2 Modules

2.1 Rings and ring homomorphisms

1. (a) It is obvious that $C_R(S) \neq \emptyset$.For any $b_1, b_2 \in C_R(S), a \in R$,
   $a(b_1 - b_2) = ab_1 - ab_2 = b_1a - b_2a = (b_1 - b_2)a$,
   and $a(b_1b_2) = (ab_1)b_2 = b_1(ab_2) = (b_1b_2)a$.
   Hence $C_R(S)$ is a subring of R.
   (b) According to the above, $C(D)$ is a subring of D.
   For any $b_1, b_2 \in C(D), d \in D$, then $b_1b_2 = b_2b_1$, so $C(D)$ is abelian.
   Since $b_1d^{-1} = d^{-1}b_1$, $b_1^{-1}d = db_1^{-1}$, i.e $b_1^{-1} \in C(D)$.
   Hence $C(D)$ is a field.
   (c) Since $E_{ii} \in M_n(P)$, $TE_{ii} = E_{ii}T$,then $t_{ij} = 0$ for $i \neq j$.
   And for $i \neq j, E_{ij} \in M_n(P)$,then $TE_{ij} = E_{ij}T$,then $t_{ii} = t_{ij}$.
   Hence $M_n(P) = \{kE | k \in P\}$.

2. For any $a, b \in R$, $(a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b = a + b$, so $ab = -ba$. Similarly, $(a - b)^2 = a^2 - ab - ba + b^2 = a + b = a - b$, then $b = -b$. Hence $ab = -ba = ba$, R is commutative.

3. (a) Since the sum of two subrings is a subring, $S + I$ is a ring. While I is an ideal of R and $I + S$ is a subring of R, so I is an ideal of $I + S$.
   For any $a_1, a_2 \in S \cap I$, any $b \in S$, $a_1b \in S \cap I$ and $ba_1 \in s \cap I$; moreover $a_1 - a_2 \in S \cap I$. Hence $S \cap I$ is an ideal of S.

(b) Define $\varphi : S+I \to S/(S\cap I)$, $a+I \mapsto a+(S\cap I)$ for any $a \in S$, then φ is a group epimorphism. According to the fundamental theory of homomorphism, $(S+I)/I \cong S/(S\cap I)$ as groups. For any $a_1, a_2 \in S$, $\varphi((a_1+I)(a_2+I)) = \varphi(a_1a_2+I) = a_1a_2 + (S\cap I) = (a_1 + (S\cap I))(a_2 + (s\cap I)) = \varphi(a_1+I)\varphi(a_2+I)$.Hence φ is a ring isomorphism.

4. (a) For any $a_1 + I, a_2 + I \in J/I$, and any $r + I \in R/I$, $(a_1 + I) - (a_2 + I) = (a_1 - a_2) + I \in J/I$, $(a_1 + I)(r + I) = (a_1r) + I \in J/I$ for $J \lhd R$, similarly $(r+I)(a_1+I) = (ra_1)+I \in J/I$.Hence $J/I \lhd R/I$.

   (b) Define $\varphi : R/I \to R/J$, $a + I \mapsto a + J$ for any $a \in R$, then φ is a group epimorphism. According to the fundamental theory of homomorphism, $(R/I)/(J/I) \cong R/J$ as groups. For any $a_1, a_2 \in S$, $\varphi((a_1+I)(a_2+I)) = \varphi(a_1a_2+I) = a_1a_2+J = (a_1 + J)(a_2 + J) = \varphi(a_1 + I)\varphi(a_2 + I)$.Hence φ is a ring isomorphism.

5. For any subring $Ker(f) \subseteq K$ of R, then $f(K) \subset S$. For any $a, b \in f(K)$, there exist $x, y \in R$, s.t. $f(x) = a, f(y) = b$, then $a - b = f(x) - f(y) = f(x - y) \in f(K)$ and $ab = f(x)f(y) = f(xy) \in f(K)$, hence $f(K)$ is a subring of S.Inverse, for any subring H of S, then $Ker(f) = f^{-1}(0) \subseteq f^{-1}(H) \subseteq R$. For any $a, b \in f^{-1}(H)$, there exist $x, y \in H$ such that $f(a) = x, f(b) = y$, then $f(a - b) = f(a) - f(b) = x-y \in H$ and $f(ab) = f(a)f(b) = xy \in H$, therefore $a - b \in f^{-1}(H)$ and $ab \in f^{-1}(H)$.Hence $f^{-1}(H)$ is a subring of R.

