H.W.2

1.

(1)let $u = a_1b_1 + a_2b_2 + ... + a_nb_n$, $v = a_1^{'}b_1^{'} + a_2^{'}b_2^{'} + ... + a_n^{'}b_n^{'}$

$\Longrightarrow u - v = a_1b_1 + a_2b_2 + ... + a_nb_na_1^{'} + (-1)b_1^{'} + (-1)a_2^{'}b_2^{'} + ... + (-1)a_n^{'}b_n^{'}$

(2)A is a ideal

$\Longrightarrow rA \subseteq A$ for $r \in R$

$\Longrightarrow r(AB) = (rA)B \subseteq AB$

similarly, $(AB)r \subseteq AB$

2.

($\Rightarrow$) $1 + P \in R/P$, $0 + P \in R/P$

P is prime $\Longrightarrow P \neq R \Longrightarrow 1 \notin P \Longrightarrow 1 + P \neq P$

$\because R$ is commutative $\Longrightarrow R/P$ is commutative

if $(a + P)(b + P) = P$ where $a + P, b + P \in R/P$

$\Longrightarrow ab + P = P \Longrightarrow ab \in P \Longrightarrow a \in P$ or $b \in P(\because P$ is prime)

$\Longrightarrow a + P = P$ or $b + P = P$

($\Leftarrow$) R/P is an integral domain

$1 + P \neq P = 0 + P \Longrightarrow 1 \notin P \Longrightarrow P \neq R$

$\because ab \in P \Longrightarrow ab + P = P \Longrightarrow (a + P)(b + P) = P \Longrightarrow a + P = P$ or $b + P = P$

$\Longrightarrow a \in P$ or $b \in P \Longrightarrow P$ is prime

3.

(a) given $(a + M)$, $(b + M) \in R/M$

$(a + M)(b + M) = (ab + M) = (ba + M) = (b + M)(a + M) \therefore R/M$ is commutative

If $a + M \neq M$ then we want to find $(a + M)^{-1}$.

Since M is maximal, R is commutative $M + (a) = R$.

$\therefore 1 = m + ra$ for some $m \in M$, $r \in R$

$\Longrightarrow 1 - ra = m \in M \Longrightarrow 1 + M = ra + M = (r + M)(a + M) \Longrightarrow (a + M)^{-1}$ exists

(b) R/M is a division ring

$1 + M \neq 0 + M = M \Longrightarrow 1 \notin M \Longrightarrow M \neq R$

let $M \subseteq N \subseteq R$, N is an ideal $\Longrightarrow N \neq M$

let $a \in N - M$ $\exists ab + M = (a + M)(b + M) = 1 + M \Longrightarrow ab \in 1 + M$ (i.e. $\exists c \in M$ s.t. $ab = 1 + c$)

(c)let $R = M_2(\mathbb{R})$ then $\{ \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \}$ and R are the only ideals of R

$\Longrightarrow \{ \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \}$ is a maximal ideal of R

let $M = \{ \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \}$

We can find $(\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 0 & 0 \end{array} + M) \in R/M$

$$\begin{array}{cc} & \begin{array}{cc} 0 & 1 \end{array} \\ \begin{array}{c} 0 \\ 1 \end{array} & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{array}^{-1} \text{ not exists}$$

(d)R is commutative, M is a maximal ideal. $\Longrightarrow R/M$ is a field ($\because$ (a))
$\Longrightarrow R/M$ is an integral domain
$\Longrightarrow M$ is a prime ideal ($\because$ 3)

4.
(a)a_1, a_2, $a_3 \in R$
$\exists a \in R$ s.t. $a - a_i \in I_i$
$a_1 = b_1 + c_1$ where $b_1 \in I_1$, $c_1 \in I_2 \cap I_3$
$a_2 = b_2 + c_2$ where $b_2 \in I_2$, $c_2 \in I_1 \cap I_3$
$a_3 = b_3 + c_3$ where $b_3 \in I_3$, $c_3 \in I_1 \cap I_2$
Pick $a = c_1 + c_2 + c_3$
$a - a_1 = c_1 + c_2 + c_3 - (b_1 + c_1) = c_2 + c_3 - b_1 \in I_1$
Similarly, $a - a_2 \in I_2$, $a - a_3 \in I_3$

(b) define $\phi : R \to R/I_1 \times R/I_2 \times R/I_3$ by $\phi(a) = (a + I_1, a + I_2, a + I_3)$
check home. and onto(a), and $Ker(\phi) = I_1 \cap I_2 \cap I_3$. The problem then follows by first homomorphism theorem.

(c)let $I_1 = (n_1)$, $I_2 = (n_2)$, $I_3 = (n_3)$
By (a), choose a s.t. $a - a_i \in I_i$ (i.e. $a - a_i \pmod{n_i}$)
n_1, n_2, $n_3 \in \mathbb{N}$ where $(n_i, n_j) = 1, i \neq j$
$\mathbb{Z}/(lcm(n_1, n_2, n_3)) \cong \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \mathbb{Z}/(n_3)$

5.
(a)(6)

(b)check: $\sqrt{I}$ is an ideal
(i)if a, $b \in \sqrt{I} \Longrightarrow \exists n, m \in \mathbb{N}$ s.t. a^n, $a^m \in I$
$\Longrightarrow (a-b)^{n+m} = a^{n+m} - \binom{n+m}{1} a^{n+m-1} b + ... + (-1)^m \binom{n+m}{m} a^n b^m + (-1)^{m+1} \binom{n+m}{m+1} a^{n-1} b^{m+1} + ... + (-1)^{n+m} b^{n+m} \in I$
$\therefore a - b \in \sqrt{I}$
Let $a \in \sqrt{I}$, $b \in R$ (i.e. $\exists n$ s.t. $a^n \in I$)
$\Longrightarrow (ab)^n = a^n b^n \in I$ and $(ba)^n = b^n a^n \in I$, since I is commutative.

(ii)radical
if $a^n \in \sqrt{I} \Longrightarrow \exists m \in \mathbb{N}$ s.t. $(a^n)^m \in I \Longrightarrow a^{nm} \in I \Longrightarrow a \in \sqrt{I}$