Abstract Algebra I
Homework 8

B13902024 張沂魁

Due: 26th November 2025

In this course all rings R are commutative and contain the multiplicative identity 1_R. Furthermore, unless otherwise mentioned, R is **NEVER** the trivial ring, i.e., $R \neq \{0_R\}$. In particular, $R^2 = R$. We begin with some definitions; all questions are on the next page.

A subset I of R is called an **ideal** of R if for all $a, b \in I$ and $r \in R$, we have

(i) $a - b \in I$; and

(ii) $ra \in I$.

(We do not differentiate between left and right ideals.) If $I = 0$, it is called the **trivial ideal**. If $I \neq R$, it is called a **proper ideal**. One easily checks that $I = R$ if and only if $1_R \in I$. Consequently, a nonzero ideal I of R is proper if and only if it does not contain any invertible element of R. Note that from here on we shall use the term **unit** instead of invertible element.

Given an ideal I of R, we may define the quotient group R/I in which addition is given by

$$(a + I) + (b + I) = (a + b) + I.$$

Furthermore, R/I is a ring called the **quotient ring** with multiplication

$$(a + I)(b + I) = ab + I,$$

and has multiplicative identity $1_R + I$. (Check yourself that this multiplication is well-defined.)

A **field** is a ring such that every nonzero element is a unit. A **prime ideal** P of R is a proper ideal such that

$$ab \in P \quad \Longrightarrow \quad a \in P \quad \text{or} \quad b \in P.$$

A **maximal ideal** M is a proper ideal such that if there is another proper ideal M' with $M \subset M'$, then $M' = M$.

Remark. In this course we shall also assume every proper ideal of R is contained in some maximal ideal. This can be shown using Zorn's lemma. In fact these statements are equivalent, but you have to prove it via an equivalent form of Zorn's lemma —the existence of a choice function, or more commonly known as the Axiom of Choice.

Exercise 1 Let R be a ring, and I an ideal of R.

(a) Prove that if I is maximal, then it is a prime ideal.

(b) Prove that I is prime if and only if R/I is an integral domain.

(c) Prove that I is maximal if and only if R/I is a field.

Solution:

(a) If I is maximal, then suppose $ab \in I$ for some $a, b \in R$, then we want to show $a \in I$ or $b \in I$. If $a \in I$, then we're done. If $a \notin I$, then consider

$$(I, a) = \{x + ar : x \in I, r \in R\},$$

then we claim that (I, a) is an ideal. For $c, d \in (I, a)$, we know $c = x_1 + ar_1$ and $d = x_2 + ar_2$ for some $x_1, x_2 \in I$ and $r_1, r_2 \in R$, then

$$c - d = (x_1 - x_2) + a(r_1 - r_2) \in (I, a)$$

since $x_1 - x_2 \in I$ and $r_1 - r_2 \in R$ by the definition of ideals and rings. Also, if $e = x + ar \in (I, a)$ for $x \in I$ and $r \in R$, then for any $f \in R$, we know

$$fe = f(x + ar) = fx + a(rf) \in (I, a)$$

since $fx \in I$ and $rf \in R$. Hence, (I, a) is an ideal. Note that $I \subseteq (I, a)$ since for all $i \in I$, we know $i = i + a \cdot 0$, so $i \in (I, a)$ and we're done. Now since I is maximal, so if (I, a) is proper, then $(I, a) = I$, but note that $a \notin I$ but $a \in (I, a)$, so $(I, a) \neq I$, and thus (I, a) cannot be proper, i.e. $(I, a) = R$. Since $(I, a) = R$, so

$$1_R = x + ar \text{ for some } x \in I \text{ and } r \in R,$$

so we have

$$b = bx + (ab)r = bx - (-r)(ab) \in I$$

since $bx \in I$ and $ab \in I$. Hence, if $a \notin I$, then $b \in I$, and thus I is an prime ideal.

(b) If I is prime, and suppose by contradiction, R/I is not an integral domain, then $(a + I)(b + I) = I$ for some $a, b \in R$ s.t. $a + I \neq I$ and $b + I \neq I$, i.e. $a, b \notin I$. Note that

$$ab + I = (a + I)(b + I) = I,$$

so $ab \in I$, but since I is prime, so $a \in I$ or $b \in I$, which is a contradiction, so R/I is an integral domain.

Now if R/I is an integral domain, and suppose $ab \in I$ for some $a, b \in R$, then

$$I = ab + I = (a + I)(b + I),$$

so $a + I = I$ or $b + I = I$ since R/I is an integral domain, and this means $a \in I$ or $b \in I$, which shows I is an prime ideal.