6. Let $\Omega = \{I | I \lhd R, I is nilpotent\}$, for any $I_1, I_2 \in \Omega$, there exist $n_1, n_2 \in \mathbb{Z}$ such that ${I_1}^{n_1} = {I_2}^{n_2} = 0$, then $(I_1 + I_2)^{n_1+n_2} = \{\sum a_{i_1}...a_{i_{n_1+n_2}} | a_{i_j} \in I_1 \cap I_2\}$. In product $a_{i_1}...a_{i_{n_1+n_2}}$, there are at least n_1 elements belong to I_1, since I_1 is an ideal, $a_{i_1}...a_{i_{n_1+n_2}} \in {I_1}^{n_1} = 0$; or there are at least n_2 elements belong to I_2, since I_2 is an ideal, $a_{i_1}...a_{i_{n_1+n_2}} \in {I_2}^{n_2} = 0$. Therefore $I_1 + I_2 \in \Omega$. Since R is a finite ring, there exists a only ideal I which contains the most elements, for any other ideal $J \in \Omega$, $J+I \in \Omega$ and $J+I \supseteq I$, hence $J+I = I$. If $L/I \neq \overline{0}$ is a nilpotent ideal of R/I, then there exists $m \in \mathbb{Z}$ such that $(L/I)^m = L^m+I/I = \overline{0}$, i.e $L^m \subseteq I$. Since $I^n = 0$, $L \in \Omega$, hence $L \subseteq I$.

7. According to exercise 2.1.5, there is a bijection between the set of all subrings of R which contain $Ker(f)$ and the set of all subrings of S. Thus there exists corresponding subring $f^{-1}(H)$ of R for any subring H of S. Since R is PID, then $f^{-1}(H)$ is principal, i.e. there exists $a \in f^{-1}(H)$ such that $f^{-1}(H) =< a >$, then $H = f(f^{-1}(H)) =< f(a) >$. Hence every ideal of S is principal.

8. (a) If there is not a least positive integer n such that $n \cdot a = 0$ for any $a \in R$, then $char(R) = 0$. Otherwise, if $char(R) = n$ is not prime and $n = sr$ where $1 < s, r < n$, then $ra \neq 0$, $sa \neq 0$ and $ra \cdot sa = rsa \cdot a = 0$, but R is a domain, therefore $char(R)$ is prime.

(b) For any $(\overline{a}, b), (\overline{c}, d), (\overline{e}, f) \in S$,

$$((\overline{a}, b)(\overline{c}, d))(\overline{e}, f) = (\overline{ac}, ad + cb + bd)(\overline{e}, f)$$
$$= (\overline{ace}, acf + ead + ecb + ebd + adf + cbf + bdf)$$

$$(\overline{a}, b)((\overline{c}, d)(\overline{e}, f)) = (\overline{a}, b)(\overline{ce}, cf + ed + df)$$
$$= (\overline{ace}, acf + ead + ecb + ebd + adf + cbf + bdf)$$

then $((\overline{a}, b)(\overline{c}, d))(\overline{e}, f) = (\overline{a}, b)((\overline{c}, d)(\overline{e}, f))$;

$$(\overline{a}, b)((\overline{c}, d) + (\overline{e}, f)) = (\overline{a}, b)(\overline{c+e}, d + f)$$
$$= (\overline{a(c+e)}, ad + af + cb + eb + bd + bf)$$
$$= (\overline{a}, b)(\overline{c}, d) + (\overline{a}, b)(\overline{e}, f)$$

then $(\overline{a}, b)((\overline{c}, d)+(\overline{e}, f)) = (\overline{a}, b)(\overline{c}, d)+(\overline{a}, b)(\overline{e}, f)$; similarly, $((\overline{a}, b) + (\overline{c}, d))(\overline{e}, f) = (\overline{a}, b)(\overline{e}, f) + (\overline{c}, d)(\overline{e}, f)$. And there are $(\overline{1}, 0) \in S$ such that $(\overline{a}, b)(\overline{1}, 0) = (\overline{1}, 0)(\overline{a}, b) = (\overline{a}, b)$. Hence S is a ring with identity.

