 0 \in P$.
from the fact that P is an ideal.
Also, since P is a prime ideal, $a \in P$ or $b \in P$. WOLG let $a \in P$.
However, a is a zero divisor that not in P. $\rightarrow\!\leftarrow$.
Therefore R is an integral domain.

□

Problem 1.9. Let R be a ring with $1 \neq 0$. Let $A = (a_1, a_2, \ldots, a_n)$ be a nonzero finitely generated ideal of R. Prove that there is an ideal B which is maximal with respect to the property that it does not contain A. [Use Zorn's Lemma.]

Solution.

Let J be ideals s.t. $A \not\subseteq J$.
Let S be a collection of all J's.
Note that $(S, \subseteq)$: poset.
Also, since $\{0\}$ is ideal of R, $\{0\} \in S$. $\therefore S$ is nonempty.
Let B_i's are subset of S and $B = \bigcup_{i \in I} B_i$.
s.t. $B_1 \subseteq B_2 \subseteq \cdots \subseteq B$
To show ①: B is ideal.
Suppose that B is not ideal.
then $\exists\, \alpha \in R$ s.t. $\alpha B \not\subseteq B$ or $B\alpha \not\subseteq B$.
WLOG, $\alpha B \not\subseteq B$. then $\exists\, b \in B$ s.t. $ab \notin B$.
Since $b \in B$, then $\exists i$ s.t. $b \in B_i$.
Since B_i is ideal, $ab \in B_i . \subseteq B$. $\lightning$ contradiction.
$\therefore B$ is ideal. $\Rightarrow B \in S$.
Hence, B is upperbound in S.

To show ②: $A \not\subseteq B$
Suppose that $A \subseteq B$.
Let $a_j \in B_{i_j}$. for $j = 1, 2, \cdots, n$.
let $M := \max\{i_1, i_2, \cdots, i_n\}$.
Then $a_1, \cdots, a_n \in B_M \in S$. $\rightarrow\leftarrow$ contradiction.
$\therefore A \not\subseteq B$.

Therefore by Zorn's Lemma,
There is an maximal ideal that does not contain A.

$\square$

Problem 1.10. Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs: $(n_i, n_j) = 1$ for all $i \neq j$.

(1) Show that the Chinese Remainder Theorem implies that for any $a_1, \ldots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences

$$x \equiv a_1 \bmod n_1, \quad x \equiv a_2 \bmod n_2, \quad \ldots, \quad x \equiv a_k \bmod n_k$$

and that the solution x is unique mod$n = n_1 n_2 \dots n_k$.

(2) Let $n_i' = n/n_i$ be the quotient of n by n_i, which is relatively prime to n_i by assumption. Let t_i be the inverse of n_i' mod n_i. Prove that the solution x in (a) is given by

$$x = a_1 t_1 n_1' + a_2 t_2 n_2' + \cdots + a_k t_k n_k' \bmod n.$$

Note that the elements t_i can be quickly found by the Euclidean Algorithm as described in Section 2 of the Preliminaries chapter (writing $an_i + bn_i' = (n_i, n_i') = 1$ gives $t_i = b$) and that these then quickly give the solutions to the system of congruences above for any choice of $a_1, a_2, \dots, a_k$.

(3) Solve the simultaneous system of congruences

$$x \equiv 1 \bmod 8, \quad x \equiv 2 \bmod 25, \quad \text{and } x \equiv 3 \bmod 81$$

and the simultaneous system

$$y \equiv 5 \bmod 8, \quad y \equiv 12 \bmod 25, \quad \text{and} \quad y \equiv 47 \bmod 81$$

Solution.

(a) Let $R = \mathbb{Z}$ and $A_i = n_i\mathbb{Z}$. Then A_i and A_j are comaximal for $i \neq j$.

So the following natural map $\varphi : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ defined by

$$x \mapsto (x \pmod{n_1},\ x \pmod{n_2},\ \cdots,\ x \pmod{n_k})$$

is surjective. Also $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_k}$ by 1st isomorphism theorem.

Let $(a_1, a_2, \cdots, a_k) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. Then there's $x \in \mathbb{Z}$ s.t.

$$x \equiv a_1 \pmod{n_1},\ x \equiv a_2 \pmod{a_2},\ \cdots,\ x \equiv a_k \pmod{n_k}$$

Then x is unique up to mod n by isomorphism theorem.

(b) Since $(a_1, a_2, \cdots, a_k) = \sum_{i=1}^{k} a_i e_i$ for $e_i = (0, 0, \cdots, 0, \overset{\text{ith coordinate}}{1}, 0, \cdots, 0)$, $\varphi(t_i \cdot \frac{n}{n_i}) = e_i$ for the inverse t_i of $\frac{n}{n_i} \pmod{n_i}$

we can find that

$$\varphi\left(\sum_{i=1}^{k} a_i t_i n_i'\right) = \varphi\left(\sum_{i=1}^{k} a_i t_i \frac{n}{n_i}\right) = \sum_{i=1}^{k} a_i\, \varphi\left(t_i \frac{n}{n_i}\right) = \sum_{i=1}^{k} a_i e_i$$