(c) If I is maximal, then for all $a \in R$ s.t. $a + I \neq I$, we know $(I, a) = R$, so there exists $i \in I$ and $r \in R$ s.t.

$$1_R = i + ra.$$

Now since $i \in I$, so $i + I = I$ and thus $ra + I = ra + i + I = 1 + I$, and thus $(r + I)(a + I) = ra + I = 1 + I$, which shows $a + I$ is a unit. Now if $a + I = I$, then $a + I$ is $0_{R/I}$, so we don't have to check whether such $a + I$ is a unit, and thus we have shown that R/I is a field.

Now if R/I is a field, then we want to show I is maximal. Suppose $I \subseteq J \subsetneq R$ and J is an ideal, then $J/I \subseteq R/I$, and since

- $\forall j_1, j_2 \in J$, $(j_1 + I) - (j_2 + I) = (j_1 - j_2) + I \in J \in I$.
- $\forall (r + I) \in R/I$ and $j + I \in J/I$, $(r + I)(j + I) = rj + I \in J/I$.

Thus, J/I is an ideal of R/I. Now we claim that if I is an ideal of a field F, then $I = \{0\}$ or $I = F$. If $I = \{0\}$, then we're done. If $\exists a \neq 0$ s.t. $a \in I$, then $a^{-1} \in F$, and thus $1_F = a^{-1} \cdot a \in I$, but this gives $I = F$ since $f = f \cdot 1_F \in I$ for all $f \in F$. Hence, the claim is proved. Now by this claim, we know $J/I = \{0_{R/I}\}$ or $J/I = R/I$.

- Case 1: $J/I = \{0_{R/I}\}$, then for all $j \in J$, we know $j + I = I$, i.e. $j \in I$, so $J = I$.
- Case 2: $J/I = R/I$, then $\forall r \in R$, we have $r + I = j + I$ for some $j \in J$, so $r = j + i'$ for some $i' \in I \subseteq J$. Hence, $r = j + i' \in J$, and thus $R \subseteq J$, which gives $R = J$.

However, we suppose $J \neq R$, so the only possible case is Case 1, which shows $J = I$, and thus I is maximal.

Exercise 2 Prove that 0 is a maximal ideal of a ring R if and only if every homomorphism of rings $R \to S$ is injective.

Solution: If 0 is a maximal ideal of a ring R, and suppose $\varphi : R \to S$ is some ring homomormophism, then consider $\ker \varphi$:

- If $a, b \in \ker \varphi$, then $\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$.
- If $r \in R$ and $a \in \ker \varphi$, then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0$.

Hence, $\ker \varphi$ is an ideal of R. Since $0 \in \ker \varphi$ and 0 is an maximal ideal, so $\ker \varphi = \{0\}$ or $\ker \varphi = R$. If $\ker \varphi = R$, then $\varphi(1_R) = 0_S \neq 1_S$ since we suppose all rings here are not the trivial ring, so φ violates the definition of a ring homomorphism, which is a contradiction. Hence, $\ker \varphi = \{0\}$, and thus φ is injecitve. Since this proof can be used for every ring homomorphism from R to S, so every homomorphism of rings $R \to S$ is injective.

Now if every homomorphism of rings $R \to S$ is injective, and suppose by contradiction 0 is not a maximal ideal of R, then there exists a proper ideal A of R s.t. $\exists a \in A$ s.t. $a \neq 0$. Then, consider

$$\pi : R \to R/A, \quad a \mapsto r + A,$$

we know π is a ring homomorphism. (and R/A is not the trivial ring) However,

$$\pi(0) = A = a + A = \pi(a),$$

so π is not injective, which is a contradiction.

Exercise 3 Let I be an ideal of R and let

$$\operatorname{Rad} I = \{r \in R : r^n \in I \text{ for some (positive integer) } n\}.$$

Show that $\operatorname{Rad} I$ is an ideal of R. (Please do not interpret the set wrongly; n is not fixed.)

Solution: If $a, b \in \operatorname{Rad}(I)$, then $a^{n_1}, b^{n_2} \in I$ for some $n_1, n_2 \in \mathbb{N}$. Now we claim that $(a-b)^{n_1 n_2} \in I$ and thus $a - b \in \operatorname{Rad}(I)$. From now on, if we write zr for $z \in \mathbb{N}$ and $r \in R$, then it means

$$\underbrace{r + r + \cdots + r}_{z \text{ times}}.$$

Hence, by Binomial theorem, we know

$$(a-b)^{n_1 n_2} = \sum_{k=0}^{n_1 n_2} \binom{n_1 n_2}{k} a^k (-b)^{n_1 n_2 - k}. \tag{1}$$