(c) It is obvious that φ is injective. For any $a, b \in R$, $\varphi(a+b) = (0, a+b) = (0, a)+(0, b) = \varphi(a)+\varphi(b)$ and $\varphi(a)\varphi(b) = (0, a)(0, b) = (0, ab) = \varphi(ab)$, therefore φ is a ring monomorphism.

9. Since F is a field, for any $a, b \in F$, $ab = ba$, then $(a + b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$, in particular, $(a + b)^p = \sum_{k=0}^{p} C_p^k a^{p-k} b^k$. Then $C_p^k a^{p-k} b^k = 0, 1 \leq k \leq p - 1$ for $p \mid C_k^p, 1 \leq k \leq p - 1$. Thus $(a + b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$, therefore φ is a ring endomorphism of F. While $Ker\varphi \lhd F$, then $Ker\varphi = 0$ or $Ker\varphi = F$. While for any $0 \neq a \in F$, $\varphi(a) = a^p \neq 0$, thus

$Ker\varphi = 0$, i.e. φ is injective. Hence when F is a finite domain, φ is surjective. Therefore F is perfect.

10. If $a + b\sqrt{p} = 0$ where $a, b \in \mathbb{Q}$, then $\sqrt{p} = -\frac{a}{b} \in \mathbb{Q}$ or $b = 0$, thus $a = 0$, therefore $1, \sqrt{p}$ is linear independent in $\mathbb{Q}$. Similarly, $1, \sqrt{q}$ is linear independent in $\mathbb{Q}$. Since $\mathbb{Q}[\sqrt{p}], \mathbb{Q}[\sqrt{q}]$ both are linear spaces in $\mathbb{Q}$ of dimension 2. Thus they are isomorphic as linear spaces in $\mathbb{Q}$. If there is an isomorphism $\varphi : \mathbb{Q}[\sqrt{p}] \to \mathbb{Q}[\sqrt{q}]$, then $\varphi(\sqrt{p}^2) = \varphi(p) = \varphi(1) + \cdots + \varphi(1) = p$, thus $\varphi(\sqrt{p}) = \pm\sqrt{p} = \mathbb{Z}[\sqrt{q}]$, therefore $\pm\sqrt{p} = a + b\sqrt{q}$, then $p = a^2 + 2ab\sqrt{q} + b^2 q$, thus $2ab\sqrt{q} = p - a^2 - b^2 q$ is rational number. If $a = 0$,then $\pm\sqrt{p} = b\sqrt{q}$,thus $p = b^2 q$, then $p \mid b$, therefore $b = kp$, hence $k^2 q = 1$, it is a contradiction. If $b = 0$, then $\pm\sqrt{p} = a$ is rational number, it is a contradiction.Thus $\pm\sqrt{p} \notin \mathbb{Z}[\sqrt{q}]$, hence φ is not a ring isomorphism.

11. (a) Define $\varphi : F[x] \setminus 0 \to \mathbb{N}$, $\varphi(f(x)) = deg(f(x))$ for any $f(x) \in F[x]$. For $f(x), g(x) \in F[x]$, and $f(x)g(x) \neq 0$, then $deg(f(x)g(x)) = deg(f(x)) + deg(g(x)) \geq deg(f(x))$. For $f(x), g(x) \in F[x]$, and $g(x) \neq 0$, according to division algorithm, then φ satisfied the conditions of Euclidean ring. And for any subring H, there exists a element $g(x)$ of least degree such that $H =< g(x) >$, then $F[x]$ is an ED.

    (b) Define $\varphi : \mathbb{Z} \setminus 0 \to \mathbb{N}$, $\varphi(a) = |a|$ for any $a \in \mathbb{Z}$. For $a, b \in \mathbb{Z}$, and $ab \neq 0$, then $|ab| = |a||b| \geq |a|$ for $|b| \neg 1$. For $a, b \in F[x]$, and $b \neq 0$, according to division algorithm, then φ satisfied the conditions of Euclidean ring. And for any subring H, there exists a element b of least absolute value such that $H =< b >$, then $\mathbb{Z}$ is an ED.