Hence $\sum_{i=1}^{k} a_i t_i n_i' \pmod{n}$ is the desired solution. ▨

(c) $\begin{cases} n_1 = 2^3 \\ n_2 = 5^2 \\ n_3 = 3^4 \end{cases}$ $\begin{cases} a_1 = 1 \\ a_2 = 2 \\ a_3 = 3 \end{cases}$

$(25 \times 81, 8) = 1 \to t_1 = 1$, $(8 \times 81, 25) = 1 \to t_2 = 12$, $(8 \times 25, 81) = 1 \to t_3 = 32$

$\therefore x = 1 \times 1 \times 2025 + 2 \times 12 \times 648 + 3 \times 32 \times 200 \pmod{16200}$

$\boxed{x \equiv 4377 \pmod{16200}}$

(d) Using (c) to get t_i's,

$x = 5 \times 1 \times 2025 + 12 \times 12 \times 648 + 47 \times 32 \times 200 \pmod{16200}$

$\boxed{\therefore x \equiv -763 \pmod{16200}}$

□

2. Homework 2 (Due: Apr 19)

For all problems, suppose that R is a ring with $1 \neq 0$ and M is a left R-module.

Problem 2.1. An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

(1) Prove that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M (called the torsion submodule of M).
(2) Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule. [Consider the torsion elements in the R-module R.]
(3) If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

Solution.

(1) Suppose that R is an integral domain.

Let $m, n \in \mathrm{Tor}(M)$, then $\exists\, r, s \in R$ s.t.

$rm = 0$. $sn = 0$.

$$rs(m + (-n)) = (rs)m + (rs)(-n) = s(rm) - r(sn) = 0$$

$\Rightarrow \mathrm{Tor}(M)$ is a subgroup of M.

$\forall\, m \in \mathrm{Tor}(M)$, $r \in R$. $\exists\, r_0 \in R$

$$r_0(rm) = (r_0 r)m = (r r_0)m = r(r_0 m) = r \cdot 0 = 0.$$

$rm \in \mathrm{Tor}(M)$

$\Rightarrow \mathrm{Tor}(M)$ is a submodule of M

(2) $R = M_{2\times 2}(\mathbb{Z})$, $M = R$, action : matrix multiplication.

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Tor}(M)$$

but $$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin \mathrm{Tor}(M).$$

(3) Let $r, s \in R$. $rs = 0$. M is an R-module.

$m \in M$. $m \neq 0$.

① If $sm = 0$, m is a nonzero tortion element

② If $sm \neq 0$, sm is a nonzero tortion element

$\square$

Problem 2.2. (1) If N is a submodule of M, the *annihilator of N in R* is defined to be $\{r \in R \mid rn = 0 \text{ for all } n \in N\}$. Prove that the annihilator of N in R is a 2-sided ideal of R.

(2) If I is a right ideal of R, the *annihilator of I in M* is defined to be $\{ m \in M \mid am = 0$ for all $a \in I\}$. Prove that the annihilator of I in M is a submodule of M.

(3) Let M be the abelian group (i.e., $\mathbb{Z}$-module) $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.
   (a) Find the annihilator of M in $\mathbb{Z}$ (i.e., a generator for this principal ideal).
   (b) Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.

Solution.

(1) N: submodule of $M \Rightarrow \mathrm{Ann}_R(N)$: 2-sided ideal of R.

$0_R \in R \Rightarrow 0_R \in \mathrm{Ann}_R(N) \Rightarrow \mathrm{Ann}_R(N) \neq \phi$.

for every $r_1, r_2 \in \mathrm{Ann}_R(N)$ and $r \in R$

- $(r_1 - r_2)n = r_1 n - r_2 n = 0 - 0 = 0$ for all $n \in N \Leftrightarrow r_1 - r_2 \in \mathrm{Ann}_R(N)$
- $(rr_1)n = r(r_1 n) = r0 = 0$ for all $n \in N \Leftrightarrow rr_1 \in \mathrm{Ann}_R(N)$
- $(r_1 r)n = r_1(rn) = 0$ for all $n \in N \Leftrightarrow r_1 r \in \mathrm{Ann}_R(N)$

$\to \mathrm{Ann}_R(N)$ is 2-sided ideal of R.

(2) I: right ideal of R, $\Rightarrow \mathrm{Ann}_M(I)$ is a submodule of M.

$0_R \in I \Rightarrow 0_R \in \mathrm{Ann}_M(I) \Rightarrow \mathrm{Ann}_M(I) \neq \phi$.

for every $a \in I$, $r \in R$, $m_1, m_2 \in M$

$$\begin{aligned} a(m_1 + rm_2) &= am_1 + a(rm_2) \\ &= am_1 + (ar)m_2 \\ &= 0 + 0 \quad (\because ar \in I) \\ &= 0 \end{aligned}$$

$\therefore m_1 + rm_2 \in \mathrm{Ann}_M(I)$

$\therefore$ by the submodule criterion

$\mathrm{Ann}_M(I)$ is a submodule of M.