Note that since R is commutative so the Binomial theorem holds. Now we claim that if $n_1 \geq 2$, then in each term of Equation 1 we have $k \geq n_1$ or $n_1 n_2 - k \geq n_2$. If not, then $k < n_1$ and $n_1 n_2 - k < n_2$ for some $0 \leq k \leq n_1 n_2$, but this gives

$$n_1(n_2 - 1) = n_1 n_2 - n_1 < n_1 n_2 - k < n_2,$$

and this is impossible if $n_1 \geq 2$. Hence, the claim is true. Thus, if $n_1 \geq 2$, then in each term we have $k \geq n_1$ or $n_1 n_2 - k \geq n_2$, and this means

$$\binom{n_1 n_2}{k} a^k (-b)^{n_1 n_2 - k} \in I$$

for all $0 \leq k \leq n_1 n_2$ by the definition of ideals, and thus

$$\sum_{k=0}^{n_1 n_2} \binom{n_1 n_2}{k} a^k (-b)^{n_1 n_2 - k} \in I.$$

Now if $n_1 = 1$, then

$$(a-b)^{n_1 n_2} = (a-b)^{n_2} = \sum_{k=0}^{n_2} \binom{n_2}{k} a^k (-b)^{n_2 - k},$$

and for $k = 0$ we know

$$\binom{n_2}{0} a^0 (-b)^{n_2 - 0} = (-b)^{n_2} \in I,$$

and for $1 \leq k \leq n_2$ we know

$$\binom{n_2}{k} a^k (-b)^{n_2 - k} \in I$$

since $a \in I$. Hence, we have

$$\sum_{k=0}^{n_2} \binom{n_2}{k} a^k (-b)^{n_2 - k},$$

and thus we have shown that for every case $(a-b)^{n_1 n_2} \in I$, i.e. $a - b \in \operatorname{Rad}(I)$.

If $a \in \mathrm{Rad}(I)$, then $a^n \in I$ for some $n \in \mathbb{N}$, and for all $r \in R$, we have

$$(ra)^n = r^n \cdot a^n \in I,$$

which means $ra \in I$.

Hence, $\mathrm{Rad}(I)$ is an ideal of R.

For an element $a \in R$, we shall use (a) to denote the ideal generated by a. Ideals generated by one element are called **principal ideals**. We say that a **divides** $b \in R$ (written $a \mid b$) if there exists $x \in R$ such that $ax = b$. Also, a and b are **associates** if $a \mid b$ and $b \mid a$. In an integral domain, the definition of a and b are associates is equivalent to there exists a unit u such that $au = b$.

Exercise 4 Let a, b, u be elements of R with u a unit.

(a) Show that $a \mid b$ if and only if $(b) \subset (a)$.

(b) Show that a and b are associates if and only if $(a) = (b)$.

(c) Show that $(u) = R$.

Solution:

(a) If $a \mid b$, then $ax = b$ for some $x \in R$, and for all $y \in (b)$ we have $y = bk$ for some $k \in R$, which means

$$y = bk = axk \in (a),$$

so $(b) \subseteq (a)$.

Now if $(b) \subseteq (a)$, then $b \in (b) \subseteq (a)$, and thus $b = ax$ for some $x \in R$, i.e. $a \mid b$.

(b) If a and b are associates, then $a \mid b$ and $b \mid a$, so by (a) we know $(b) \subseteq (a)$ and $(a) \subseteq (b)$, which gives $(a) = (b)$.

Now if $(a) = (b)$, then $(a) \subseteq (b)$ and $(b) \subseteq (a)$, so $b \mid a$ and $a \mid b$ by (a), so a and b are associates.

(c) Since $1_R = u^{-1} \cdot u \in R$, so for all $r \in R$ we know

$$r = r \cdot 1_R \in (u),$$

which means $R \subseteq (u)$, and thus $(u) = R$.

We say that an element $c \in R$ is **irreducible** if c is a nonzero nonunit and

$$c = ab \quad \Longrightarrow \quad a \text{ or } b \text{ is a unit.}$$

An element $p \in R$ is **prime** if p is a nonzero nonunit and

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ or } p \mid b.$$

Exercise 5 Let R be an integral domain, and $p, c \in R$ be nonzero nonunits.

(a) Show that p is prime if and only if (p) is a prime ideal.

(b) Show that c is irreducible if and only if (c) is maximal (with respect to inclusion) among proper principal ideals of R.

(c) Prove that every prime element of R is irreducible.

Solution:

(a) If p is prime, then for $ab \in (p)$, we know $ab = kp$ for some $k \in R$, so $p \mid ab$, and thus $p \mid a$ or $p \mid b$ since p is prime, i.e. $a \in (p)$ or $b \in (p)$, so (p) is a prime ideal.

If (p) is a prime ideal, and if $p \mid ab$, then $ab \in (p)$, and thus $a \in (p)$ or $b \in (p)$ since (p) is a prime ideal, and this means $p \mid a$ or $p \mid b$, so p is prime.

(b) We can rephrase the problem: c is irreducible if and only if $(c) \subseteq (d) \subsetneq R$ implies $(d) = (c)$ for $d \in R$.