(c) Define $\varphi : \mathbb{Z}[\sqrt{-1}]\backslash 0 \to \mathbb{N}$, $\varphi(a+b\sqrt{-1}) = a^2+b^2$ for any $a+b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$, For $a+bi, c+di \in \mathbb{Z}$, and $(a+bi)(c+di) = (ac-bd)+(ad+bc)i \neq 0$, then $(ac-bd)^2+(ad+bc)^2 = (a^2+b^2)(c^2+d^2) \geq a^2+b^2$. For $a+bi, c+di \in \mathbb{Z}$, and $c+di \neq 0$, denote $p+qi = \frac{a+bi}{c+di}$ where $p, q \in \mathbb{Q}$, then there are $s, r \in \mathbb{Z}$ such that $|s-p| \leq \frac{1}{2}$ and $|r-q| \leq \frac{1}{2}$, thus $a+bi = (s+ri)(c+di)+k+li$, and $k^2+l^2 = ((p-s)^2+(q-r)^2)(c^2+d^2) \leq \frac{1}{2}(c^2+d^2)$, then φ satisfied the conditions of Euclidean ring. And for any subring H, there exists a element $c+d\sqrt{-1}$ of least modulus such that $H =< c+d\sqrt{-1} >$, then $\mathbb{Z}[\sqrt{-1}]$ is an ED.

12. $(\frac{1+\sqrt{-19}}{2})^0 = 1$, therefore $R =< (\frac{1+\sqrt{-19}}{2}) >$, i.e. R is a PID. Since every Euclidean ring is unique factorization domain, but $((\frac{1+\sqrt{-19}}{2})(\frac{-3-\sqrt{-19}}{2})) = 5 = 5 \cdot 1$, hence R is not a Euclidean domain.

13. $(\Rightarrow)$:J is an ideal of $M_n(R)$, $I' = e_{11}Je_{11}$, define

$$I = \{a | e_{11}a'e_{11} = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, a' \in J\},$$

where $e_{11} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$. It is obvious that $(I, +) \leq (R, +)$, for any $a \in I$ and any $r \in R$,

$e_{11}a'e_{11}\cdot(rE) = are_{11} = e_{11}a'(rE)e_{11}$ where $a' = (a_{ij})$ and $a_{11} = a$. Thus $ar \in I$, similarly, $ra \in I$, hence $I \lhd R$. Since $e_{11}a'e_{11} \in J$, $e_{11}a'e_{11} = ae_{11} \in J$ for any $a \in I$, while $e_{i1}ae_{11}e_{1j} = ae_{ij} \in J$, then $M_n(I) \subset J$. For any $A = (a_{ij}) \in J, a_{ij} \neq 0$, then $e_{1i}Ae_{j1} = a_{ij}e_{11} \in J$, thus $a_{ij} \in I$, therefore $J \subset M_n(I)$, hence $J = M_n(I)$.

($\Leftarrow$):For any $(a_{ij}) \in M_n(\mathbb{R})$, $a_{ij} \in \mathbb{R}$, and any $(b_{ij}) \in M_n(\mathbb{I})$, $b_{ij} \in \mathbb{I}$, $(a_{ij})(b_{ij}) = (c_{ij})$, $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$, since $I \lhd R$, $(c_{ij}) \in M_n(\mathbb{I})$. Similarly, $(b_{ij})(a_{ij}) = (d_{ij})$, $d_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}$, hence $J \lhd M_n(\mathbb{R})$.

14. If there are $I \lhd M_n(R)$ such that $I \neq 0$ and $I \neq R$, then there are $0 \neq (a_{ij}) \in I$, according to Exercise 2.1.13, $M_n(R)$ is simple.

15.

$$\begin{aligned}\pi_i((a_i)_{i\in I}(b_i)_{i\in I}) &= \pi_i((a_ib_i)_{i\in I}) \\ &= a_ib_i = \pi_i((a_i)_{i\in I})\pi_i((b_i)_{i\in I})\end{aligned}$$

Since π_i is a abelian group homomorphism, π_i is a ring homomorphism. Similarly, we can proof that ι_i is a ring homomorphism.