(3) M : abelian group

$\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$

(a) $\mathrm{Ann}_{\mathbb{Z}}(M)$

α : annihilate $M \Leftrightarrow \alpha$: annihilate each coordinate

$\therefore \alpha \mid 24 \wedge \alpha \mid 15 \wedge \alpha \mid 50 \Rightarrow \alpha = \mathrm{lcm}\{24, 15, 50\}$
$= 600$

$\therefore \mathrm{Ann}_{\mathbb{Z}}(M) = 600\mathbb{Z}$

(b) $I = 2\mathbb{Z}$, $\mathrm{Ann}_M(I)$

the element in I : $2a$ $(a \in \mathbb{Z})$

Let $M = \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$

$\cdot\ (m_1, m_2, m_3) \in \mathrm{Ann}_M(I)$

$2am_1 \equiv 0 \mod 24 \Leftrightarrow m_1 \equiv 0, 12 \mod 24$

$2am_2 \equiv 0 \mod 15 \Leftrightarrow m_2 \equiv 0 \mod 15$

$2am_3 \equiv 0 \mod 50 \Leftrightarrow m_3 \equiv 0, 25 \mod 50$

$\therefore \mathrm{Ann}_M(I) = \{(0,0,0), (0,0,25), (12,0,0), (12,0,25)\}$

$\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

□

Problem 2.3. (1) Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\pi/2$ radians. Show that V and 0 are the only $F[x]$-submodules for this T.

(2) Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is projection onto the y-axis. Show that $V, 0$, the x-axis and the y-axis are the only $F[x]-$ submodules for this T.

(3) Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by π radians. Show that every subspace of V is an $F[x]$-submodule for this T.

Solution.

(1) The $F[x]$-submodules for T corresponds to the vector subspace $W \leq V$
s.t. T-invariant. $T(W) \subseteq W$. $T(x,y) = (y,-x)$.
Sps $\exists W_0$ satisfies T-invar and $0 \subsetneq W_0 \subsetneq V$. that W_0 is 1-dim'l $\simeq \mathbb{R}$.
However, T is a clockwise $\frac{\pi}{2}$ rotation that $T(W) \nsubseteq W$. So $\nexists W_0$
Therefore the T-invariant subspaces are just V and 0.
that V and 0 are the only $F[x]$-submodules for T.

(2) Similar as (1), $T(x,y) = (0,y)$.
Find the T invariant subspace W.
- Clearly 0 and V.
- 1-dim'l case, let (a,b) be the basis of W.

$T(a,b) = (0,b) = t(a,b)$, $\Rightarrow (-ta, (1-t)b) = (0,0)$,
$at = 0$ & $(1-t)b = 0$.
$\Rightarrow$ i) $a = 0$, $t = 1$. $\Rightarrow$ $(0,b) \Rightarrow W$: y-axis.
ii) $a \neq 0 \Rightarrow t = 0. \Rightarrow b = 0.$ $\Rightarrow (a,0) \Rightarrow W$: x-axis.

Therefore $0, V$, x-axis and y-axis.

(3) Similar as (1), (2) $T(x,y) = (-x,-y)$. Clearly 0 and V are T-invariant.
Through the geometric meaning of T, every basis elt (a,b) of 1-dim'l
Subspace goes to $(-a,-b)$ that lies on the same line.
Therefore every subspace of V is an $F[x]$-submodule of T.

□

Problem 2.4. (1) For any left ideal I of R define

$$IM = \left\{ \sum_{\text{finite}} a_i m_i \mid a_i \in I, m_i \in M \right\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

(2) Let $A_1, A_2, \ldots, A_n$ be R-modules and let B_i be a submodule of A_i for each $i = 1, 2, \ldots, n$. Prove that

$$(A_1 \times \cdots \times A_n) / (B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n).$$

(3) Let I be a left ideal of R and let n be a positive integer. Prove that

$$R^n/IR^n \cong R/IR \times \cdots \times R/IR \quad (n \text{ times}).$$

(4) Assume R is commutative. Prove that $R^n \cong R^m$ if and only if $n = m$, i.e., two free R-modules of finite rank are isomorphic if and only if they have the same rank. [Apply the previous problem with I a maximal ideal of R. You may use the fact that if F is a field, then $F^n \cong F^m$ if and only if $n = m$.]

Solution.

(1) I: left ideal of R, M: R-module

$IM = \{\sum_{\text{finite}} a_i m_i : a_i \in I,\ m_i \in M\}$ is a submodule of M.

$0_R \in R \Rightarrow 0_R \in I \Rightarrow 0_R \in IM \Rightarrow IM \neq \emptyset$.

Let $x = \sum a_i m_i$, $y = \sum b_j m_j$ with $a_i, b_j \in I$, $m_i, m_j \in M$.

for every $r \in R$

$x + ry = \sum a_i m_i + r \sum b_j m_j$

$= \sum a_i m_i + \sum r(b_j m_j) = \sum a_i m_i + \sum (rb_j) m_j$

$= \sum (a_i m_i + rb_j m_j) \in IM$ ($\because rb_j \in I$)

$\therefore$ by the submodule criterion

IM is a submodule of M

(2) $A_1, \cdots, A_n$: R-module, B_i: submodule of A_i, $i = 1, \cdots, n$

$A_1 \times \cdots \times A_n / B_1 \times \cdots \times B_n \cong A_1/B_1 \times \cdots \times A_n/B_n$

define a map $\varphi: A_1 \times \cdots \times A_n \longrightarrow A_1/B_1 \times \cdots \times A_n/B_n$

$(a_1, \cdots, a_n) \longmapsto \varphi(a_1, \cdots, a_n) = (a_1 + B_1, \cdots, a_n + B_n)$