If c is irreducible, and if $(c) \subseteq (d) \subsetneq R$ for some $d \in R$, then $d \mid c$, so $c = dk$ for some $k \in R$. Since, c is irreducible, so d or k is a unit.

- Case 1: d is a unit, then $(d) = R$, so this case is impossible.
- Case 2: k is a unit, then $d = ck^{-1}$ and thus $c \mid d$. Hence, we have $d \mid c$ and $c \mid d$, which means c and d are associates, and thus $(c) = (d)$ by 4(b).

Hence, we must have $(d) = (c)$ since Case 2 is the only possible case.

Now if $(c) \subseteq (d) \subsetneq R$ implies $(d) = (c)$ for $d \in R$, and suppose $c = ab$, then we want to show a is a unit or b is a unit.

- Case 1: a is a unit, then we're done.
- Case 2: a is not a unit, then (a) is a proper ideal of R, and since $a \mid c$, so $(c) \subseteq (a)$, which gives $(c) = (a)$, so $a = ck$ for some $k \in R$, so

$$c = ab = (ck)b \implies c(1_R - kb) = 0.$$

Since c is nonzero and R is an integral domain, so we must have $1_R = kb$, which shows b is a unit, and we're done.

(c) Suppose p' is a prime element of R and $(p') \subseteq (q) \subsetneq R$ for some $q \in R$, then we know $p' = qs$ for some $s \in R$, and thus $p' \mid q$ or $p' \mid s$ since p' is prime.

- Case 1: If $p' \mid s$, then $(s) \subseteq (p') \subseteq (q) \subsetneq R$, so

$$s = qx = p'y = qsy \implies s(1 - qy) = 0.$$

Since p' is prime and thus non-zero, which gives s is non-zero. Hence, $1 - qy = 0$ since R is an integral domain. Thus, q is a unit, so $(q) = R$, which is impossible.
- Case 2: If $p' \mid q$, then $(q) \subseteq (p')$, which gives $(p') = (q)$.

Since Case 2 is the only possible case, so we know $(p') = (q)$. Hence, by (b) we know p' is irreducible, and we're done.

A **principal ideal domain (PID)** R is an integral domain in which every ideal is principal, i.e., of the form (r) for some $r \in R$.

Exercise 6 Let R be a PID.

(a) Prove that an element $p \in R$ is prime if and only if it is irreducible.

(b) Prove that every nonzero ideal I of R is maximal if and only if it is prime.

Solution:

(a) Since every PID is an Integral domain, so $p \in R$ is prime implies p is irreducible by 5(c).

Now if $p \in R$ is irreducible, and suppose $p = ab$. Then consider

$$(p, a) = \{xp + ya : x, y \in R\},$$

we know (p, a) is an ideal and thus $(p, a) = (d)$ for some $d \in R$. Hence, we have $p \in (p, a) = (d)$, and thus $p = ds$ for some $s \in R$. Since p is irreducible, so d or s is a unit.

- Case 1: d is a unit, then $(d) = R$, which means

  $$1_R = xp + ya \text{ for some } x, y \in R,$$

  so we have

  $$b = xpb + yab = xpb + yp = p(xb + y),$$

  which gives $p \mid b$.
- Case 2: s is a unit, then $ps^{-1} = d$ and thus $p \mid d$, so we know p and d are associates and thus $(p) = (d) = (p, a)$. Thus, $a \in (p, a) = (p)$, i.e. $p \mid a$.

Hence, $p \mid a$ or $p \mid b$ would occur, and thus p is prime.

(b) If $I = (d)$ is a maximal non-zero ideal of R, and suppose $ab \in I = (d)$, then $ab = dk$ for some $k \in R$. Consider $(I, a) = \{xd + ya : x, y \in R\}$, then we know $I \subseteq (I, a)$, and we thus have two cases:

- Case 1: $(I, a) \neq I$, then $(I, a) = R$ since I is maximal, so $\exists x, y \in R$ s.t.

  $$1_R = xd + ya \implies b = xbd + yab = xbd + ydk = d(xb + yk),$$

  so $d \mid b$ and thus $b \in (d)$.
- Case 2: $(I, a) = I$, then $a \in (I, a) = I = (d)$.

Hence, $a \in (d)$ or $b \in (d)$ would occur and thus $(d) = I$ is prime.

If $I = (p)$ is a non-zero prime ideal of R, then p is prime by 5(a), and thus p is irreducible by 6(a), so by 5(b), we know $(p) \subseteq (q) \subsetneq R$ implies $(p) = (q)$ for all $q \in R$. However, since R is a PID, so every ideal can be written in the form of (q) for some $q \in R$, and thus for all proper ideal (q) of R, we must have $(p) = (q)$, i.e. $(p) = I$ is maximal.