16. If $e_i = (0, \cdots, 0, 1_{R_i}, 0, \cdots, 0)$,then $e_1 + \cdots + e_n = 1_R$. Define $A_i = \pi_i(e_i(I)) = \pi_i(I)$ where π_i is a canonical projection. For any $a \in R_i$ and any $b \in A_i$, then $a = \pi_i\iota_i(a), a \cdot b = \pi_i(\iota_i(a))\pi_i(e_ix) = \pi_i(\iota(a)e_ix)$ where $\pi_i(e_ix) = b, x \in I$, thus $ab \in A_i$, similarly, $ba \in A_i$, this means $A_i \lhd R_i$. Let $I' = A_1 \times \cdots \times A_n$, for any $a \in I$, $a = (\pi_1(a), \pi_2(a), \cdots, \pi_n(a)) \in I'$, then $I \subset I'$. For any $(a_1, \cdots, a_n) \in I'$, then there are

$b_i \in I$ such that $\pi_i(b_i) = a_i$, let $a = \sum_{i=1}^{n} e_i b_i \in I$, then $(a_1, \cdots, a_n) = (\pi_1(a), \cdots, \pi_n(a)) \in I'$. Hence $I = A_1 \times \cdots \times A_n$.

For example, $R = \mathbb{Z} \times \mathbb{Z}$ is a group about additive and define multiplication $(a, b) \cdot (c, d) = (0, 0)$, and $I = \{(3n, 9n) | n \in \mathbb{Z}\} \lhd R$, but there isn't I_1, I_2 such that $I = I_1 \times I_2$.

17. (1)$\Rightarrow$(2):Let $e_i = (0, \cdots, 0, 1_{R_i}, 0, \cdots, 0)$, then $e_i e_j = \delta_{ij} e_i$, $e_i(a_1, \cdots, a_n) = (0, \cdots, 0, a_i, 0, \cdots, 0) = (a_1, \cdots, a_n)e_i$ and $\sum_{i=1}^{n} e_i = (1, \cdots, 1)$ is an identity of $R_1 \times \cdots \times R_n$.

    (2)$\Rightarrow$(1):Let $R_i = e_i R$, then $R = \sum_{i=1}^{n} R_i$. For any $a \in R_1 \cap \sum_{i=2}^{n} R_i$, then $a = \sum_{i=1}^{n} e_i a = e_1 a + \cdots + e_n a$, thus $e_1 a = a$ and $e_2 a + \cdots + e_n a = 0$, while $e_i(e_2 a + \cdots + e_n a) = e_i a = e_i 0 = 0$, and $a = e_1 a = e_2 b_2 + \cdots + e_n b_n$, therefore $a = e_1 a = e_1(e_2 b_2 + \cdots + e_n b_n) = 0$, hence $R_1 \cap \sum_{i=2}^{n} R_i = 0$. Similarly, $R_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{n} R_j = 0$. Thus $R = \bigoplus_{i=1}^{n} R_i$ as abelian group. While $R e_i R = e_i R^2 \subset e_i R$, $e_i R \cdot R \subset e_i R$, thus $e_i R \lhd R$, hence $R \simeq R_1 \times \cdots \times R_n$.

18. According to Exercise 2.1.11, $\mathbb{Z}[i]$ is an ED. Since $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2 + 1)$, $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2 + 1) \cong (\mathbb{Z}[x]/(p))/((x^2 + 1, p)/(p)) \simeq \mathbb{Z}_p[x]/(x^2 + 1)$.

19. If $R = \{a_1, \cdots, a_n\}$ is a finite domain, then for any $a, b \in R$, if $a a_i = a a_j$, then $a(a_i - a_j) = 0$, thus $a_i =$

a_j for R is a domain. This means $\{aa_1, \cdots, aa_n\} = R = \{a_1, \cdots, a_n\}$. Since $b \in R$, there is $a_i \in R$ such that $aa_i = b$, similarly, there is $a_j \in R$ such that $a_j a = b$. Since there is $e \in R$ such that $ea = a$ for any $a \in R$, and there is $c \in R$ such that $bc = a$, $ea = eba = bc = a$. Moreover, for any $a \in R$, there is $a' \in R$ such that $a'a = e$. According to Exercise 1.1.6, $(R, \cdot)$ is a group. Hence R is a field.