Since $a_i + ra_i' + B_i = (a_i + B_i) + (ra_i' + B_i)$

$= a_i + B_i + r(a_i' + B_i)$ for all $i \in \{1, 2, \cdots, n\}$,

φ is R-module homomorphism

$\ker\varphi = \{(a_1, \cdots, a_n) : \varphi(a_1, \cdots, a_n) = (B_1, \cdots, B_n)\} = B_1 \times \cdots \times B_n$ ($\because a_i + B_i = 0 + B_i \Rightarrow a_i \in B_i$)

φ is surjective since,

$\therefore$ by the 1st isomorphic theorem

$A_1 \times \cdots \times A_n / B_1 \times \cdots \times B_n = A_1 \times \cdots \times A_n / \ker\varphi \cong \operatorname{im}\varphi = \varphi(a_1, \cdots, a_n)$

$= A_1/B_1 \times \cdots \times A_n/B_n$

(3) I: left ideal of R, $n \in \mathbb{Z}^+$

$R^n / IR^n \cong R/IR \times \cdots \times R/IR$

if $IR^n = (IR)^n$

then by (2) $R^n/IR^n = R^n/(IR)^n \cong R/IR \times \cdots \times R/IR$

So we have to show $IR^n = (IR)^n$

(i) $IR^n \subseteq (IR)^n$

for every $a \in I$, $r_i \in R$

$a(r_1, \cdots, r_n) \in IR^n \Rightarrow a(r_1, \cdots, r_n) = (ar_1, \cdots, ar_n) \in (IR)^n$

$\therefore IR^n \subseteq (IR)^n$

(ii) $IR^n \supseteq (IR)^n$

Consider arbitrarily $(a_1 r_1, \cdots, a_n r_n) \in (IR)^n$

Let $x_i = (0, \cdots, 0, a_i r_i, 0, \cdots, 0) \in IR^n$

then $x_i = a_i(0, \cdots, 0, r_i, 0, \cdots, 0)$

since IR^n is closed under finite sum

$(a_1 r_1, \cdots, a_n r_n) = \sum_{i=1}^{n} x_i \in IR^n$

$\therefore (IR)^n \subseteq IR^n$

$\therefore IR^n = (IR)^n$

$\therefore R^n/IR^n = R^n/(IR)^n \cong R/IR \times \cdots \times R/IR$

(4) R: commutative ring

$R^n \cong R^m \Leftrightarrow n = m$

$\Leftarrow$ We need to show if $|A| = |B|$ then $F(A) \cong F(B)$

Let $\varphi: A \longrightarrow B$: bijective map

$\varphi^{-1}: B \to A$: inverse of φ

then $\exists\, \Phi: F(A) \to F(B)$: R-module homomorphism

$\exists\, \Phi^{-1}: F(B) \to F(A)$: R-module homomorphism.

$\Phi^{-1} \circ \Phi = id_{F(A)} \to \Phi$ is injective

$\Phi \circ \Phi^{-1} = id_{F(B)} \to \Phi$ is surjective

$\}$ bijective

$\therefore \Phi: F(A) \to F(B)$: isomorphism

$\therefore F(A) \cong F(B)$

$\therefore n = m \Rightarrow R^n \cong R^m$

$\Rightarrow$ Let M, N: R-module with $M \cong N$ and let I: ideal of R

then $M/IM \cong N/IN$

$\because \varphi: M \to N$: isomorphism $\to$ $\exists\, \phi_1: M/IM \longrightarrow N/IN$, $m + IM \mapsto \phi_1(m) + IN$

$\exists\, \phi_2: N/IN \longrightarrow M/IM$, $n + IN \to \phi_2(n) + IM$

$\phi_2 \circ \phi_1$: id on M/IM

$\phi_1 \circ \phi_2$: id on N/IN

$\to \phi_1, \phi_2$: isomorphism

Now let $R^n \cong R^m$ and

I: maximal ideal of R.

then

$(R/IR)^n \cong R^n/IR^n \cong R^m/IR^m \cong (R/IR)^m$

$\therefore$ two vector spaces are isomorphic

$\therefore$ they have same rank

□

Problem 2.5. Let I be a nonempty index set and for each $i \in I$ let M_i be an R-module. The direct product of the modules M_i is defined to be their direct product as abelian groups (cf. Exercise 15 in Section 5.1) with the action of R componentwise multiplication. The direct sum of the modules M_i is defined to be the restricted direct product of the abelian groups M_i (cf. Exercise 17 in Section 5.1) with the action of R componentwise multiplication. In other words, the direct sum of the M_i's is the subset of the direct product, $\prod_{i\in I} M_i$, which consists of all elements $\prod_{i\in I} m_i$ such that only finitely many of the components m_i are nonzero; the action of R on the direct product or direct sum is given by $r\prod_{i\in I} m_i = \prod_{i\in I} rm_i$ (cf. Appendix I for the definition of Cartesian products of infinitely many sets). The direct sum will be denoted by $\oplus_{i\in I} M_i$.

(1) Prove that the direct product of the M_i's is an R-module and the direct sum of the M_i's is a submodule of their direct product.
(2) Show that if $R = \mathbb{Z}, I = \mathbb{Z}^+$ and M_i is the cyclic group of order i for each i, then the direct sum of the M_i 's is not isomorphic to their direct product. [Look at torsion.]

Solution.

(1) $\prod_{i\in I} M_i$ is abelian group by componentwise addition and the action of R on $\prod_{i\in I} M_i$ by componentwise scalar multiplication satisfies the R-module axioms by checking componentwisely. Therefore $\prod_{i\in I} M_i$ is R-module. $\blacksquare$

Also, $\bigoplus_{i\in I} M_i$ is R-module by checking one more condition : finitely many of the components are nonzero :

If $m, m' \in \bigoplus_{i\in I} M_i$, then $m+m'$ has finitely many nonzero components

$0 \in \bigoplus_{i\in I} M_i$ and $-m \in \bigoplus_{i\in I} M_i$ for all $m \in \bigoplus_{i\in I} M_i$.

Since all elements of $\bigoplus_{i\in I} M_i$ are in $\prod_{i\in I} M_i$, $\bigoplus_{i\in I} M_i$ is R-submodule of $\prod_{i\in I} M_i$. $\blacksquare$

(2) Suppose that $\bigoplus_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z} \simeq \prod_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}$ as $\mathbb{Z}$-module.

Then $\bigoplus_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z} = \prod_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}$ by (1) and $\mathrm{Tor}(\bigoplus_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}) = \mathrm{Tor}(\prod_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z})$

Since $\mathrm{Tor}(\bigoplus_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}) = \bigoplus_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}$ by vanishing all finite nonzero components, $\mathrm{Tor}(\prod_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}) \neq \prod_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}$: This is contradiction

($(0,1,1,1,\cdots) \in \prod_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}$ cannot be vanished.)

Hence $\bigoplus_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z} \not\simeq \prod_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}$

$\blacksquare$

$\square$

Problem 2.6. (1) Show that the element "$2 \otimes 1$" is 0 in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ but is nonzero in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.
(2) Show that $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ and $\mathbb{C}\otimes_{\mathbb{C}}\mathbb{C}$ are both left $\mathbb{R}$-modules but are not isomorphic as $\mathbb{R}$-modules.
(3) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ are isomorphic left $\mathbb{Q}$-modules. [Show they are both 1-dimensional vector spaces over $\mathbb{Q}$.]
(4) If R is any integral domain with quotient field Q, prove that $(Q/R) \otimes_R (Q/R) = 0$.
(5) Let $\{e_1, e_2\}$ be a basis of $V = \mathbb{R}^2$. Show that the element $e_1 \otimes e_2 + e_2 \otimes e_1$ in $V \otimes_{\mathbb{R}} V$ cannot be written as a simple tensor $v \otimes w$ for any $v, w \in \mathbb{R}^2$.

Solution.

(1) $2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$ in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$

Define $\varphi : 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by.

$$\varphi(2n, m) = nm$$

Then φ is $\mathbb{Z}$-balanced map with $\varphi(2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$

Hence there's an unique group homomorphism $\Phi : 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ s.t.

$\Phi(2 \otimes 1) = \varphi(2, 1) = 1 + 2\mathbb{Z}$ so that $2 \otimes 1 \neq 0$. (Otherwise $\Phi(2 \otimes 1) = 0$)

$\therefore 2 \otimes 1 \neq 0$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. $\blacksquare$

(2) Since $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ are vector spaces over $\mathbb{R}$ ($\because \mathbb{C}$ is both $(\mathbb{R}, \mathbb{R})$-bimodule and $(\mathbb{R}, \mathbb{C})$-bimodule.) But their rank is different :

$\{1 \otimes_{\mathbb{R}} 1, 1 \otimes_{\mathbb{R}} i, i \otimes_{\mathbb{R}} 1, i \otimes_{\mathbb{R}} i\}$, $\{1 \otimes_{\mathbb{C}} 1, 1 \otimes_{\mathbb{C}} i\}$ are bases of $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$, respectively :

$$(a+bi) \otimes_{\mathbb{R}} (c+di) = ac(1 \otimes_{\mathbb{R}} 1) + ad(1 \otimes_{\mathbb{R}} i) + bc(i \otimes_{\mathbb{R}} 1) + bd(i \otimes_{\mathbb{R}} i)$$

$$(a+bi) \otimes_{\mathbb{C}} (c+di) = 1 \otimes_{\mathbb{C}} (a+bi)(c+di) = (ac-bd)(1 \otimes_{\mathbb{C}} 1) + (ad+bc)(1 \otimes_{\mathbb{C}} i)$$

Hence they are not isomorphic by the rank. $\blacksquare$

(3) First, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ are left $\mathbb{Q}$-modules since $\mathbb{Q}$ is both $(\mathbb{Q}, \mathbb{Z})$-bimodule and $(\mathbb{Q}, \mathbb{Q})$-bimodule.

Also, they have same rank 1 so that they are isomorphic :

$$\left(\frac{a}{b}\right) \otimes_{\mathbb{Z}} \left(\frac{c}{d}\right) = \left(\frac{a}{bd} \times d\right) \otimes_{\mathbb{Z}} \left(\frac{c}{d}\right) = \left(\frac{a}{bd}\right) \otimes_{\mathbb{Z}} (c) = \left(\frac{ac}{bd}\right) \otimes_{\mathbb{Z}} 1 = \left(\frac{ac}{bd}\right)(1 \otimes_{\mathbb{Z}} 1)$$

$$\left(\frac{a}{b}\right) \otimes_{\mathbb{Q}} \left(\frac{c}{d}\right) = \left(\frac{a}{b} \times \frac{c}{d}\right) \otimes_{\mathbb{Q}} 1 = \left(\frac{ac}{bd}\right)(1 \otimes_{\mathbb{Q}} 1)$$

Hence $\{1 \otimes_{\mathbb{Z}} 1\}$, $\{1 \otimes_{\mathbb{Q}} 1\}$ are bases of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$, respectively.

So $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$. $\blacksquare$

(4) Let $\left(\frac{r_1}{r_2} + R\right) \otimes_R \left(\frac{r_4}{r_3} + R\right)$ be an element of $(\mathbb{Q}/R) \otimes_R (\mathbb{Q}/R)$ with $r_1 \neq 0, r_3 \neq 0$.

Then $\left(\frac{r_1}{r_2} + R\right) \otimes_R \left(\frac{r_4}{r_3} + R\right) = \left(\left(\frac{r_2}{r_1 r_3} + R\right) r_3\right) \otimes_R \left(\frac{r_4}{r_3} + R\right) = \left(\frac{r_2}{r_1 r_3} + R\right) \otimes_R (r_4 + R) = \left(\frac{r_2}{r_1 r_3} + R\right) \otimes_R (0 + R) = 0$.

Since we choose the element arbitrarly, $(\mathbb{Q}/R) \otimes_R (\mathbb{Q}/R) = 0$.

(5) Let $v = a_{11} e_1 + a_{12} e_2$ and $w = a_{21} e_1 + a_{22} e_2$. Then $e_1 \otimes e_2 + e_2 \otimes e_1 = v \otimes w$ implies that

$$(a_{11} a_{21}) e_1 \otimes e_1 + (a_{11} a_{22} - 1) e_1 \otimes e_2 + (a_{12} a_{21} - 1) e_2 \otimes e_1 + (a_{12} a_{22}) e_2 \otimes e_2 = 0.$$

So $a_{11} a_{21} = 0$, $a_{12} a_{22} = 0$, $a_{11} a_{22} = 1$, $a_{12} a_{21} = 1$ implies that $0 = 1$: contradiction!

Hence $e_1 \otimes e_2 + e_2 \otimes e_1$ cannot be expressed as $v \otimes w$. $\blacksquare$

$\square$

Problem 2.7. Suppose R is commutative and $N \cong R^n$ is a free R-module of rank n with R-module basis $e_1, \ldots, e_n$.

(1) For any nonzero R-module M show that every element of $M \otimes N$ can be written uniquely in the form $\sum_{i=1}^{n} m_i \otimes e_i$ where $m_i \in M$. Deduce that if $\sum_{i=1}^{n} m_i \otimes e_i = 0$ in $M \otimes N$ then $m_i = 0$ for $i = 1, \ldots, n$.

(2) Show that if $\sum m_i \otimes n_i = 0$ in $M \otimes N$ where the n_i are merely assumed to be R linearly independent then it is not necessarily true that all the m_i are 0 . [Consider $R = \mathbb{Z}, n = 1, M = \mathbb{Z}/2\mathbb{Z}$, and the element $1 \otimes 2$.

Solution.

(1) Pf) We can proof this statement using the isomorphism $\theta : M \bigotimes_R (R^n) = M \bigotimes_R (\bigoplus_n R) \cong \bigoplus_n (M \bigotimes R) \cong \bigoplus_n M$. ($\theta$ can be justifies by the good condition(commuatative ring) of R and inductivelty by the isomorphism of tho direct sum and tensor product isomorphism.) Furthermore, for all $i = 1, \ldots, n$, We can think a natural injection θ_i from $M \bigotimes (0, \cdots, R, \cdots, 0)$(only ith comoponent isn't zero) to $\bigoplus M$.Since $\bigoplus M$ is a direct sum, all elements has unique expression. And these injective maps tell the given unique form of the problem. Zero element is the trivial case of this consequence.

(2) Pf) Linear independent is weak condition to promise unique expression;

Pf) Let $R = \mathbb{Z}$, $n = 1$, $M = \mathbb{Z}/2\mathbb{Z}$ and the element $1 \bigotimes 2$. $1 \bigotimes 2 = 2 \bigotimes 1 = 0$. Hence doesn't have unique expression.

$\square$

Problem 2.8. Suppose that

$$\begin{tikzcd}
A \arrow[r, "\psi"] \arrow[d, "\alpha"'] & B \arrow[r, "\varphi"] \arrow[d, "\beta"'] & C \arrow[d, "\gamma"'] \\
A' \arrow[r, "\psi'"] & B' \arrow[r, "\varphi'"] & C'
\end{tikzcd}$$

is a commutative diagram of groups and that the rows are exact. Prove that

(1) if φ and α are surjective, and β is injective then γ is injective. [If $c \in \ker \gamma$, show there is a $b \in B$ with $\varphi(b) = c$. Show that $\varphi'(\beta(b)) = 0$ and deduce that $\beta(b) = \psi'(a')$ for some $a' \in A'$. Show there is an $a \in A$ with $\alpha(a) = a'$ and that $\beta(\psi(a)) = \beta(b)$. Conclude that $b = \psi(a)$ and hence $c = \varphi(b) = 0$.]
(2) if ψ', α, and γ are injective, then β is injective,
(3) if φ, α, and γ are surjective, then β is surjective,
(4) if β is injective, α and φ are surjective, then γ is injective,
(5) if β is surjective, γ and ψ' are injective, then α is surjective.

Solution.

(1) φ, α : surjective, β : injective $\Rightarrow \gamma$: injective

$\forall c \in \ker\gamma \quad \exists b \in B$ s.t. $c = \varphi(b)$ (φ: surjective)

$\Rightarrow \varphi'(\beta(b)) = \gamma(\varphi(b)) = 0$ (diagram commute) $\uparrow c \in \ker\gamma$

$\Rightarrow \beta(b) \in \ker\varphi' = \operatorname{im}\psi'$

$\Rightarrow \exists a' \in A'$ s.t. $\beta(b) = \psi'(a')$

$\Rightarrow \exists a \in A$ s.t. $a' = \alpha(a)$

$\Rightarrow \psi'(\alpha(a)) = \beta(\psi(a)) = \beta(b)$

$\Rightarrow \psi(a) = b$ (β: injective)

$\Rightarrow c = \varphi(b) = 0$

$\Rightarrow \gamma$: injective

(2) ψ', α, γ : injective, $\Rightarrow \beta$: injective

$\forall b \in \ker\beta, \quad \beta(b) = 0 \Rightarrow \varphi'(\beta(b)) = 0$

$\Rightarrow \gamma(\varphi(b)) = 0$

$\Rightarrow \varphi(b) = 0$

$\Rightarrow b \in \ker\varphi = \operatorname{im}\psi$

$\Rightarrow \exists a \in A$ s.t. $b = \psi(a)$

$\Rightarrow \beta(\psi(a)) = \psi'(\alpha(a)) = 0$

$\Rightarrow \alpha(a) = 0$ (ψ' : injective)

$\Rightarrow a = 0$ (α: injective)

$\Rightarrow b = \psi(a) = \psi(0) = 0$

$\Rightarrow \beta$: injective

(3) φ, α, γ : surjective $\Rightarrow \beta$: surjective.

$\forall b' \in B'$. let $c' = \varphi'(b')$

$\Rightarrow \exists c \in C$ s.t. $c' = \gamma(c)$ (γ : surjective)

$\Rightarrow \exists b \in B$ s.t. $c = \varphi(b)$ (φ: surjective)

$\Rightarrow \varphi'(\beta(b)) = \gamma(\varphi(b))$

$\Rightarrow \varphi'(\beta(b) - b') = 0$

$\Rightarrow \beta(b) - b' \in \ker\varphi' = \operatorname{im}\psi'$

$\Rightarrow \exists a' \in A'$ s.t. $\beta(b) - b' = \psi'(a')$

$\Rightarrow \exists a \in A$ s.t. $a' = \alpha(a)$

$\Rightarrow \psi'(\alpha(a)) = \beta(\psi(a))$

$\Rightarrow \beta(b) - b' = \beta(\psi(a))$

$\Rightarrow b' = \beta(b) - \beta(\psi(a))$

$= \beta(b - \psi(a))$

$\Rightarrow \beta$: surjective

(4) = (1)

(5) β: surjective, γ, ψ' : injective $\Rightarrow \alpha$: surjective

$\forall a' \in A' \quad \exists b' \in B'$ s.t. $b' = \psi'(a')$.

$\Rightarrow b' \in \operatorname{im}\psi' = \ker\varphi'$

$\Rightarrow \varphi'(b') = 0$

for each $b' \in B' \quad \exists b \in B$ s.t. $b' = \beta(b)$ (β: surjective)

$\Rightarrow \varphi'(\beta(b)) = \gamma(\varphi(b)) = 0$

$\Rightarrow \varphi(b) = 0$ (γ : injective)

$\Rightarrow b \in \ker\varphi = \operatorname{im}\psi$

$\Rightarrow \exists a \in A$ s.t. $b = \psi(a)$

$\Rightarrow \psi'(\alpha(a)) = \beta(\psi(a)) = \beta(b) = b' = \psi'(a')$

$\Rightarrow a' = \alpha(a)$ (ψ': injective)

$\Rightarrow \alpha$: surjective.

$\square$

Problem 2.9. Let P_1 and P_2 be R-modules. Prove that $P_1 \oplus P_2$ is a projective R-module if and only if both P_1 and P_2 are projective.

Solution.

Pf) $\Leftarrow$) Suppose that P_1 and P_2 are projective $R-$modules. Think the following diagram,

$$\begin{tikzcd}
& P_i \arrow[d, shift left, "\iota_i"] \\
& P_1 \bigoplus P_2 \arrow[u, shift left, "\Pi_i"] \arrow[d, "f"] \arrow[dl, dotted, "h"'] \\
A \arrow[r, "g"] & B \arrow[r] & 0
\end{tikzcd}$$

We can define $f_i : P_i \to B = f\iota_i$. Since, each P_i is projective, there exists $h_i : P_i \to A$ making the diagram commutes. Then these two homomorphism define the unique homomorphism $h : P_1 \bigoplus P_2 \to A$, defined by componentwisely through $h_i (i = 1, 2)$.

$\Rightarrow$) Suppose that $P_1 \bigoplus P_2$ is projecvtive and the following diagram is given. For $i = 1, 2$.

$$\begin{tikzcd}
& P_1 \bigoplus P_2 \arrow[d, shift left, "\Pi_i"] \\
& P_i \arrow[u, shift left, "\iota_i"] \arrow[d, "f"] \arrow[dl, dotted, "h"'] \\
A \arrow[r, "g"] & B \arrow[r] & 0
\end{tikzcd}$$

Since $P_1 \bigoplus P_2$ is projective, for $f' : P_1 \bigoplus P_2 \to B$ defined by $f' := f\Pi_i$. There exists $h' : P_1 \bigoplus P_2 \to A$ making the following diagram cummute. Define $h := h'\iota_i : P_i \to A$. Then $gh = g(h'\iota_i) = (gh')\iota_i = f'\iota_i = (f\Pi_i)\iota_i = f(\Pi_i\iota_i) = f1_{P_i} = f$. and so, each P_i is projective.

$\square$

Problem 2.10. Let $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$ be a sequence of R-modules.

(1) Prove that the associated sequence

$$0 \longrightarrow \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \longrightarrow 0$$

is a short exact sequence of abelian groups for all R-modules D if and only if the original sequence is a split short exact sequence. [To show the sequence splits, take $D = N$ and show the lift of the identity map in $\mathrm{Hom}_R(N, N)$ to $\mathrm{Hom}_R(N, M)$ is a splitting homomorphism for φ.]

(2) Prove that the associated sequence

$$0 \longrightarrow \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \longrightarrow 0$$

is a short exact sequence of abelian groups for all R-modules D if and only if the original sequence is a split short exact sequence.

Solution. (1)

Pf) $\Leftarrow$) It's enough to check $Hom_R(D, -)$ is exact. In other words, it's enough to show for all $f \in Hom(D, N)$, $f' \in Hom(D, M)$ such that $f = \varphi' f'$. Since the original exact sequence is split exact, there exists $\iota : N \to M$ such that $\varphi\iota = 1_N$. For all $f \in Hom(D, N)$ let $f' = \iota f \in Hom(D, M)$. Then $\varphi' f' = \varphi(\iota f) = (\varphi\iota)f = 1_N f = f$.

$\Rightarrow$) First, Put $D = R$, Then since $Hom(R, M) \cong M$, the original sequence is exact. Second, fix $D = N$. And choose $1_N \in Hom(N, N)$. Since the associated sequence is exact, there exists $\iota \in Hom(N, M)$ such that $\varphi'\iota = \varphi\iota = 1_N$. It implies the original sequence is a split sequence.

(2)

Pf) $\Leftarrow$) It's enough to check $Hom_R(-, D)$ is exact. In other words, it's enough to show ψ' is surjective map. Since the original sequence is split exact, there exists $\iota \in Hom(M, L)$ satisfying $\iota\psi = 1_L$. For all $f \in Hom(L, D)$, we can define $f' \in Hom(M, D)$ by $f' = f\iota$. Then $\psi' f' = \psi'(f\iota) = (f\iota)\psi = f(\iota\psi) = f1_L = f$. Hence ψ' is surjective.

$\Rightarrow$)If the original sequence is exact, we can make the following arguments make sense; fix $D = L$ Then $1_L \in Hom(L, L)$. Since the associated sequence is exact, there exists $\iota \in Hom(M, L)$ such that $\psi'\iota = \iota\psi = 1_L$. This implies the original sequence is a split sequence.

*The original sequence is exact.
Pf)
(1): φ is surjecvtive) Let $D = coker(\varphi)$. Then we can choose natural projection $\Pi \in Hom(N, D)$. Since φ' is injective and $\varphi'\Pi = \Pi\varphi = 0$, Π must be a zero map and φ is surjective.

(2): ψ is injective) Let $D = L$, Then for the identity, $1_L \in Hom(L, L)$. Since ψ' is surjective, there exists $f \in Hom(M, L)$ such that $\psi' f = f\psi = 1_L$. Hence ψ must be injective.

(3): $ker\varphi = im\psi$
$\supset$) By the exactness, $\psi'\varphi' = 0$ and so $0 = (\varphi\psi)'$.(I think it seems natural in the sense of a contravariant functor, but also we can see it easily by defining the map by the composition.) Let $D = N$ and choose the identity map $1_N \in Hom(N, N)$. Then $0 = (\varphi\psi)'1_N = 1_N(\varphi\psi) = \varphi\psi$. This implies $ker\varphi \supset im\psi$.

$\subset$) Now, let $D = coker(\psi)$ and choose the natural projection $\Pi \in Hom(M, D)$. Then $\psi'\Pi = 0$, and by the exactness there exists $f \in Hom(N, D)$ such that $\varphi' f = \Pi$. It means $ker\varphi \subset im\psi$.(It may use the contraposition of this proposition and contradiction. i.e, if $x \notin im\psi$, it can't be contained in $ker\varphi$. If not, $0 = \Pi(x) = f\varphi(x) \neq 0$. Contradiction!)

By (1), (2) and (3) the original sequence is exact.

$\square$